Kollaboratives Management von Informationssicherheitsrisiken in strategischen Allianzen

Ein Meta-Framework zum Aufbau eines gemeinsamen Prozesses

Michael Schmidt

München 2024

INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Kollaboratives Management von Informationssicherheitsrisiken in strategischen Allianzen

Ein Meta-Framework zum Aufbau eines gemeinsamen Prozesses

Dissertation
an der Fakultät für Mathematik, Informatik und Statistik
der Ludwig-Maximilians-Universität München

eingereicht von

Michael Schmidt

am 20. Februar 2024

1. Gutachter: Prof. Dr. Helmut Reiser, Ludwig-Maximilians-Universität München (LMU)

2. Gutachter: Prof. Dr. Bernhard Neumair, Karlsruher Institut für Technologie (KIT)

Tag der mündlichen Prüfung: 07.06.2024

Eidesstattliche Versicherung

(gemäß § 8 Abs. 2 Nr. 5 der Promotionsordnung vom 12. Juli 2011)

Hiermit erkläre ich, Michael Schmidt, an Eides statt, dass die Dissertation mit dem Titel „Kollaboratives Management von Informationssicherheitsrisiken in strategischen Allianzen“ von mir selbstständig und ohne unerlaubte Beihilfe angefertigt wurde.

Eching, 17.06.2024, Michael Schmidt

Danksagung

Diese Arbeit entstand während meiner Tätigkeit am Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften. In dieser Zeit war ich ebenfalls als Vertreter für das Deutsche Forschungsnetz (DFN) im EU-Projekt GÉANT aktiv. Durch diesen Mix aus lokalen Aufgaben und einer Zusammenarbeit mit den internationalen Partnern konnte ich wertvolle Erfahrungen sammeln, welche diese Arbeit erst ermöglicht haben.

Allen voran gilt mein besonderer Dank meinem Doktorvater Prof. Dr. Helmut Reiser, der diese Arbeit mit seiner Zeit und Expertise unterstützt hat. Dabei hat er nicht nur stets zum Schreiben eigener wissenschaftlicher Artikel angeregt, sondern insbesondere zum Peer-Review anderer Veröffentlichungen, um die eigene Gedankenwelt zu verlassen. Ebenfalls bedanken möchte ich mich bei Prof. Dr. Bernd Neumeier für die investierte Zeit in seiner Rolle als Zweitgutachter.

Insgesamt danke ich allen Kolleginnen und Kollegen, mit denen ich über die Jahre am LRZ zusammengearbeitet habe. Ebenso gilt mein Dank allen Personen aus dem GÉANT-Umfeld, mit denen ich spannende Themen aus den Bereichen Trust & Identity und Security bearbeiten durfte. Neben den wertvollen Erfahrungen und dem gesammelten Wissen haben mir diese Tätigkeiten stets viel Freude bereitet.

Ich möchte mich besonders bei Michael Brenner bedanken, der nicht nur meine anfängliche Leidenschaft für Prozesse geweckt hat, sondern auch meine erste Veröffentlichung gefördert und so den Grundstein für den wissenschaftlichen Werdegang gelegt hat. Vielen Dank auch an Stefan Metzger, der mir am LRZ von Anfang an viele Möglichkeiten geboten hat mich einzubringen, das integrierte Managementsystem am LRZ mitzugestalten und ohne den ich bestimmt nicht im Bereich Risikomanagement gelandet wäre. Miran Mizani danke ich für die gemeinsamen Paper, die spannenden Diskussionen und seine stets motivierte Ausstrahlung, mit der er mich oftmals neu anspornen konnte. Gerne erinnere ich mich auch an die Zusammenarbeit mit Tanja Hanauer und Markus Gillmeister zurück, mit denen ich sehr viel Spaß hatte, den Risikomanagementprozess am LRZ zu gestalten.

Zuletzt spielt natürlich auch das private Umfeld eine besondere Rolle und daher möchte ich allen meinen Freunden danken, die über die Jahre hinweg an meiner Seite waren. Ein besonderer Dank gilt meinen Eltern und meiner Schwester für den familiären Rückhalt und die Unterstützung über meinen bisherigen Lebensweg hinweg. Von ganzem Herzen danke ich meiner Lebensgefährtin Sandra, die mich bei diesem Projekt von Anfang an begleitet, stets bestärkt und unterstützt hat.

Zusammenfassung

In den letzten Jahrzehnten wurden IT Produkte und Services immer komplexer, was auch zu einer zunehmenden Verflechtung der Unternehmen geführt hat. Kaum eine Organisation kann in diesen verknüpften Märkten noch völlig isoliert agieren und kommt ohne Beziehungen zu anderen Organisationen aus. Es formen sich zunehmend organisations- oder branchenübergreifende Partnerschaften, um Herausforderungen gemeinsam zu meistern. Manche Organisationen gehen einen Schritt weiter und formen strategische Allianzen, die eine besonders intensive Zusammenarbeit pflegen. Im Gegensatz zu einer einfachen Geschäftsbeziehung über einzelne Dienstleistungen oder einer kooperativen Partnerschaft in einem bestimmten Geschäftsbereich, zielt eine Allianz auf eine enge Kollaboration ab, um die gemeinsamen Ziele der Partner zu erreichen. Neben den gemeinsamen Unternehmungen die in einer Allianz die Geschäftsziele vorantreiben, besteht auch die Möglichkeit, weitere Herausforderungen durch gemeinsame IT Managementfunktionen zu lösen. Ein zentraler Aspekt in der Informationssicherheit ist das Risikomanagement, welches jede Organisation, die ein Informationssicherheitsmanagementsystem betreibt, implementiert hat. Allianzen entwickeln sich oftmals in gleichen Branchen oder Lieferketten, wodurch diese sowohl von den gleichen Bedrohungen betroffen sein können als auch gemeinsame Risiken behandeln wollen. Um die Zusammenarbeit in diesem Bereich zu erleichtern, wird in dieser Arbeit ein Meta-Framework für organisationsübergreifendes Informationssicherheitsrisikomanagement (ISRM) in strategischen Allianzen erstellt. Dabei wird davon ausgegangen, dass die Organisationen bereits ein Vorgehen zum ISRM etabliert haben, welches sich allerdings im Kontext eines Enterprise Risk Managements nur auf die eigene Organisation bzw. erweitert durch ein Supply Chain Risk Management auf Lieferanten bezieht. Die Frage ist also, wie die Teilnehmer der Allianz über das einfache Teilen von Informationen hinaus zusammenarbeiten können, um übergreifende Risiken zu identifizieren und eventuell gemeinsam zu behandeln. Das Framework besteht aus vier Komponenten, welche Organisationen dabei unterstützen, einen kollaborativen Prozess innerhalb der Allianz zu etablieren. Dazu liefert es ein Partnerschaftsmodell, mit dessen Hilfe sich die Anwendbarkeit des Prozesses innerhalb einer Partnerschaft evaluieren lässt. Eine gemeinsame Terminologie liefert die Grundlage, um die Konzepte und Begriffe innerhalb der Allianz zu vereinheitlichen und eine effektive Kommunikation zu ermöglichen. Der kollaborative Prozess definiert Abläufe, Schnittstellen und Verantwortlichkeiten innerhalb der Allianz, um gemeinsame Risiken zu verwalten. Letztlich liefern unterstützende Ressourcen die Werkzeuge für die Definition von Bedrohungen, Assets und einer Risikomethode im Prozess.

Abstract

IT products and services have become increasingly complex over the last few decades, which has resulted in an increasing interdependence of businesses. Hardly any organisation is capable to operate in complete isolation in these interconnected markets or without relationships to other organisations. More and more interorganisational or cross-sector partnerships are being formed to overcome challenges together. Some organisations are taking this even further and forming strategic alliances that foster particularly intensive collaboration. In contrast to a simple business relationship based on individual services or a co-operative partnership in a specific business area, an alliance is aimed at close collaboration in order to achieve the partners' common goals. In addition to the joint activities that drive the business objectives in an alliance, there is also the possibility of solving other challenges through joint IT management functions. A key aspect of information security is risk management, which every organisation that operates an information security management system has in place. Alliances often develop within one industry or supply chain, which means that are likely to be affected by similar threats and may want to address these common risks. In order to facilitate collaboration in this area, this thesis develops a meta-framework for interorganisational information security risk management (ISRM) in strategic alliances. It is assumed that the organisations have already established an ISRM process, albeit one that only refers to their own organisation in the context of enterprise risk management or is extended to suppliers through supply chain risk management. This raises the question of how the participants in the alliance can cooperate beyond the simple task of information sharing in order to identify overarching risks and possibly deal with them together. The framework consists of four components that support organisations in establishing a collaborative process within the alliance. It provides a partnership model that can be used to evaluate the applicability of the process within a partnership. A common terminology provides the basis for harmonising the concepts and terms within the alliance and enabling effective communication. The collaborative process defines procedures, interfaces and responsibilities within the alliance to manage shared risks. Finally, supporting resources provide the tools to define threats, assets and a risk methodology in the process.

Inhaltsverzeichnis

Kapitel 1

Einführung

Der sichere Umgang mit Informationen ist ein Thema, welches zunehmend von Unternehmen aller Größen und Branchen als eine Kerndisziplin eingestuft wird. Insbesondere durch die stark erhöhte Medienaufmerksamkeit die von öffentlich gewordenen Sicherheitsvorfällen ausgelöst wird und dem daraus resultierenden Reputationsverlust [1, 2], ist das Thema Security in den Fokus des Top-Managements vieler Organisationen gewandert. Ein Rückblick in die nähere Vergangenheit zeigt, dass Angriffe auf Unternehmen im Verlauf der letzten 20 Jahre immer häufiger zu großen öffentlichen Skandalen geführt haben, insbesondere, wenn personenbezogene Daten betroffen waren. Die Beispiele sind zahlreich, angefangen bei großen Ereignissen wie dem AOL Datenleck 2004 [3] mit dem Verlust von 92 Millionen Datensätzen, über den Diebstahl von über 500 Millionen Kreditkartendaten der Marriot Hotels 2018 [4], bis hin zur Offenlegung der persönlichen Daten von über 533 Millionen Facebook-Nutzern im Jahr 2021 [5]. Diese und viele weitere Vorfälle [6] in den vergangenen Jahren haben gezeigt, dass ganzheitliches Sicherheitsmanagement und der Umgang mit potenziellen Gefahren ein in Organisationen lange vernachlässigtes Thema war. Insbesondere durch solche medienwirksamen Ereignisse wurden inzwischen auch viele Verantwortliche in Unternehmen sensibilisiert und das intrinsische Interesse an der Vermeidung von Sicherheitsvorfällen steigt, da Security nicht mehr nur als Kostenfaktor, sondern Wettbewerbsvorteil erkannt wurde. Auf der anderen Seite schaffen nationale und internationale Vorschriften, wie das *IT-Sicherheitsgesetz* [7, 8], die *Datenschutzgrundverordnung* [9] oder die *NIS-Direktive* [10, 11], einen strengen rechtlichen Rahmen, durch den Organisationen ein zusätzliches extrinsisches Interesse am Schutz ihrer Daten haben. Somit müssen Unternehmen nicht mehr nur den klassischen Schutz der IT-Systeme gewährleisten, sondern auch organisatorische sowie menschliche Faktoren berücksichtigen und dabei Aspekte wie Datenschutz und Compliance einbeziehen. Aus diesem Grund stehen das Thema Sicherheitsmanagement und damit in Zusammenhang stehende Zertifizierungen, etwa gemäß *ISO/IEC 27001* [12] oder in Deutschland auch *IT-Grundschutz* [13], immer stärker im Fokus. Die dabei etablierten Managementsysteme versprechen einen ganzheitlichen Ansatz, um Sicherheitsprobleme zu adressieren. Den meisten gemeinsam ist, dass sie ein risikobasiertes Vorgehen fördern, um Gefahren zu erkennen, diese zu priorisieren und im Einklang mit der Unternehmens-, IT- und Sicherheitsstrategie zu behandeln.

1.1 Motivation

IT-Sicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht seit 2005 jährlich einen Bericht zur Lage der IT-Sicherheit in Deutschland [14]. Seit dem ersten Erscheinen hat sich die Länge des Berichts verdoppelt, die Anzahl gelisteter Gefährdungen ist kontinuierlich gestiegen und die Auswirkungen auf staatliche, wirtschaftliche und gesellschaftliche Aspekte haben zugenommen. Parallel dazu hat sich auch der Reifegrad der IT-Sicherheit, welche auf die Absicherung von IT-Systemen abzielt und versucht technische Schwachstellen zu minimieren, in vielen Unternehmen bereits deutlich erhöht. Allerdings hat sich auch gezeigt, dass viele Vorfälle gar nicht auf technischen, sondern organisatorischen Schwachstellen basieren, wie etwa aufgrund von mangelndem Sicherheitsbewusstsein des Personals, fehlerhaften oder undefinierten Prozessen, Systemausfällen oder Sicherheitsproblemen bei Lieferanten [15, 16, 17]. Organisationen sind also gut beraten, auf die Gesamtheit der sicherheitsrelevanten Maßnahmen zu achten und ihr Sicherheitsprogramm entsprechend auszuweiten.

IS Risiken

Nachdem Security lange Zeit hauptsächlich ein technisches Thema gewesen war, ist die Information Security (IS) im Zuge der Digitalisierung heute zum zentralen Aspekt in Organisationen aller Größen und Branchen geworden [18]. Der Umgang mit Informationen, deren Speicherung und Verarbeitung, ist für die meisten Unternehmen in Industrienationen inzwischen unerlässlich geworden und der Bedarf nimmt stetig zu. Durch diese zunehmende Abhängigkeit von Informationen und informationsverarbeitenden Systemen wird auch deren Schutz immer wichtiger, aber auch komplexer und ressourcenintensiver [19]. Dabei rückt das Risk Management (RM) immer weiter in den Fokus des Sicherheitsmanagements [20]. Ursprünglich eine klassische wirtschaftswissenschaftliche Disziplin, wurden die Grundprinzipien des risikobasierten Vorgehens inzwischen für verschiedenste Bereiche adaptiert. So findet sich auch ein kombiniertes Feld aus IS und RM, das sogenannte Information Security Risk Management (ISRM). Dabei unterscheidet sich das ISRM insofern, als es die grundsätzlichen Konzepte im Design, der Risikoeinschätzung und der Risikobehandlung adaptiert [21]. Es bietet spezifische Methoden zur Identifikation von Informationssicherheitsrisiken, deren Bewertung und Behandlung, um damit Organisationen bei der Planung ihrer Sicherheitsstrategie zu unterstützen. Das ISRM liefert einen Lösungsansatz für ein immer größer werdendes Problem des Sicherheitsmanagements: das Ressourcenmanagement. Bei zunehmender Bedrohungslage strebt das Information Security Management (ISM) den bestmöglichen Schutz von Informationen und Technologie an, jedoch verfügt jede Organisation nur über begrenzte Ressourcen, um auf Bedrohungen zu reagieren.

Beziehungen

Unabhängig von der IS begegnen Organisationen diesem Engpass oftmals mit Partnerschaften, die ihnen Zugriff auf zusätzliche Ressourcen (Produkte, Anlagen, Organisationseinheiten oder Beziehungen) verschaffen [22, 23]. Daher suchen Organisationen aller Art heute verstärkt nach Allianzen, welche die eigenen strategischen sowie operativen Fähigkeiten ergänzen. Dabei interagieren Organisationen stärker und in mehr Bereichen miteinander als bei einer klassischen Lieferantenbeziehung. Durch das Integrieren von Produkten und Dienstleistungen werden allerdings auch Abhängigkeitsbeziehungen geschaffen. „Suddenly, information security risks cross boundaries, so that organisations become dependent on

their partners to create information security“ [24, S. 419]. Dabei findet oftmals der Risikobegriff Anwendung, bei dem sowohl potenzielle Risiken als auch Chancen der Partnerschaft gegeneinander abgewogen werden. [25, 26, 27]

Risiken

Die zunehmende Anzahl solcher Partnerschaften in den letzten zwei Jahrzehnten spiegelt sich auch im starken Anstieg der Forschung zu strategischen Allianzen wider [28]. Was allerdings selten betrachtet wird, ist die Kollaboration im RM selbst als gemeinsame Managementfunktion von Organisationen. Dabei geht es um die Etablierung eines kollaborativen Prozesses zur Einbeziehung der strategischen Partner in die Identifizierung, Bewertung und Behandlung von Risiken. Diese Risiken können sowohl die Organisationen der Partnerschaft im Einzelnen betreffen, aus kausalen Verknüpfungen der Unternehmensaktivitäten entstehen oder die Partnerschaft als Ganzes tangieren. Durch Anwendung eines gemeinsamen RM kann das Vorgehen zur Reduzierung von Risiken von einer organisationsinternen in eine ganzheitliche Strategie transformiert werden, bei der die Perspektiven der Lieferanten, Partner und Stakeholder miteinbezogen werden. Weiterhin kann die Auswirkung für jede einzelne Organisation, durch Verteilen der Risiken auf die Partner, verringert werden (insbesondere im IS Bereich). Ein gemeinsames Vorgehen führt außerdem zu einer Erhöhung der Sichtbarkeit von Risiken innerhalb der Partnerschaft und letztlich auch zu einer gemeinsamen Risiko-Kultur. [29]

Kollaboration im RM

Zwar existieren bereits einzelne Forschungsarbeiten zum kollaborativen (joint/relational) Supply Chain Risk Management (SCRM), diese liefern allerdings keinen ganzheitlichen Ansatz zum gemeinsamen RM [30, 31, 32, 33]. Friday et al. [29] berichten in ihrem umfassenden, systematischen Literaturreview zum Collaborative Risk Management (CRM): „its conceptualisation is fragmented by multiple definitions, theories, and fractional application of relational capabilities, all of which limit understanding of the concept and its development“ und schlussfolgern „Despite the support for collaborative approaches as an important means to enhance conventional SCRM techniques, CRM remains in its infancy, its advancement hindered by lack of consensus on key conceptual and theoretical foundations“. Somit ist die Idee eines organisationsübergreifenden CRM als potenzielle Erweiterung zum klassischen RM zum aktuellen Zeitpunkt noch nicht klar definiert. Neben einheitlichen Strukturen und Konzepten fehlt ein grundsätzliches Verständnis für diese Art der Zusammenarbeit und wie sie weiterentwickelt werden kann. Dabei bezieht sich die meiste Literatur auf andere RM Teilbereiche, während sich im ISRM kaum Ansätze für ein kollaboratives, organisationsübergreifendes Vorgehen finden.

Existierende Ansätze

Auch im IS Bereich ist ein kollaboratives Vorgehen innerhalb von strategischen Partnerschaften denkbar, bei dem übergreifende oder geteilte Sicherheitsaspekte gemeinsam betrachtet werden. Karlsson et al. [24] zeigen jedoch, dass das Thema der interorganisationalen IS inzwischen zwar höchst relevant geworden ist und eine große Anzahl an wissenschaftlichen Veröffentlichungen existiert, aber das Feld als Ganzes weiterhin eher unreif bleibt und weitere Aufmerksamkeit benötigt. Sie kommen daher unter anderem zu dem Ergebnis, dass zukünftige Forschung sich auf „existing processes and how they are carried out in inter-organisational settings“ [24, S. 437] konzentrieren sollte. Diese Arbeit beschäftigt sich nun im Detail mit einem ISM Prozess und untersucht die Anwendbarkeit und Umsetzung des ISRM in interorganisationalen Beziehungen.

1.2 Fragestellung

Klassisches RM

Bei Durchführung des ISRM in einer einzelnen Organisation können neue Risiken dadurch ermittelt werden, dass Sicherheitsschwachstellen in Abläufen und Systemen identifiziert und potenzielle Bedrohungen zu diesen modelliert werden. Folgend sind bei nicht akzeptablen Risiken auch Maßnahmen zu implementieren, welche das Risiko reduzieren und damit letztlich das Sicherheitsniveau der Organisation erhöhen. Dieses Vorgehen lässt sich nicht direkt auf einen organisationsübergreifenden Ansatz abbilden, da die Auswirkungen von Schadensszenarien nur organisationsintern, also von und für die Organisation, bewertet werden. Die Berechnung eines Risikos basiert auf den Rahmenbedingungen in der eigenen Organisation, d.h. sie berücksichtigen die etablierten Sicherheitsmaßnahmen und sind an den Organisationswerten ausgerichtet.

Herausforderungen

Soll das ISRM nun innerhalb einer organisationsübergreifenden Partnerschaft stattfinden, kann die Identifikation, Bewertung und Behandlung von Risiken nicht mehr nur nach innen gerichtet erfolgen. Stattdessen müssen diese Schritte mit den Partnern abgestimmt und koordiniert werden, um ein gemeinsames Vorgehen zu etablieren. Aufgrund der unterschiedlichen Strukturen, Abläufe und auch (IS) Reifegrade in einer solchen Partnerschaft kann ein einheitliches Vorgehen allerdings nicht einfach etabliert werden, wenn die Unabhängigkeit der Einzelorganisationen erhalten bleiben soll. Dabei wird in dieser Arbeit davon ausgegangen, dass eine Vereinheitlichung von Strukturen, Funktionen und Prozessen über Organisationsgrenzen hinweg im Kontext einer strategischen Allianz nicht erreichbar oder angestrebt ist. Solche Konstellation, bei denen alle Organisationen über die gleiche Macht bzw. Entscheidungskompetenz innerhalb der Partnerschaft verfügen, wurden in der Vergangenheit seltener betrachtet [34].

Organisationshierarchie

Bei der organisationsübergreifenden Zusammenarbeit im Kontext von Managementfunktionen werden Umgebungen mit zwei oder mehr Organisationen betrachtet, die eine strategische Partnerschaft eingehen, um dadurch gemeinsame Ziele zu erreichen. Die teilnehmenden Organisationen können, je nach Typ der Beziehung, gleichzeitig als Lieferanten, Dienstleister und Kunden von Diensten auftreten. Dabei findet die Zusammenarbeit oftmals auf einer partnerschaftlichen Ebene statt, die sich nicht direkt in einer traditionellen Kunden-Lieferanten-Beziehung widerspiegelt. Das steht im Kontrast zum klassischen ISRM, bei dem meist einzelne Organisationen mit einer Top-Down Management-Hierarchie betrachtet werden. So ist etwa laut der internationalen Norm *ISO/IEC 27001* [12] die Durchsetzbarkeit von Vorgaben innerhalb einer Unternehmensgruppe eine zwingende Voraussetzung, ohne die auch keine Zertifizierung erfolgen kann.

Unabhängigkeit

Im Gegensatz dazu sind die Organisationen innerhalb einer Partnerschaft organisatorisch und/oder wirtschaftlich unabhängig voneinander. Es fehlt also eine übergeordnete autoritäre Dachorganisation, welche ein zentrales und weisungsbefugtes Management bereitstellen könnte. Somit sind die Organisationen selbstständig und etablieren Schnittstellen in bestimmten Bereichen, in denen die Partner zusammenarbeiten wollen. Es scheint daher unwahrscheinlich und unpraktikabel in vielen verschiedenen Organisationen mit unterschiedlichen Rahmenbedingungen den exakt gleichen Prozess zu etablieren. Dies würde mindestens die gleiche Organisationsstruktur, jedoch insbesondere Abstimmung bei Aus-

wahl von Rahmenwerken und Standards voraussetzen, was eine hohe organisatorische Hürde darstellt. Es gilt also, einen verteilten Ansatz zum ISRM zu finden, welcher von den Organisationen unabhängig voneinander durchgeführt werden kann. Das heißt, das klassische Vorgehen muss um entsprechende Kommunikationsschnittstellen zur Kooperation, etwa bei der Risikoeinschätzung und Behandlung, erweitert werden. Da eine solche Erweiterung etablierte Techniken und Frameworks unterstützen soll, ist die Integration in ein generisches Prozessmodell notwendig.

Forschungsfrage

Zwar finden sich bereits viele Standards und Rahmenwerke in den Bereichen IS und RM, jedoch keines das die organisationsübergreifende Kooperation im ISRM explizit betrachtet. Trotzdem ist davon auszugehen, dass eine generelle Methodik, wie sie etwa im internationalen Standard ISO 31000 [35] definiert ist, auch organisationsübergreifend analog anwendbar ist. Es gilt allerdings herauszufinden, wie diese per Definition organisationsinternen Prozesse angepasst oder erweitert werden können, um Schnittstellen für die Kommunikation von Risikoinformationen und die Kollaboration bei den ISRM Aktivitäten zu ermöglichen. Ausgehend von den beschriebenen Rahmenbedingungen stellt sich die Frage, wie ein neues Vorgehen konzipiert werden kann, welches das ISRM für die Anwendung im organisationsübergreifenden Kontext adaptiert und dessen spezifische Anforderungen berücksichtigt.

> *Ziel dieser Arbeit ist die Erweiterung des ISRM zur Anwendung in interorganisationalen Beziehungen von zwei oder mehr Organisationen. Das Ergebnis soll durch die Verknüpfung von verteilten Aktivitäten den Aufbau eines gemeinsamen Prozesses unterstützen, um ein kollaboratives Management von Sicherheitsrisiken zu ermöglichen. Dieses Konzept soll Organisationen klare Vorteile gegenüber einem isolierten Vorgehen liefern und das Sicherheitsniveau der gesamten Allianz langfristig verbessern.*

Teilfragen

Um dieses Ziel zu erreichen soll untersucht werden, wie existierende Methoden und Modelle adaptiert und um entsprechende Schnittstellen zur Koordination und Kommunikation von Risiken sowie notwendigen Prozessartefakten erweitert werden können. Aufbauend auf etablierten Industriestandards zum ISRM wird ein Meta-Framework zur Verknüpfung autonomer Managementprozesse erstellt, welches Organisationen beim Aufbau eines kollaborativen Prozesses helfen kann. Daraus ergeben sich die folgenden Teilfragestellungen:

- **Anwendbarkeit:** In welchem organisatorischen Kontext, d.h. welchen Arten bzw. Ausprägungen von interorganisationalen Beziehungen, kann kollaboratives ISRM sinnvoll angewendet werden?
- **Standardisierung:** Welche Aspekte des ISRM müssen einheitlich definiert werden, um eine Zusammenarbeit zwischen unabhängigen Organisationen zu ermöglichen?
- **Kollaboration:** Wie können relevante ISRM Aktivitäten erweitert werden, um die Kommunikation und Zusammenarbeit zwischen Prozessen in mehreren Organisationen zu ermöglichen?
- **Organisation:** Wie lässt sich die Zusammenarbeit in einem solchen interorganisationalen Prozess im Hinblick auf Hierarchien, Verantwortlichkeiten und Entscheidungsfindung organisieren?

1.3 Einordnung der Arbeit

Literatur

Obwohl der Bereich RM sehr groß ist und sehr viele Teilbereiche umfasst, konzentriert sich der Großteil davon auf Risiken innerhalb der Grenzen einer einzelnen Organisation. Dabei wird der Umgang mit Risiken und Chancen als rein organisationsinterne Aufgabe betrachtet, bei denen Bedrohungen der einzige externe Faktor sind. Dementsprechend setzen die entstehenden Risiken die eigene Organisation ins Zentrum, die Beziehung zu anderen Organisationen wird nicht berücksichtigt und auch deren Behandlung wird unabhängig durchgeführt. Organisationsübergreifende Anwendungsfälle werden in der Praxis nur selten betrachtet, wobei sich zumindest in der wissenschaftlichen Literatur Beispiele für organisationsübergreifendes RM [29] finden lassen.

Supply Chain Risk Management

Als Erweiterung des internen RM stehen beim SCRM zumindest Lieferantenorganisationen im Mittelpunkt der Betrachtung [36]. Jedoch wird auch hier kein kombinierter Ansatz verfolgt, bei dem das RM des Lieferanten und das eigene integriert wird. Stattdessen werden diese Organisationen zur Risikoquelle und als zusätzliche Dimension hinzugefügt. Ein kollaboratives Vorgehen bei der Analyse oder Behandlung von Risiken ist nicht vorgesehen. Insgesamt sind die herkömmlichen Methoden des SCRM bei der Steuerung von organisationsübergreifenden Auswirkungen von Risiken nicht besonders effektiv [29]. Zwar existiert bereits die grundsätzliche Idee der Zusammenarbeit in Form eines CRM, aber ein anwendbares Prozessmodell oder praktische Ansätze existieren dazu bisher nicht.

Information Security Risk Management

Noch weniger Ansätze finden sich im Spezialgebiet des ISRM. Der Teilbereich ist deutlich jünger als das RM als Ganzes und nicht alle bekannten Methoden aus anderen Bereichen wurden bereits adaptiert. Während RM und viele Teilbereiche klassische wirtschaftswissenschaftliche Disziplinen sind, entspringt die IS der Informatik. Das ISRM als Schnittmenge hat damit eine natürliche Verbindung zu Informationen und Technologie. Somit sind auch Anwendungsbereich und Rahmenbedingungen des ISRM unterschiedlich von anderen RM Teilbereichen, weshalb Methoden nicht einfach übernommen werden können. Hier gibt es bisher kaum Bestrebungen der Entwicklung des organisationsübergreifenden Ansatzes im Sinne eines kollaborativen ISRM.

Aktuelle Forschung

Die Relevanz des Themas zeigt sich insbesondere in den kürzlichen Aktivitäten der European Union Agency for Cybersecurity (ENISA). Seit langem hat die EU Agentur wieder zum Thema ISRM publiziert und veröffentlicht Forschung zur Interoperabilität von ISRM Frameworks [37, 38]. Dabei offenbart sich, dass Kollaboration zukünftig ein essenzieller Teil der Behandlung von IS-Risiken sein wird. Diese Zusammenarbeit soll nicht nur organisationsübergreifend, sondern auch länderübergreifend notwendig werden, um das Cyber Security Niveau in der EU zu stabilisieren. Die ENISA konzentriert sich dabei insbesondere auf die Austauschbarkeit und Vergleichbarkeit der Risikobewertung, um das Risikoniveau verschiedener Organisationen uniform darstellen zu können. Ziel der ENISA ist es, eine Methode zu entwickeln, um den Mitgliedsstaaten die Zusammenarbeit im ISRM zu ermöglichen. Der Ansatz zielt jedoch im Kern auf die Interoperabilität verschiedener, internationaler Methoden ab, um deren Ergebnisse vergleichbar zu machen. Die ENISA stellt aktuell kein Vorgehen bereit, um es mehreren Organisationen zu erlauben, ihre Prozesse zu verknüpfen und ISRM gemeinsam zu betreiben.

Informationen

Ein klassischer Bereich zur interorganisationalen Zusammenarbeit ist der Austausch von Ressourcen und Wissen zwischen Organisationen [22]. Ansätze davon wurden auch bereits adaptiert, etwa beim Teilen von IS bezogenen Informationen innerhalb eines Netzwerks von Organisationen [39, 40]. Insbesondere das Teilen von Informationen bezogen auf technische Schwachstellen und Security Incidents ist dabei weit verbreitet [41, 42, 43, 44]. Einen Schritt weiter geht die gezielte Zusammenarbeit im *Security Incident Management* Prozess, um die Widerstandsfähigkeit der teilnehmenden Organisationen zu erhöhen [45]. Davon abgesehen finden sich kaum Beispiele zur Kooperation von Organisationen im Bereich ISM (mehr Details zu den genannten Anwendungsfällen liefert Kapitel 4).

Kollaboratives ISRM

Betrachtet man die Vorteile einer Kooperation zwischen Organisationen in diesen Bereichen, so lässt sich die Hypothese aufstellen, dass eine Kollaboration im ISRM ebenfalls Gelegenheit zur Zusammenarbeit liefert. Dabei ist von ähnlichen Vorteilen auszugehen, insbesondere in Bezug auf die Nutzung gemeinsamer Ressourcen und den Austausch von Informationen über Risiken, die letztlich zur Stärkung der teilnehmenden Organisationen und der Allianz als Ganzes führen könnten. Ein verteiltes Vorgehen zum ISRM ist dabei nicht nur in strategischen Partnerschaften unabhängiger Organisationen denkbar, sondern eventuell auch innerhalb von Teilbereichen einer verteilten Unternehmensstruktur oder föderalistisch organisierter Institutionen.

Scope und Abgrenzung

Im Rahmen der Arbeit sollen explizit nicht die fundamentalen Grundsätze des ISRM, wie etwa der Berechnung oder der Nutzung von Artefakten wie Assets und Bedrohungen, bewertet werden. Stattdessen sollen existierende Methoden analysiert und bezüglich ihrer Tauglichkeit für ein interorganisationales ISRM evaluiert werden. Weiterhin sollen die etablierten Kernaspekte des ISRM extrahiert und der Prozess lediglich zur organisationsübergreifenden Anwendung adaptiert werden. Das geplante Framework setzt ein existierendes ISRM in den Organisationen der Allianz voraus und definiert lediglich, wie das Enterprise Risk Management (ERM) der Partner verknüpft werden kann. Dabei soll ebenfalls nicht untersucht werden, wie sich strategische Partnerschaften bilden oder welchen Mehrwert diese liefern. Im Fokus stehen existierende Allianzen, welche ISRM als gemeinsame Managementfunktion etablieren wollen.

Veröffentlichungen

Im Kontext des Promotionsvorhabens wurden weiterhin verschiedene Artikel publiziert, welche in Anhang C gelistet werden. Nicht alle diese Veröffentlichungen stehen im direkten Zusammenhang mit dem Thema der Dissertation, manche betrachten eine angrenzende Fragestellung und andere sind eine Vorabveröffentlichung dieser Arbeit.

1.4 Vorgehensmodell

Dieses Kapitel lieferte eine Einführung in die Motivation und Problemstellung der Arbeit. Dabei wurde die Möglichkeit einer Zusammenarbeit im ISM und insbesondere ISRM in strategischen Partnerschaften aufgezeigt, welche neue Chancen für die beteiligten Organisationen eröffnet. In den nachfolgenden Kapiteln wird das angesprochene Meta-Framework erstellt, welches ein grundlegendes Konzept zum Aufbau eines interorganisationalen ISRM liefert. Die restliche Arbeit ist gemäß dem Vorgehensmodell in Abbildung 1.1 strukturiert.

Kapitel 2 Als nächstes beschäftigt sich Kapitel 2 mit den notwendigen Grundlagen für diese Arbeit. Dazu gehören die grundlegenden Begriffe aus den Bereichen IS und RM, sowie existierende Rahmenwerke und Vorgehensmodelle aus dem ISRM. Weiterhin wird ein Überblick über den aktuellen Forschungsstand im Bereich der strategischen, organisationsübergreifenden Zusammenarbeit von mehreren Organisationen geliefert.

Kapitel 3 Kapitel 3 liefert einen Überblick über verschiedene Szenarien von Organisationsbeziehungen, welche in der Industrie vorkommen. Zusätzlich wird ein Fallbeispiel aus dem öffentlichen Sektor vorgestellt, welches sich aufgrund seiner Eigenschaften besonders gut für eine Kollaboration anbietet. Aus existierender Literatur und den vorgestellten Szenarien werden die Erfolgskriterien für ein gemeinsames ISRM definiert und entsprechende Anforderungen abgeleitet, welche ein Rahmenwerk für interorganisationales ISRM erfüllen muss. Anschließend wird das Konzept zur Erstellung des kollaborativen Frameworks vorgestellt.

Kapitel 4 In Kapitel 4 werden die Rahmenbedingungen für interorganisationales ISRM definiert. Dazu werden als Erstes die verschiedenen Arten von Beziehungen zwischen Organisationen und ihre Eigenschaften untersucht, um deren Eignung für eine strategische Zusammenarbeit zu bewerten. Basierend auf den existierenden Erkenntnissen aus der Organisationstheorie, wird die Form der Zusammenarbeit definiert, die für ein gemeinsames ISRM notwendig ist. Anschließend werden für diese Formen konkrete Beziehungstypen beschrieben, in denen ein interorganisationales ISRM überhaupt sinnvoll anwendbar wäre.

Kapitel 5 Kapitel 5 untersucht verschiedene etablierte Prozess-Frameworks und vergleicht deren Terminologie. Auf dieser Basis werden Schlüsselkonzepte identifiziert, die ein Rahmenwerk für interorganisationales ISRM etablieren muss, um unabhängig vom organisationsspezifischen Vorgehen anwendbar zu sein. Diese bilden gemeinsam mit häufig verwendeten Kernbegriffen eine einheitliche Terminologie des ISRM. Die Terminologie liefert damit die Grundlage für die domainspezifische Zusammenarbeit innerhalb einer strategischen Partnerschaft.

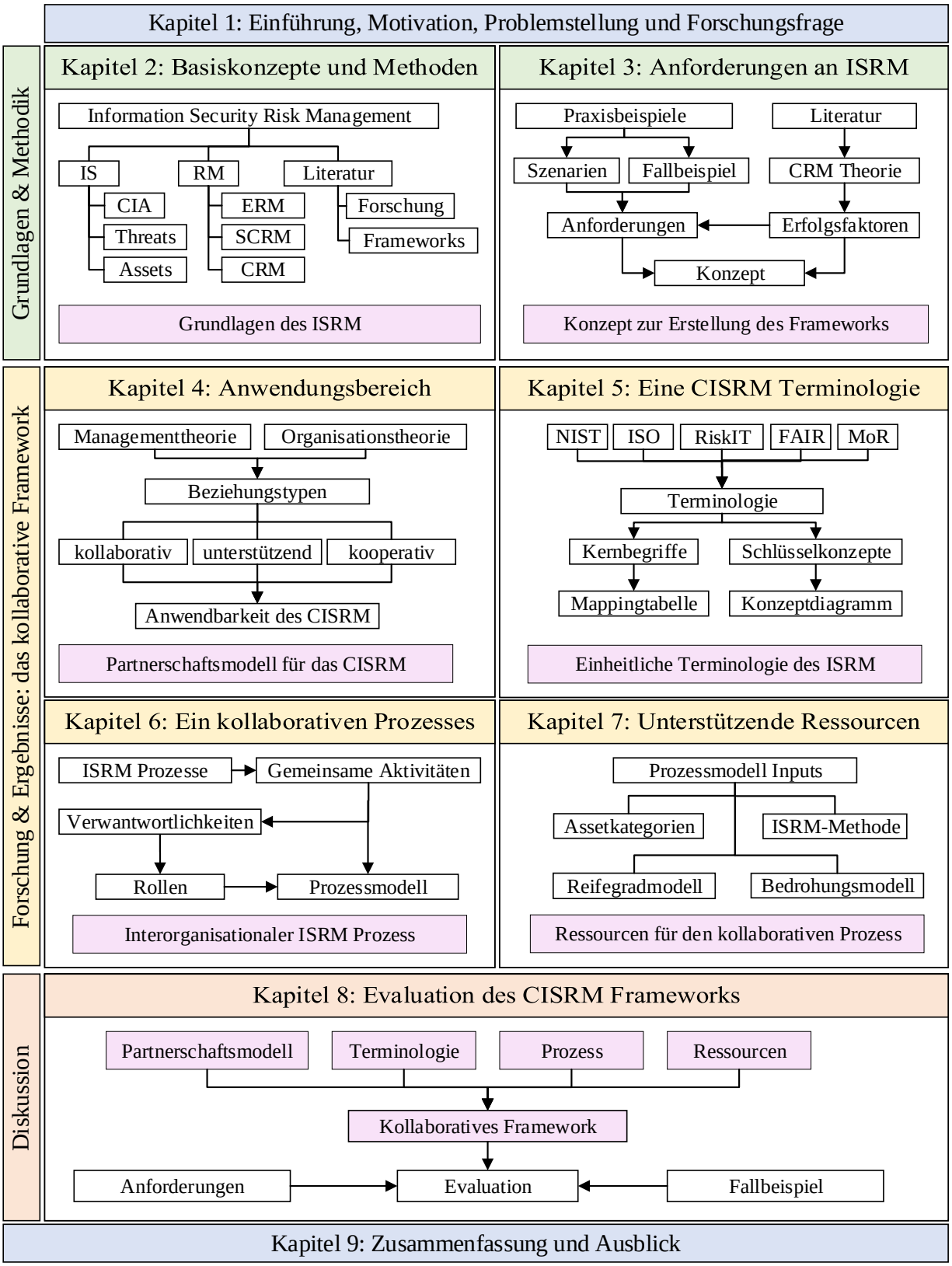
Kapitel 6 In Kapitel 6 werden die ISRM-Frameworks erneut untersucht, allerdings diesmal mit Hinblick auf die definierten Prozesse. Die verschiedenen Prozessmodelle werden miteinander verglichen, um ein generisches Prozessmodell abzuleiten. Anschließend wird untersucht, welche Aktivitäten dieses Prozesses gemeinsam durchgeführt werden können. Durch Hinzufügen von Verantwortlichkeiten für die gemeinsamen Aktivitäten ergibt sich letztlich ein kollaborativer ISRM Prozess.

Kapitel 7 Auf den vorherigen Erkenntnissen aufbauend werden in Kapitel 7 ergänzende Ressourcen definiert, welche für einen kollaborativen Prozess notwendig sind. Dazu gehören vergleichbare Assetkategorien der Partner, ein Bedrohungsmodell für die Allianz, ein Schema eines Reifegradmodells zur Auswahl der Partner und eine gemeinsame ISRM Methode.

Kapitel 8 Die Anwendung des erstellten Rahmenwerks wird in Kapitel 8 beschrieben. Es wird der Aufbau eines kollaborativen ISRM im Kontext der in Kapitel 3 vorgestellten Beziehungstypen anhand eines Beispiels skizziert. Dabei wird das Vorgehen anhand des kollaborativen Prozesses erklärt.

Kapitel 9 Letztlich wird die Arbeit in Kapitel 9 zusammengefasst. Dabei wird das erstellte Konzept für interorganisationales ISRM diskutiert und anschließend auf dessen Limitierungen eingegangen. Abschließend wird ein Ausblick auf Möglichkeiten zur praktischen Anwendung sowie zur weiteren Forschung geliefert.

Abbildung 1.1: Vorgehensmodell und Ergebnisse



Kapitel 2

Basiskonzepte und Methoden

Inhaltsangabe

Das RM als Managementdisziplin ist ein sehr diverser und heterogener Bereich. Ausgehend von einer generellen Idee was ein Risiko ist und wie damit umgegangen werden sollte, existieren viele verschiedene Ansätze. Diese unterscheiden sich bereits bei der Frage, aus welchen Teilen ein Risiko besteht und wie es bewertet werden kann. Trotzdem hat sich ein allgemeines Verständnis in Theorie und Praxis etabliert, welches einen grundlegenden Ansatz beschreibt. Gleiches gilt für das ISRM als Kombination des allgemeinen RM und der IS. Dabei wurde das RM um die aus der IS bekannten Schutzziele und sicherheitsspezifischen Ansätze erweitert. Durch diese Eingrenzung scheint das ISRM einheitlicher beschaffen zu sein, jedoch unterscheiden sich auch hier die genauen Zusammenhänge.

Theorie und Praxis

Nicht alle existierenden Ansätze und Konzepte sind notwendig, um einen funktionierenden ISRM Prozess zu etablieren. In der Praxis hat sich gezeigt, dass Organisationen oftmals nur einzelne Elemente etablieren und sich ihren eigenen Prozess nach Bedarf zusammenbauen. Trotzdem sind die grundlegenden Ideen immer die gleichen, welche in verschiedenen Ausprägungen Eingang in alle Risikoprozesse finden. Nichtsdestotrotz sind die theoretischen Grundlagen essenziell, um in der Forschung neue Vorgehensweisen zu entwickeln.

Einführung RM

Um einen grundsätzlichen Überblick zu schaffen, werden in diesem Kapitel die wichtigsten Begriffe und Konzepte des ISRM erklärt (Abschnitt 2.1). Es werden die Ideen vorgestellt, welche dem ISRM zugrunde liegen und die aktuell gängigen Verfahren zur Berechnung der relevanten Werte skizziert. Dabei werden die am weitesten verbreiteten Definitionen aus der Literatur herangezogen und nur am Rande auf Sonderfälle eingegangen. Am Ende soll ein klares Verständnis über Risiken, sowie deren Zusammenhang mit Assets, Schwachstellen, Bedrohungen und Maßnahmen vorherrschen.

Arten des RM

Anschließend werden die verschiedenen Arten des RM vorgestellt, die für die Arbeit relevant sind (Abschnitt 2.2). Das RM als übergeordnete Disziplin hat heute sehr viele verschiedene Ausprägungen, die bestimmte Unterkategorien definieren. Obwohl die grundlegenden Konzepte im RM vererbt werden, so haben diese verschiedenen Prozesse jeweils einen unterschiedlichen Schwerpunkt auf bestimmte Aspekte. Dazu gehört neben dem Fokus auf IS etwa die Integration der Risiken des gesamten Unternehmens oder die Risikobetrachtung von Lieferanten.

ISRM Frameworks

Letztlich werden aktuelle Ansätze zum ISRM vorgestellt, welche heute in Organisationen zum Einsatz kommen (Abschnitt 2.3). Standardisierungsorganisationen und Industrieverbände stellen schon lange Rahmenwerke (Frameworks) bereit, um einen ISRM Prozess zu implementieren. Diese sind jeweils auf die Bedürfnisse einer Zielgruppe zugeschnitten, wodurch sich Branchenspezifisch leichte Unterschiede ergeben. Inhalt und Struktur der am weitesten verbreiteten Frameworks werden dabei kurz beschrieben und deren ISRM Vorgehensweise illustriert.

Bewertung des ISRM

Abschließend wird der aktuelle Stand des ISRM im Hinblick auf eine potenzielle interorganisationale Zusammenarbeit bewertet (Abschnitt 2.4). Dies liefert den Ausgangspunkt für die weitere Analyse des Themas im nächsten Kapitel.

2.1 Der Risikobegriff in der Informationssicherheit

Ziele und Risiken

Der Zweck einer jeden Organisation lässt sich durch die Definition einer unternehmerischen Vision und davon abgeleiteten Missionen abbilden. Um diese Missionen zu erfüllen, werden vom Topmanagement strategische Ziele definiert. Von diesen lassen sich wiederum taktische und operative Ziele ableiten, die auf verschiedenen Ebenen der Organisation umzusetzen sind und unterschiedliche Disziplinen betreffen können. Ein *Risiko* beschreibt ganz generell einen Umstand, der dazu führt, dass eines dieser Ziele beeinflusst wird. Im Gegensatz zum normalen Sprachgebrauch, in dem der Begriff *Risiko* eher negativ konnotiert ist, kann ein Risiko in dieser Definition die Zielerreichung sowohl negativ als auch positiv beeinflussen (Abbildung 2.1). Dabei wird ein Risiko mit positiver Auswirkung (auf die Zielerreichung) oftmals als *Chance* bezeichnet. [46]

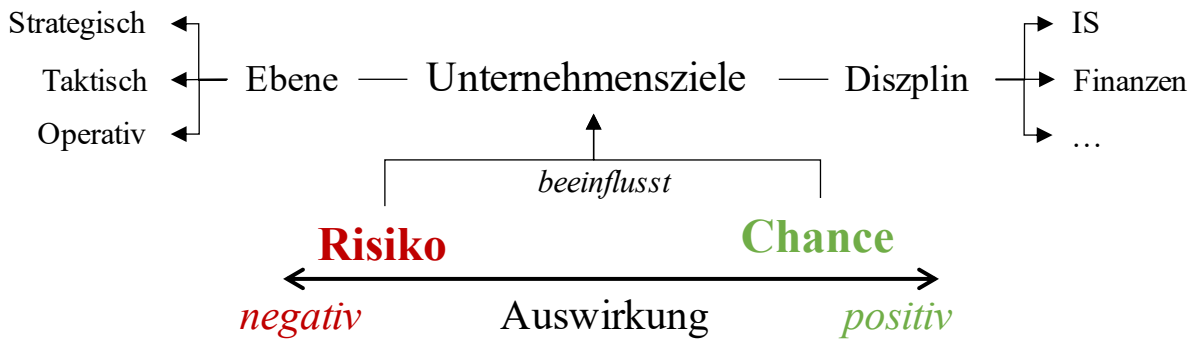
Typen

Traditionell hat sich das RM nur mit den negativen Risiken befasst, den sogenannten *echten Risiken* (pure risk). Echte Risiken bieten nur zwei Optionen: Entweder führen Sie zu einem Verlust bzw. einer negativen Auswirkung oder nicht. Das bedeutet, wenn das Risiko nicht eintritt, dann verbessert sich die Ausgangssituation damit nicht. Ein klassisches Beispiel wäre etwa die Gefahr durch Feuer für ein Gebäude. Brennt das Gebäude ab, dann können die negativen Auswirkungen für den Besitzer sehr hoch sein. Tritt dagegen kein Brand auf, dann hat der Besitzer zwar keinen Nachteil, aber auch keinen Vorteil. Im Gegensatz dazu gibt es *spekulative Risiken* (speculative risk), welche die Option eines Gewinns bieten. Investiert ein Service Provider etwa in einen neuen Service, dann besteht auch hier die Möglichkeit, dass der Service am Markt nicht erfolgreich ist. In diesem Fall tritt wie beim echten Risiko ein Verlust ein. Allerdings, besteht auch die Möglichkeit, dass der Service die gesetzten Ziele erreicht oder sogar übertrifft. Dies führt dann zu einem positiven Effekt für den Service Provider, etwa finanziellem Gewinn oder einer neuen Kundengruppe. [47]

Risiken und IS

Die IS definiert sich über die Aufrechterhaltung von Schutzzielen bzw. Grundwerten durch die Etablierung eines Sicherheitsprozesses, der geeignet ist, diese vor Sicherheitsereignissen zu schützen [48]. Insbesondere die drei Schutzziele Confidentiality, Integrity, Availability (CIA), spielen eine zentrale Rolle bei allen Elementen der IS [49]. Sie sind die Grundlage für die Bewertung von Sicherheitsmaßnahmen und notwendig für die Entscheidungsprozesse. Oftmals werden auch die zusätzlichen Ziele der Authentizität, Nicht-Abstreitbarkeit und Zurechenbarkeit verwendet, jedoch spielen diese eher eine untergeordnete Rolle. Das ISRM kombiniert nun diese Ziele der IS mit dem Konzept des *Risikos* aus dem klassischen RM. Dabei ersetzen die spezifischen IS-Ziele die üblichen Unternehmensziele. Es ist zu bedenken, dass sich auch die Ziele der IS letztlich in die Zielkaskade einfügen lassen, da sie nur eine Spezifizierung der operativen Ziele darstellen. Somit lässt sich auch das ISRM als Teilbereich in das RM eingliedern, vergleichbar mit anderen Spezialisierungen wie etwa Umwelt- oder Qualitätsrisiken, welche ebenfalls auf einer Anpassung der Ziele basieren. Daneben existieren jedoch weitere Unterschiede zum allgemeinen RM. So arbeitet das ISRM nicht mit spekulativen, sondern nur mit echten Risiken. Das Konzept der *Chancen* wird nicht aufgegriffen, da in der IS die Zielerreichung nicht positiv beeinflusst werden kann. Die Schutzziele stellen einen Zustand dar, der erhalten werden soll. Sie können zwar durch negative Effekte verletzt (Verlust der CIA), jedoch nicht zusätzlich verbessert werden.

Abbildung 2.1: Unterscheidung zwischen Risiken und Chancen



So ist etwa ein Verlust der CIA durch ein Risiko vorstellbar, ein Übertreffen der CIA durch eine Chance jedoch nicht. Weiterhin sind zur Beschreibung eines Risikos im ISRM üblicherweise die Begriffe *Asset*, *Schwachstelle* und *Bedrohung* notwendig. Die International Organization for Standardization (ISO) [1] gilt als international anerkannte Autorität in Bezug auf Standarddokumente. Daher beginnen die folgenden Beschreibungen jeweils mit den Definitionen aus den zugehörigen ISO Standards und erklären dann sukzessive die Konzepte des ISRM.

2.1.1 Asset

Definition

Ein Asset ist ein „item, thing or entity that has potential or actual value to an organization“ [50]. Es lässt sich damit als generell Vermögenswert bzw. im Kontext der IS besser als Unternehmenswert übersetzen. Im Gegensatz zu rein wirtschaftlichen Vermögenswerten, kann ein IS Asset auch immaterielle Werte darstellen, die keinen direkten finanziellen Wert besitzen. Zu den materiellen Werten gehört alles, was die Organisation besitzt oder nutzt, etwa Produkte, Hardware oder Gebäude. Im Gegensatz dazu sind immaterielle Werte zwar für die Organisation von Bedeutung, besitzen aber keinen direkten monetären Gegenwert, etwa Wissen oder Reputation. Im Kontext der IS wird dabei auch oftmals von *Information Assets* gesprochen [49]. Auch das zeigt, dass Informationen als Unternehmenswert angesehen werden können. Die Schutzziele der IS zielen spezifisch auf den Schutz von Informationen ab und stellen den Erhalt der CIA sicher.

Assets im ISRM

Das IS Asset kann als zentrales Element des ISRM angesehen werden. Der gesamte Prozess ist auf die Bewertung und den Schutz der Assets, bzw. der CIA des Assets, ausgerichtet. Davon sind ein Großteil der IS Assets immaterielle Werte und lediglich einer kleiner Teil sind materielle Werte. Dabei sind letztere deutlich einfacher zu identifizieren und zu bewerten, da ihr Einfluss auf Geschäftsprozesse und Services oftmals direkt sichtbar ist. Die Auswirkung von immateriellen Informationswerte auf die Geschäftsergebnisse und den Erfolg der Organisation sind dagegen schwer zu ermitteln. Es existieren dabei zwei Perspektiven,

[1] `https://www.iso.org`

die den Wert eines Assets beeinflussen: direkter und indirekter Einfluss auf die Geschäftsergebnisse. Zum einen können Informationen selbst von Geschäftsprozessen oder Services genutzt werden, das heißt sie liefern selbst einen Mehrwert. Zum anderen können sie andere Aktivitäten indirekt beeinflussen, indem sie die Erstellung neuer Werte, anderer Produkte oder zusätzlichen Wissens beitragen, welche dann wiederum einen Mehrwert generieren. Diesen festzulegen gestaltet sich gerade mit Bezug auf immaterielle, indirekte Assets als schwierig. [51]

Business Impact Analyse

Somit haben nicht alle Assets den gleichen Wert bzw. die gleiche Bedeutung für eine Organisation, sondern manche Assets sind wichtiger als Andere. Die Wichtigkeit eines Assets im Kontext der Organisation wird häufig als *Kritikalität* bezeichnet. Sie ist ein Maß für die potenzielle Auswirkung des Verlustes eines Schutzziels des Assets auf die Organisation. Teilweise werden auch die Begriffe *Schutzbedarf* [52] oder *Sicherheitskategorie* [53] synonym verwendet, obwohl deren Anwendung tatsächlich nicht einheitlich ist und diese kontextabhängig ein abgewandeltes Konzept beschreiben. Das Vorgehen zur Einstufung der Kritikalität wird üblicherweise als Business Impact Analysis (BIA) bezeichnet, ein Begriff aus dem Bereich Business Continuity [54]. Dabei wird die Auswirkung des Verlusts eines Schutzziels auf die Organisation untersucht. Eine in Standards üblicherweise verwendete Methode ist die quantitative Klassifikation der Kritikalität, z.B. in *Niedrig*, *Mittel* und *Hoch*, basierend auf der Einstufung der zugehörigen Schutzziele (standardmäßig CIA) [55]. Zur Berechnung der gesamten Kritikalität des Assets wird meist das Maximum der Werte der verwendeten Schutzziele verwendet (Maximumprinzip). Allerdings existiert dazu keine harte Anforderung, eine Abwandlung basierend auf den spezifischen Bedürfnissen der Organisation ist daher denkbar und legitim. Im Standardfall lässt sich der *Business-Impact* jedoch folgendermaßen definieren:

$$\textbf{Kritikalität} = \textbf{max}(\textbf{Schutzziel}_1, \textbf{Schutzziel}_2, \ldots \textbf{Schutzziel}_n)$$

Zur Einstufung der einzelnen Schutzziele dienen von der Organisation selbst festgelegte Kriterien. Dazu muss sich die Organisation zuerst die für sie relevante Szenarien überlegen, welche die Geschäftsergebnisse gefährden könnten. Vom BSI [56] vorgeschlagene und häufig verwendete oder abgewandelte Beispiele für potenzielle Schadensszenarien sind etwa:

- Verstoß gegen Gesetze/Vorschriften/Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Innen- oder Außenwirkung

Für jedes Szenario lässt sich definieren, wie der Verlust eines Schutzziels auf einer Skala von geringen bis existenzbedrohenden Auswirkungen einzuordnen wäre. Dieses Vorgehen lässt sich für jedes definierte Schutzziel wiederholen und liefert so eine strukturierte Entscheidungstabelle für eine nachvollziehbare Bewertung der Kritikalität. Die bewerteten Assets bilden sowohl die Grundlage für das ISM als auch das weitere Vorgehen im ISRM.

2.1.2 Schwachstelle

Definition

Eine Schwachstelle ist eine „weakness of an asset or control that can be exploited by one or more threats“ [49]. Sie bezieht sich immer auf ein Asset, welches einen Fehler oder eine Schwäche aufweist. Gerade im Bereich Systemanalyse wird analog auch der Begriff *System* verwendet, welcher sowohl technisch (Softwaresystem, Infrastruktur) als auch organisatorisch (Organisationseinheit) interpretiert werden. Die Schwachstelle stellt damit das formale Bindeglied zwischen Assets und Bedrohungen im ISRM dar:

Schwachstelle ≡ Asset + ausnutzbare Schwäche

Verwundbarkeit

Eine Schwachstelle ist eine dem Objekt oder System innewohnende Eigenschaft, die dazu führt, dass es negativ beeinflusst werden kann. Sie ist die inhärente Manifestation eines Zustands, der von natürlichen Gefahren betroffen oder gezielt ausgenutzt werden kann. Solche grundsätzlich schädlichen Ereignisse werden allgemein als *Bedrohung* bezeichnet, welche im nächsten Abschnitt noch genauer erläutert werden. Ein System, das mindestens eine Schwachstelle aufweist, wird als *verwundbar* (vulnerable) bezeichnet. Dabei gibt es zwei mögliche Herangehensweisen: die Auffassung der Verwundbarkeit als Zustand oder als Wahrscheinlichkeit. Bei ersterem wird die Verwundbarkeit eines Systems als absoluter Status angesehen, d.h. ein System ist entweder verwundbar oder nicht. Die tatsächlichen Konsequenzen eines Ereignisses auf das System spielen dabei keine Rolle. Letzteres betrachtet die Verwundbarkeit als Unsicherheitsfaktor, welcher die Möglichkeit negativer Konsequenzen nach einem Ereignis beschreibt. Diese müssen jedoch auch bei Eintreten des Ereignisses nicht automatisch auftreten und auch die Schwere der Konsequenzen ist nicht abzusehen. Das Gegenstück zur Verwundbarkeit eines Systems wird *Widerstandsfähigkeit* (resilience) genannt. Die Widerstandsfähigkeit bezeichnet die Fähigkeit eines Systems einer Disruption standzuhalten, nachdem eine Schwachstelle ausgenutzt wurde. Dabei werden zwei verschiedene Aspekte berücksichtigt. Auf der einen Seite ist ein System widerstandsfähig, wenn es das Ausnutzen der Schwachstelle ohne wesentliche Störung aushalten kann. Auf der anderen Seite ist ein System auch dann widerstandsfähig, wenn es zwar eine große Störung erleidet, aber innerhalb akzeptabler Zeit und mit angemessenen Kosten wiederhergestellt werden kann, also in den Normalzustand zurückkehrt. [57, 58]

Tech. Schwachstelle

Im Bereich der IT-Security geht es im Speziellen um technischen Schwachstellen eines Softwaresystems, welche allerdings nur einen kleinen Teil im ISRM darstellen. Insbesondere viele traditionelle Frameworks nutzen zur Risikoanalyse eine Liste technischer Schwachstellen und verweisen auf die Nutzung von Schwachstellen Scannern [59]. In diesem Bereich haben sich Bewertungssysteme zur Einstufung der Kritikalität einer Schwachstelle etabliert. Ein bekanntes Framework ist das Common Vulnerability Scoring System (CVSS) [60], welches eine Metrik zur qualitativen Bewertung bietet. Dabei werden grundlegende Eigenschaften einer Schwachstelle abgefragt und auf einen numerischen Wert abgebildet. Je höher der Wert, desto schwerwiegender die Schwachstelle. Dieser Wert lässt sich dann wiederum auf eine qualitative Bewertungsskala abbilden, analog zu der BIA bei den Assets. Hier zeigt sich nun jedoch eine Lücke zwischen dem ISRM als organisatorische Managementfunktion und dem Umgang mit technischen Schwachstellen. Obwohl technische Schwachstellen im

Kontext des Schwachstellenmanagements bewertet werden, lässt sich aus deren Kritikalität nicht direkt ein Einfluss auf die Geschäftsziele ableiten. [61]

Org. Schwachstelle

An dieser Stelle hilft die Abbildung auf die vorher genannten organisatorische Assets weiter. Softwaresysteme können selbst Assets sein oder sind Teil eines Assets. Die bewerteten Assets repräsentieren direkt die Auswirkung auf die Geschäftsergebnisse und Ziele Organisation bei Verlust der Schutzziele. Eine kritische Schwachstelle eines Softwaresystems kann also trotzdem nur einen geringen Schweregrad haben, wenn das zugehörige Asset nur geringe Bedeutung für die Organisation besitzt. Durch diese Unterscheidung und die Verknüpfung mit Assets wird es vom reinen IT-Risiko zum IS-Risiko. Voraussetzung dafür ist, dass eine Schwachstelle zuerst durch eine Bedrohung ausgenutzt wird.

2.1.3 Bedrohung

Definition

Eine Bedrohung ist eine „potential cause of an unwanted incident, which can result in harm to a system or organization“ [49]. Die Bedrohung ist oftmals eng mit den Begriffen *Ereignis* und *Angriff* verknüpft. Ereignisse sind generisch und umfassen sowohl gesteuerte als auch ungesteuerte Phänomene, z.B. Naturkatastrophen. Wie auch Risiken können Ereignisse selbst sowohl positiv als auch negativ sein. So könnten etwa fallende Energiepreise am Markt ein positives Ereignis sein, da so die IT-Infrastruktur und damit die Services der Organisation günstiger betrieben werden können. Im Gegensatz dazu sind die potenziellen Konsequenzen einer Bedrohung immer negativ, d.h. Bedrohungen sind die Teilmenge der negativen Ereignisse. Ein Angriff ist eine Spezialform einer Bedrohung, die durch einen menschlichen Akteur absichtlich begangen wird. Damit ergibt sich die Bedrohung aus

$$\textbf{Bedrohung} \equiv \textbf{Ereignis} + \textbf{negativer Effekt}$$

Gefahrenquellen

Als Gefahrenquelle (threat agent) wird der Auslöser einer Bedrohung bezeichnet [62]. Diese Auslöser lassen sich grundlegend in menschliche, umgebungsbezogene und technologische Gefahrenquellen einteilen [63]. Zu jeder Bedrohung muss immer eine Gefahrenquelle existieren, unabhängig von deren Art. Bei einer technischen Bedrohung wie einer Malware oder einer nicht-technischen Bedrohung wie Diebstahl ist die Gefahrenquelle etwa jeweils ein menschlicher Angreifer, welcher der Organisation Schaden zufügen will. Obwohl ersteres eine technische Bedrohung darstellt, ist der Auslöser für diese letztlich ein Mensch, der eine technische Schwachstelle angreift. Eine technologische Gefahrenquelle wären etwa die Server der Organisation selbst, welche eine Fehlfunktion verursachen könnten. Auch umgebungsbezogene Bedrohungen wie eine Flutwelle oder ein Vulkanausbruch haben eine Gefahrenquelle, nämlich die Umwelt. Die Analyse verschiedener Gefahrenquellen kann dabei helfen, verschiedene Arten von Bedrohungen zu identifizieren, welche die Assets der Organisation gefährden.

Bedrohungen klassifizieren

Bedrohungen lassen sich in verschiedene Kategorien einordnen, wobei die Aufteilung von der gewählten Perspektive abhängt. Die Klassifikation von Bedrohungen ist eine Voraussetzung für die sogenannte *Bedrohungsmodellierung* (threat modelling), eine Aktivität bei der die für eine Organisation relevanten Bedrohungen identifiziert werden sollen. Eine übliche Trennung ist die Unterscheidung zwischen internen und externen Bedrohungen [63,

64]. Diese bezieht sich dabei nicht auf die Bedrohung selbst, sondern auf die Lokation der Gefahrenquelle in Bezug zur Organisation. So könnte etwa Malware von einem externen Hacker eingeschleust oder von einem unachtsamen Mitarbeiter aus dem Internet geladen werden. Hier zeigt sich bereits eine mögliche weitere Dimension in der Klassifizierung, die Unterscheidung in absichtlich und unabsichtlich erzeugte Bedrohungen [63]. Während die Intention des Hackers ein absichtlicher Angriff auf die Organisation ist, so möchte der Mitarbeiter der Organisation eigentlich nicht schaden, sondern sein Verhalten führt „aus Versehen“ zu negativen Konsequenzen.

Bedrohungskataloge

Im Gegensatz zu Schwachstellen, die sich auf ein bestimmtes Asset beziehen oder Risiken, die spezifisch für eine Organisation sein können, sind Bedrohungen generisch. Egal, ob die Gefahrenquelle technologisch, menschlich oder umweltbezogen ist, die entstehenden Bedrohungen stellen grundsätzlich eine Gefahr für Assets jeder Organisation dar. Da es nur eine endliche Menge an Bedrohungen gibt, werden von nationalen und internationalen Organisationen Listen mit Bedrohungen erstellt, die von anderen genutzt werden können. Beispiele dafür sind etwa die in Deutschland bekannten Gefährdungskataloge im *IT-Grundschutz-Kompendium* [52] oder auf europäischer Ebene die *Threat Taxonomy* [65]. Insbesondere für technische Bedrohungen stellt das *MITRE ATT&CK* [66] Framework eine stetig wachsende Wissensdatenbank bereit. Diese Kataloge liefern Organisationen eine Grundlage für die Bedrohungsmodellierung, um aus den vorhandenen generischen Bedrohungen die für ihre Assets relevanten zu identifizieren. Die anwendbaren Bedrohungen können dann die Grundlage für die Analyse von organisationsspezifischen Risiken dienen.

2.1.4 Risiko

Definition

In der klassischen RM Definition bezeichnet ein *Risiko* den „effect of uncertainty on objectives“ [67]. Ein Risiko bezeichnet grundsätzlich eine Abweichung vom Normalzustand, welche das erwartete Ergebnis positiv oder negativ beeinflusst. Basierend auf der allgemeinen RM Definition der Unsicherheit der Zielerreichung, kann diese auch für das ISRM adaptiert werden: „In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives“ [49]. Insbesondere in den Definitionen der ISO spielt das Konzept der Unsicherheit bei Risiken eine zentrale Rolle. Obwohl zumindest der Begriff *uncertainty* in der Literatur häufig verwendet wird und das Konzept in wissenschaftlichen Veröffentlichungen schon oft diskutiert wurde, existiert bislang kein allgemeiner Konsens über das Zusammenspiel von Risiken, Wahrscheinlichkeiten und Unsicherheit [68]. Dabei kann sich die Unsicherheit auf alle Aspekte eines Risikos beziehen. Unsicherheit bedeutet, dass es sowohl unklar ist, ob ein Ereignis eintritt oder nicht, als auch, was die Konsequenzen sein könnten [69]. Bereits Aven und Renn [70] haben ein großes Problem mit auf Unsicherheit basierenden Risikodefinitionen aufgezeigt. So führen die üblichen Definitionen über einen unsicheren Ausgang des Ereignisses oder dessen unsicheren Konsequenzen zu konzeptuellen Schwierigkeiten und sind nicht mit den üblichen Anwendungen im RM kompatibel. Sie schlagen daher vor, ein Risiko als Unsicherheit über den Schweregrad der Konsequenzen einer Aktivität auf einen Wert zu betrachten. In der Systemanalyse sagt Haimes [57] etwa, dass ein Risiko eine

Funktion mit 5 Komponenten ist:

- Zeit
- Die Wahrscheinlichkeit der Bedrohung bzw. des Ereignisses
- Die Wahrscheinlichkeit der Konsequenzen
- Dem Statusvektor des Systems (Performanz, Anfälligkeit und Widerstandsfähigkeit)
- Dem Vektor der sich ergebenden Konsequenzen

Diese Definition ist konzeptuell viel leichter verständlich und passt auch zum heute üblichen Vorgehen in der Praxis, dass sich eher an einschätzbaren Wahrscheinlichkeiten als an Unsicherheit orientiert.

IS Risiken

Ein Informationssicherheitsrisiko im Speziellen bezeichnet ein Risiko mit Einfluss auf Informationen, meist in Form von Daten, einer Organisation. Das Sicherheitsrisiko ist das zentrale Element im ISRM, da alle vorangegangenen Definitionen und Aktivitäten darauf ausgerichtet sind, dieses am Ende beschreiben und bewerten zu können [62]. Generell lässt sich das potenzielle Ausmaß eines einzelnen Risikos, genannt *Risikohöhe* oder Level of Risk (LoR), aus den Größen *Eintrittswahrscheinlichkeit* und *Auswirkung* (oftmals auch Schaden oder Konsequenzen) ermitteln [49]. Die Auffassung, dass sich ein IS-Risiko tatsächlich über diese beiden Werte definiert, ist weit verbreitet [58, 61]. Nach dieser einfachen Definition ergibt sich ein Risiko aus der Kombination der Werte für Eintrittswahrscheinlichkeit und Auswirkung:

Risikohöhe = Eintrittswahrscheinlichkeit * Auswirkung

Dabei lassen sich die beiden Eingangswerte direkt von den Bestandteilen eines Risikos ableiten. Die Eintrittswahrscheinlichkeit des Risikos basiert auf der Wahrscheinlichkeit einer sich erfolgreich manifestierenden Bedrohung. Dies setzt voraus, dass (1) die Bedrohung auftritt, (2) die Bedrohung eine Schwachstelle ausnutzen kann und (3) diese Ausnutzung tatsächlich zu einem Schaden führt. Die Auswirkung wiederum bezieht sich auf die Konsequenzen der Bedrohung, d.h. Einfluss auf die Geschäftsergebnisse bzw. IS-Ziele. Durch den in der BIA eingeschätzten Wert des Assets für die Organisation lässt sich direkt der maximale Schaden für die Organisation bei Verlust eines Schutzziels ableiten.

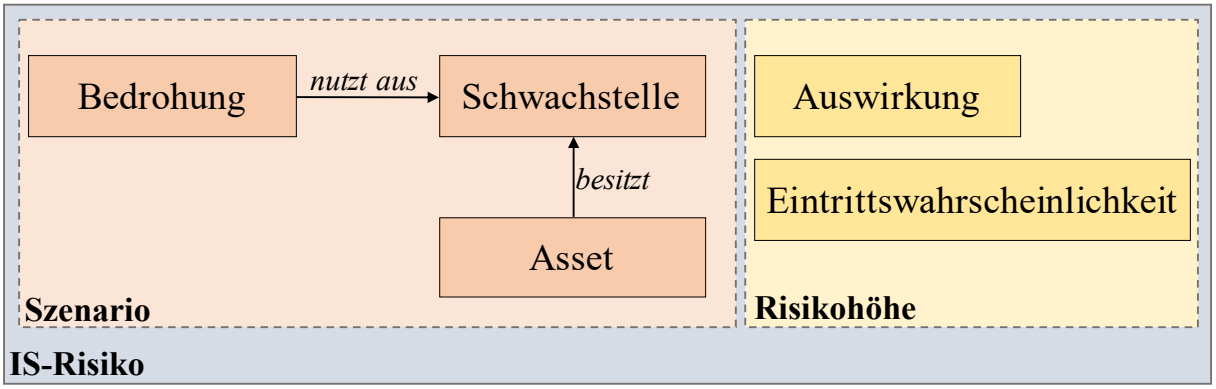
Szenario

Dabei werden oftmals auch die Begriffe *Szenario* oder *Risikoszenario* genutzt. Ein Szenario ist also eine Kombination von Bedrohungen und Schwachstellen, wobei eine Schwachstelle von mehr als einer Bedrohung ausgenutzt werden und eine Bedrohung mehrere Schwachstellen nutzen kann (n:n Beziehung):

Szenario ≡ Bedrohung x Schwachstelle

Die Verwendung der Begriffe *Szenario* oder *Risikohöhe* bzw. deren Teilaspekte im Zusammenhang mit Risiken ist in Theorie und Praxis nicht immer eindeutig. Oftmals wird vollständig auf einzelne Begriffe verzichtet und stattdessen nur von einem *Risiko* gesprochen. Letztlich ändert das allerdings nichts an der grundlegenden Zusammensetzung eines Risikos, weshalb die oben genannte Definition für das weitere Vorgehen vollkommen ausreichend ist. Durch Zusammenfassen der Bausteine eines Risikos mit dessen Eigenschaften

Abbildung 2.2: Grundlegende Zusammensetzung eines IS-Risikos



lässt sich ein Risiko wie in Abbildung 2.2 darstellen. Dabei ist die logische Trennung zwischen Szenario und Risikohöhe zu beachten. Obwohl die beiden Konzepte aufeinander aufbauen, die Auswirkung leitet sich direkt vom Asset und Eintrittswahrscheinlichkeit von der Bedrohung ab, so existiert diese zusätzlich Dimension erst ab der Bewertung des Risikos.

Bewertung

Zur Bewertung von IS Risiken existieren dabei drei grundlegende Methoden: (1) quantitativ, mit Hilfe numerischer Werte; (2) qualitativ, eine beschreibende Zuordnung zu einem Bereich; (3) hybrid, eine Kombination von qualitativ und quantitativ. Die quantitative Bewertung beschreibt ein objektives Vorgehen basierend auf messbaren Kriterien. Die zwei bekanntesten Methoden sind Annual Loss Exposure (ALE) [71] und Livermore Risk Analysis Methodology (LRAM) [72]. Es gibt jedoch zwei große Probleme bei der quantitativen Bewertung. So ist das Vorgehen rechenintensiv und damit sehr zeitaufwändig, weshalb wiederum viele Ressourcen (Zeit, Geld, Personen) von der Organisation investiert werden müssen. Die Ergebnisse der Berechnung sollten den Wert des Assets für die Organisation in einer sinnvollen, management-spezifischen Sprache darstellen, jedoch gestaltet sich die Abbildung auf etwa einen monetären Wert als sehr herausfordernd. Weiterhin basiert das Vorgehen auf einer ausreichend großen und belastbaren Datenbasis, welche nicht zur Verfügung stehen. Erfahrungswerte von anderen Organisationen oder historische Daten sind gerade im Bereich IS meist nicht vorhanden, da Daten zur Risikobewertung so gut wie nie von Organisationen veröffentlicht werden. Aus diesem Grund wird die quantitative Methode im ISRM nur sehr selten verwendet. Die große Mehrheit an Frameworks und Industriestandards nutzt qualitative Methoden, weshalb dieses auch bei Organisationen am weitesten verbreitet ist. Bei der qualitativen Bewertung wird versucht, Risiken mit nicht-numerischen Werten einzuschätzen. Dazu können die Eingangswerte Eintrittswahrscheinlichkeit und Auswirkung in einer Risikomatrix dargestellt werden. Jeder Wert bildet eine Dimension der Matrix, üblicherweise auf einer Skala von 3 bis 5, wodurch sich die qualitative Bewertung ergibt. Eine Alternative stellt die linguistische Einstufung dar, bei welcher gewichtete Kriterien selektiert werden müssen. Dies ist insbesondere hilfreich, wenn die Ausgangssituation viele Unsicherheiten aufweist und eine direkte Zuordnung auf der Skala sich als schwierig erweist. Egal welche der beiden Einstufungsmethoden gewählt

wird, ist die qualitative Methode deutlich einfacher zu verstehen und durchzuführen als die quantitative. Ein Problem dieses Vorgehens ist jedoch, dass es vollständig auf der Erfahrung der an der Bewertung beteiligten Personen basiert. Damit ist sie im Gegensatz zur quantitativen Methode grundsätzlich fehleranfälliger und subjektiver. Weiterhin stehen nur wenige qualitative Werte zur Einstufung zur Verfügung, d.h. Eintrittswahrscheinlichkeit, Auswirkung und Risikohöhe werden auf einen relativ kleinen Wertebereich abgebildet. Diese Schwächen sind allerdings in der Praxis oftmals vernachlässigbar und die Genauigkeit der Ergebnisse für die meisten Organisationen ausreichend. Letztlich besteht natürlich auch die Möglichkeit, beide Methoden zu einem hybriden Vorgehen zu kombinieren, wenn es im spezifischen Anwendungsfall sinnvoll erscheint. [73, 74]

Risk Information Sharing

Anders als etwa Risiken im Gesundheitsbereich lassen sich die Wahrscheinlichkeiten und Auswirkungen von Informationssicherheitsrisiken nicht auf einer rein statistischen Basis vorhersagen. Zum einen ist der Bereich vergleichsweise jung, zum anderen werden eingetretene Risiken aufgrund der Sensibilität und den negativen Auswirkungen auf die betroffenen Organisationen meist geheim gehalten. Soweit keine gesetzliche Meldepflicht besteht oder die Informationen anderweitig an die Öffentlichkeit drängen, stehen keine allgemeinen Daten über Informationssicherheitsrisiken bereit. Der Austausch von Risikoinformationen könnte Organisationen dabei helfen, die eigenen Risiken besser zu verstehen. Dabei ist die Herausforderung, dass sowohl das Sammeln als auch die Weitergabe von Risikoinformationen nicht zur Belastung für die berichtende Organisation werden darf [74]. Weiterhin sind sowohl Eintrittswahrscheinlichkeit sowie Auswirkung stark von der Branche als auch dem individuellen Unternehmen abhängig. Aus diesem Grund ist es üblich, dass die Bewertung von Risiken neben öffentlichen Umfragen und Medienberichten vor allem auf subjektiven Einschätzungen wie den vergangenen Ereignissen der letzten Jahre und Erfahrungen der Mitarbeiter basiert [58]. Dies führt unter anderem dazu, dass eine Risikobewertung nur lokal für eine Organisation und nicht organisationsübergreifend gültig ist. Somit fällt es schwer, allgemeingültige Vorlagen für kritische Risiken zu erstellen oder eingeschätzte Risiken in anderen Organisationen wiederzuverwenden.

Umgang mit Risiken

Bewertete Risiken liefern die Ausgangslage für das weitere Vorgehen, welches einen essenziellen Aspekt im RM darstellt. Grundsätzlich legt eine Organisation selbst fest, welche Risiken sie behandeln möchte und welche nicht. Die Auswahl hängt von verschieden Rahmenbedingungen ab, etwa dem Risikoappetit der Organisation. Im Allgemeinen existieren verschiedene Möglichkeiten, wie eine Organisation mit Risiken umgehen kann. Übliche Mechanismen sind die Übertragung der Verantwortung an eine andere Partei (Liability Transfer), die Absicherung der eigenen Organisation gegen den potenziellen Schaden (Indemnification), die Abschwächung des Risikos (Mitigation) oder das Beibehalten des Risikos ohne weitere Aktionen (Retention) [75]. Daraus lassen sich im ISRM vier Möglichkeiten ableiten, um auf Risiken zu reagieren [73]:

- **Akzeptieren:** Die Organisation versteht das Risiko und seine potenziellen Konsequenzen, entscheidet sich jedoch diese zu akzeptieren, d.h. (vorerst) nichts zu unternehmen.
- **Vermeiden:** Die risikobehaftete Aktivität wird von der Organisation eingestellt, d.h. das Risiko kann nicht mehr eintreten.
- **Transferieren:** Alle oder Teile der risikobehafteten Aktivität werden an eine andere Partei ausgelagert, wodurch die Organisation auch nicht länger die Konsequenzen des Risikos zu tragen hat.
- **Reduzieren:** Das Risiko wird kontrolliert, d.h. die Risikohöhe wird auf einen für die Organisation angemessenen Wert reduziert.

Dabei stellen *Akzeptieren* und *Reduzieren* die in der Praxis am häufigsten verwendeten Optionen dar. Reduzieren bezeichnet letztlich den Versuch, das Auftreten eines Risikos zu verhindern oder dessen Konsequenzen zu limitieren. Zu diesem Zweck wird eine technische oder organisatorische Sicherheitsmaßnahme implementiert, welche das Risiko beeinflusst.

2.1.5 Maßnahme

Definition

Eine Maßnahme bezeichnet ein „measure that is modifying risk“ [49]. Ziel einer Maßnahme ist also grundsätzlich die Modifikation eines existierenden Risikos mit dem Ziel, die Risikohöhe zu reduzieren und dadurch die Assets der Organisation zu schützen [73]. Dabei kann eine Maßnahme ein Risiko auf zwei Arten beeinflussen: durch die Reduzierung der (1) Eintrittswahrscheinlichkeit und/oder der (2) Auswirkung [61, 74]. Bei einer Modifikation des Risikos verändert sich dessen Risikohöhe, welche anschließend als *Restrisiko* bezeichnet wird. Dabei ist es nicht möglich, das Restrisiko auf null zu reduzieren, d.h. bei einer numerischen Darstellung gilt Restrisiko > 0. Ein Risiko lässt sich durch eine Maßnahme niemals vollständig eliminieren, da trotz maximaler Sicherheitsvorkehrungen immer eine minimale Wahrscheinlichkeit des Eintritts besteht und auch eine negative Auswirkung nicht in Gänze ausgeschlossen werden kann. Das Restrisiko wird analog zur Risikohöhe berechnet, nur wird die Schutzwirkung der Maßnahme vorher von der Eintrittswahrscheinlichkeit und/oder der Auswirkung des Risikos subtrahiert:

$$\textbf{Restrisiko} = (\textbf{EW}_{Risiko} \textbf{ - Reduktion}_{Maßnahme}) \textbf{ * } (\textbf{AU}_{Risiko} \textbf{ - Reduktion}_{Maßnahme})$$

Risiko reduzieren

Da die Reduktion der Risikohöhe durch das Reduzieren der Teilwerte erreicht wird, können diese auch unabhängig voneinander durch Maßnahmen beeinflusst werden. Dabei können in beiden Fällen sowohl technische als auch organisatorische Maßnahmen zum Einsatz kommen. Maßnahmen zur Reduktion der Eintrittswahrscheinlichkeit zielen darauf ab, das Auftreten eines Risikos zu verhindern. Dazu kann versucht werden, die Häufigkeit des Szenarios zu reduzieren, indem die Rahmenbedingungen angepasst werden, die zum Eintreffen der Bedrohung führen. Ein vorstellbares Risiko für Organisationen ist etwa, dass unbefugte Personen durch Zutritt zum Bürogebäude an vertrauliche Informationen gelangen. Hier

kann physische Perimeter-Sicherheit helfen, etwa durch Aufbauen von Schließ- und Vereinzelungsanlagen. Die Häufigkeit, dass unbefugte Personen zufällig in das Gebäude gelangen wird reduziert und ein Angreifer müsste den Zutrittsschutz erst überwinden. Gelangt eine unbefugte Person trotz dieser Vorkehrungen in das Gebäude, dann schützt diese Maßnahme nicht länger vor den möglichen Konsequenzen. Daher kann eine weitere Maßnahme etabliert werden, die in diesem Fall den erlittenen Schaden so gering wie möglich hält. Dabei lässt sich das Reduzieren der Auswirkung wiederum auf zwei Arten erreichen. Entweder durch Eingrenzen des Effekts oder durch Verringern der Zeit [74]. Eine *Clean Desk Policy* könnte etwa verhindern, dass vertrauliche Informationen in den Büros offen zugänglich sind. Dadurch erhält ein Angreifer auch nach erfolgreichen Zutritt keinen direkten Zugriff auf herumliegende Dokumente. Regelmäßige Flurkontrollen durch den Sicherheitsdienst könnten hingegen die Zeit verringern, die einem Eindringling zur Verfügung steht, um an vertrauliche Informationen zu gelangen. Meist konzentriert sich das ISM hauptsächlich auf die Reduzierung der Eintrittswahrscheinlichkeit anstatt auf die Auswirkung und dann auch größtenteils auf den Wiederherstellungsaspekt und anstatt der Schadensbegrenzung [74]. Jedoch sind beide Arten der Risikoreduktion notwendig und nur durch eine sinnvolle Kombination davon ist das Erreichen eines minimalen Restrisikos möglich.

Kategorien

Maßnahmen können in drei Kategorien eingeteilt werden: präventiv, detektierend und korrigierend. Präventive Maßnahmen dienen dem Schutz vor einer Bedrohung und werden vorsorglich implementiert, um das Auftreten eines negativen Ereignisses zu verhindern. Die Maßnahme soll also die Eintrittswahrscheinlichkeit des Risikos reduzieren. Beispiele für präventive Maßnahmen sind etwa organisatorische oder technische Zutritts-, Zugangs- und Zugriffskontrollen, welche unbefugte Personen von Anfang an aufhalten sollen. Da ein Risiko jedoch durch Reduzieren nicht vollständig eliminiert werden kann, können detektierende Maßnahmen dazu dienen, das aufgetretene Ereignis zu identifizieren. Durch die schnelle Reaktion auf ein Ereignis kann der verursachte Schaden limitiert werden. Die Maßnahme reduziert also die Auswirkung des Risikos, aber nicht dessen Eintrittswahrscheinlichkeit. Zu diesem Typ gehören etwa alle Formen von Sicherheitsaudits, die geeignet sind, einen Sicherheitsvorfall zu erkennen. Eine weitere Kategorie von Maßnahmen, die deren Auswirkung reduzieren können, sind korrigierende Maßnahmen. Sie sollen nach Auftreten eines Ereignisses den Normalzustand des Systems wiederherstellen. Durch die Erhöhung der Widerstandsfähigkeit kann somit der potenzielle Schaden verringert werden. Ein klassisches Beispiel ist die Durchführung von Datensicherungen, um verlorene oder korrumpierte Daten im Bedarfsfall neu einspielen zu können. Jede Maßnahme kann mindestens einer oder einer Kombination dieser Kategorien zugeordnet werden. Eine optionale, vierte Kategorie stellen die sogenannten Kontrollmaßnahmen dar, welche zur Überprüfung der Effektivität der anderen Kategorien dienen. Ein sinnvoller Mix von Maßnahmen aus verschiedenen Kategorien kann zur bestmöglichen Reduktion der Risikohöhe beitragen. [62, 75]

Kosten-Nutzen

Anders als im ISM, welches die optimale Absicherung der Organisation zum Ziel hat, geht es im ISRM vor allem um die bewusste Abwägung von Vor- und Nachteilen der verschiedenen Optionen zur Risikobehandlung. Das RM im Allgemeinen stellt am Ende auch immer eine Methode zur Ressourcenplanung und Optimierung dar. Im ISRM wird daher versucht, mit den zur Verfügung stehenden Ressourcen die Risiken möglichst effizient zu behandeln,

d.h. die Summe der reduzierten Risikohöhe zu maximieren. Die Entscheidungsträger einer Organisation wollen üblicherweise nur den Wert einer Sicherheitsmaßnahme erkennen, um zwischen den potenziellen Konsequenzen des Risikos und den Kosten der Maßnahme abwägen zu können [76]. Die Bewertung des Ressourceneinsatzes im Verhältnis zur Wirksamkeit der Maßnahme setzt häufig ein quantitatives Vorgehen voraus. Wird der potenzielle Schaden eines Risikos durch einen finanziellen Wert dargestellt, kann auch der Kosten-Nutzen Faktor der Maßnahme durch einen Vergleich mit deren Aufwand einfach ermittelt werden [61]. Im normalen Geschäftsumfeld hat sich zur Bewertung von Investments das Return On Investment (ROI) Modell etabliert. Dieses beschreibt eine einfache Metrik zur Kosten-Nutzen-Rechnung bei Investitionen:

$$ROI = \frac{\text{Erwarteter Gewinn - Kosten der Investition}}{\text{Kosten der Investition}}$$

Security Maßnahmen bewerten

Obwohl die Berechnungsmethode in vielen Branchen sinnvoll ist, so ist sie nicht sonderlich gut für die Anwendung im ISM geeignet. Ein grundsätzliches Problem ist, dass die Metrik versucht, die Kosten und den potenziellen Gewinn einer Investition gegenzurechnen. Im ISM geht es um das Vermeiden von Verlusten für die Organisation, d.h. aus der Implementierung von Sicherheitsmaßnahmen ergibt sich üblicherweise kein Gewinn, sondern eine höhere Schutzwirkung der Assets vor Bedrohungen. Sinnvoller ist es also zu berechnen, wie viel Verlust durch den Einsatz einer Maßnahme potenziell vermieden werden könnte. [77]

Return on Security Investment

Davon abgeleitet wurde von Sonnenreich et al. [78] die Return On Security Investment (ROSI) Metrik speziell für das ISM entwickelt, womit der Kosten-Nutzen Faktor einer Sicherheitsmaßnahme berechnet werden kann. Mit Hilfe von ROSI kann bewertet werden, ob eine Maßnahme finanziell angemessen ist:

$$ROSI = \frac{\text{Vermiedener Verlust - Kosten der Maßnahme}}{\text{Kosten der Maßnahme}}$$

Verlust berechnen

Um den potenziellen Verlust eines Risikos zu berechnen, kann die ALE Metrik verwendet werden. Die Berechnung setzt dabei drei Komponenten voraus: die Kosten eines Sicherheitsvorfalls Single Loss Exposure (SLE), die Häufigkeit des Auftretens Annual Rate of Occurrence (ARO) und dem erwarteten Jahresverlust. Durch Multiplizieren beider Werte ergibt sich der potenzielle Verlust bei Eintreten eines Risikos:

$$ALE = SLE * ARO$$

Kosten einer Maßnahme

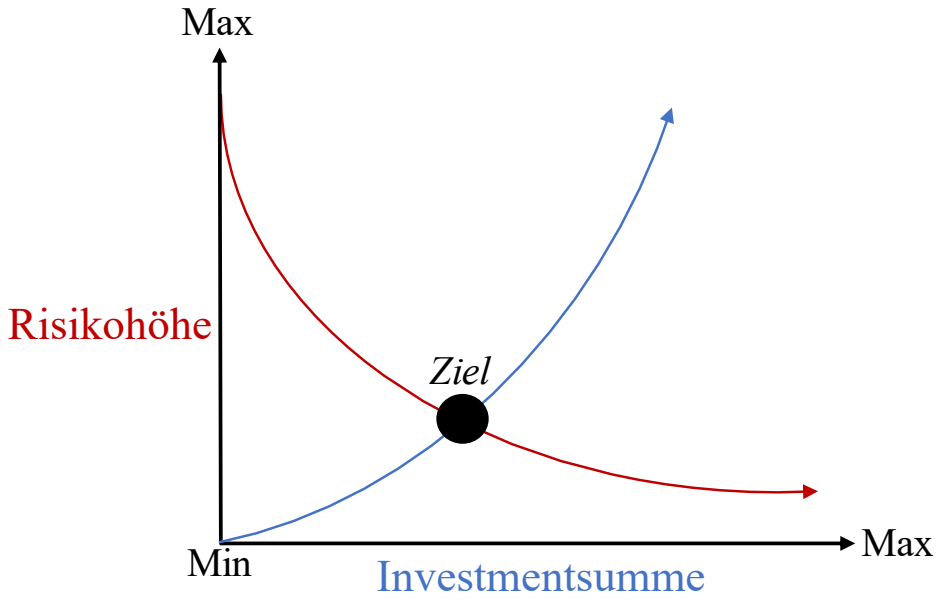
Die Kosten einer Maßnahme setzen sich aus bis zu fünf Komponenten zusammen. Der generelle *Einkaufspreis* beinhaltet alle Kosten zum Erwerb der Maßnahme bzw. Teile dieser, welche extern erworben werden müssen. Die *Installationskosten* fallen an, um die Maßnahme in der Organisation zu etablieren. Wurde die Maßnahme etabliert, beschreiben die *Betriebskosten* den Preis der Aufrechterhaltung der Maßnahme über einen gewissen Zeitraum. Weiterhin können regelmäßige *Wartungskosten* anfallen, die über den reinen Betrieb hinausgehen. Letztlich müssen manche Maßnahmen aktiv durch das Personal genutzt oder

betrieben werden, daher können auch *Schulungskosten* für die beteiligten Personen anfallen. Die Summe der anfallenden Kosten ergibt die Gesamtkosten einer Maßnahme, die bei der Auswahl berücksichtigt werden sollten. [62]

Behandlung als Investition

Diese Metriken können helfen, die Kosten einer Investition in Sicherheitsmaßnahmen einzuschätzen und gegen den Nutzen der Risikobehandlung abzuwägen. Die Schwierigkeit besteht darin, dass auch die hier vorgestellten und üblicherweise verwendeten Metriken eine quantitative Risikobewertung voraussetzen, welche im ISRM in den seltensten Fällen zum Einsatz kommt. Trotzdem bleiben Methoden wie ROSI ein wertvolles Werkzeug für Organisationen, das auch mit unsicheren Einstufungen genutzt werden kann, um verschiedene Behandlungsmethoden zu vergleichen [76]. Dabei wird versucht, mit geringstem Ressourceneinsatz den größtmöglichen Nutzen zu erzielen. Es gilt abzuwägen, bis zu welchem Punkt ein Investment in die Maßnahme noch sinnvoll ist und der potenzielle Verlust durch das Risiko diese noch zu rechtfertigen ist (Abbildung 2.3). Letztlich ist das Ziel eine optimale Ressourcenverteilung, um das Risikoniveau der Organisation maximal zu senken.

Abbildung 2.3: Abwägung im Verhältnis von Risiko und Kosten einer Sicherheitsmaßnahme [In Anlehnung an 51]



2.2 Arten des Risiko Managements

Die in der vorherigen Sektion beschriebenen Konzepte formen die Basis des RM bzw. ISRM im Speziellen. Das ISRM ist dabei nur einer der vielen Teilbereiche des RM. Inzwischen haben sich einige fest abgegrenzte RM-Teilbereiche etabliert, wobei nur ein Teil davon für diese Arbeit relevant ist. Grundsätzlich ist die Anzahl der Spezialisierungen unbegrenzt, da ein risikobasiertes Vorgehen in jeder Disziplin denkbar wäre, auch wenn die Anzahl der Anwendungen in der Praxis aktuell begrenzt ist. Neben dem allgemeinen RM und ISRM sind auch das ERM sowie das SCRM relevant für die Herleitung eines kollaborativen Vorgehens. Insbesondere der Umgang mit Risiken in Lieferketten (Supply Chains) und davon abgeleitete Strategien bilden die Basis für ein übergreifendes CRM.

2.2.1 Überblick RM

Definition RM

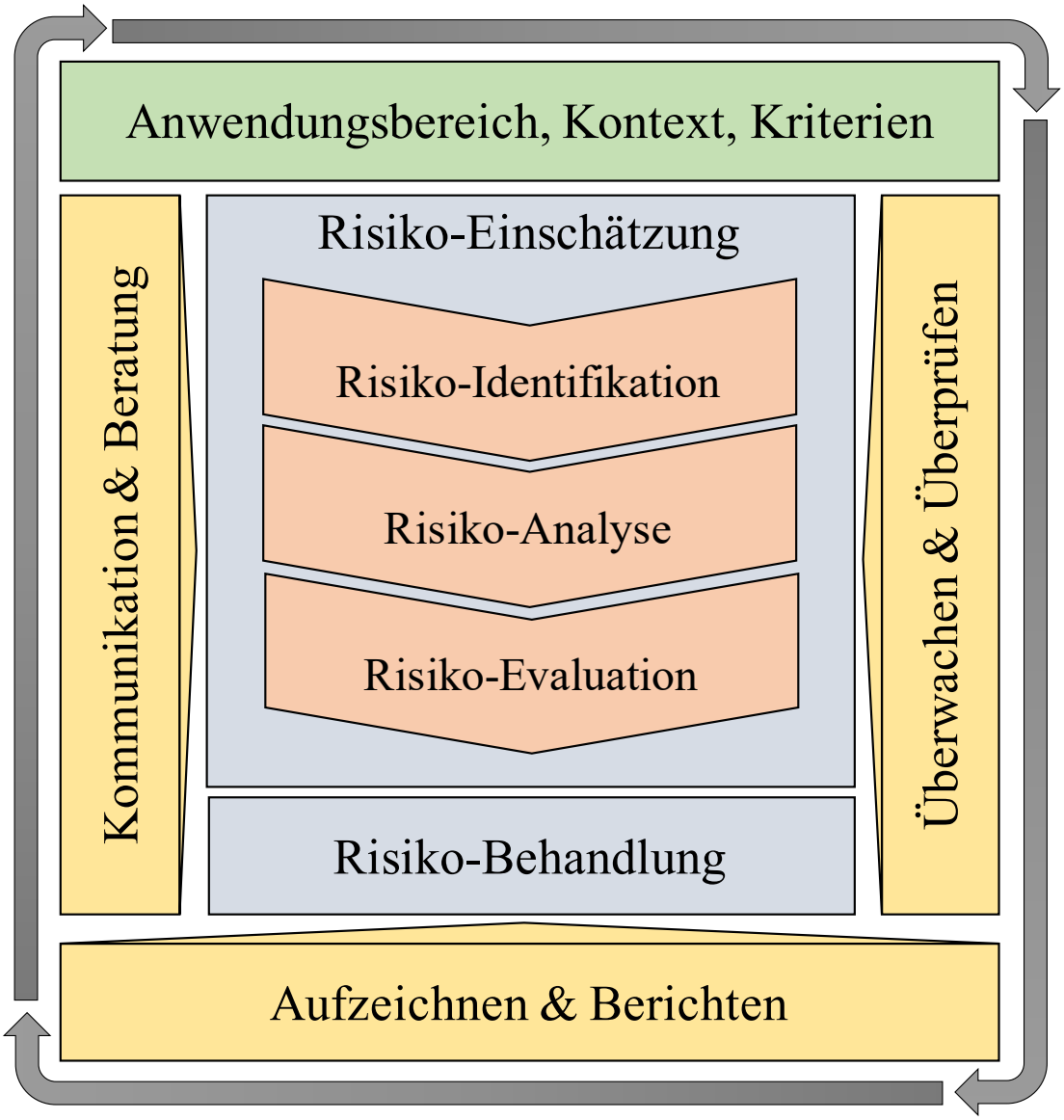
Das RM bezeichnet eine Sammlung koordinierter Tätigkeiten, um die Risiken einer Organisation zu verwalten und zu kontrollieren [35]. Dabei werden Risiken häufig durch Ereignisse mit negativer Auswirkung beschrieben, welche als Bedrohungen für Informationen, Prozesse und Dienste dargestellt werden. Diese Bedrohungen für ein Unternehmen zu identifizieren und nach ihrer Bedeutung für das Geschäftsfeld, wie Forschung und Lehre, zu priorisieren, wird oftmals als *Threat Modelling* bezeichnet. Auf dieser Grundlage verwendet das RM identifizierte Bedrohungen und ordnet sie gefährdeten Vermögenswerten des Unternehmens zu, um die resultierenden negativen Auswirkungen zu erkennen und eventuell abmildern zu können. Ziel ist es, Risiken so weit wie möglich zu minimieren, auch wenn diese meist nicht vollständig zu eliminieren sind. Das RM ist der organisatorische Prozess zum Identifizieren von Risiken, deren Analyse auf Basis von Eintrittswahrscheinlichkeit und Auswirkung sowie dem Auswählen von effektiven und wirtschaftlichen Behandlungsoptionen. Dabei muss die Behandlung eines Risikos nicht zwangsweise die Reduzierung des LoR zur Folge haben, da im Kontext der Unternehmensstrategie wirtschaftliche Optionen gewählt werden sollen. Das RM ist damit nicht nur ein Werkzeug zum Schutz des Unternehmens, sondern vor allem zur effektiven Steuerung der vorhandenen Ressourcen. Risiken existieren in vielen verschiedenen Bereichen einer Organisation, etwa als Geschäfts-, Strategie-, Umwelt-, Markt- oder Finanzrisiken.

Prozessmodell RM

Für jeden dieser Bereiche wird in der Realität ein eigener Risikomanagementprozess etabliert, welcher auf die spezifischen Risiken ausgerichtet ist und eigene Rahmenwerke nutzt. Der internationale Standard *ISO 31000* [35] definiert das RM als iterativen Prozess, welcher aus sechs Teilprozessen besteht (Abbildung 2.4). Im ersten Schritt wird der Anwendungsbereich des Prozesses sowie die konkrete Methodik definiert. Nun erfolgt eine auf Basis der gewählten Kriterien und Methodik durchgeführte Beurteilung der Risiken im Anwendungsbereich. Anschließend muss für jedes identifizierte Risiko entschieden werden, wie dieses behandelt werden soll. Die Ergebnisse der vorherigen Prozessschritte werden anschließend dokumentiert und an das Topmanagement berichtet. Weiterhin gibt es die zwei Unterstützungsprozesse für die interne und externe Kommunikation sowie die kontinuierliche Überwachung des Prozesses, welche parallel zur Beurteilung und Behandlung laufen.

Der komplette Prozess wird immer wieder durchlaufen, um sicherzustellen, dass neue Risiken identifiziert und bestehende Risiken an neue Gegebenheiten angepasst werden. Dieses Vorgehen, insbesondere der Ablauf zur Risikoeinschätzung, liefert das Muster für einen generischen RM-Prozess.

Abbildung 2.4: ISO/IEC 31000 RM Prozessmodell [In Anlehnung an 35]



2.2.2 Enterprise Risk Management

Definition ERM

Der klassische und seit Beginn des RM etablierte Ansatz war es, die verschiedenen Arten von Risiken in Organisationen individuell und domänenspezifisch zu verwalten. Bereits seit den 80er Jahren gab es jedoch Bestrebungen, ein Konzept zur Koordination der multidisziplinären Risikobereiche zu erstellen. Daraus hat sich über die nachfolgenden Jahrzehnte das sogenannte ERM entwickelt, welches einen übergeordneten Ansatz zur Konsolidierung aller unternehmensweiten Risiken beschreibt. Dabei soll das zentrale Management des Risikoportfolios der Organisation effektiver sein als die einzelnen Teilbereiche unabhängig voneinander zu verwalten. Am Ende soll die zentrale Koordinierung der Risikoentscheidungen dazu dienen, die Ressourcen der Organisation bestmöglich zu verteilen. Weiterhin versucht das ERM, den Umgang mit Risiken als Wettbewerbsvorteil zu begreifen, anstatt lediglich potenzielle Gefahren zu betrachten, die es zu vermeiden gilt. [79]

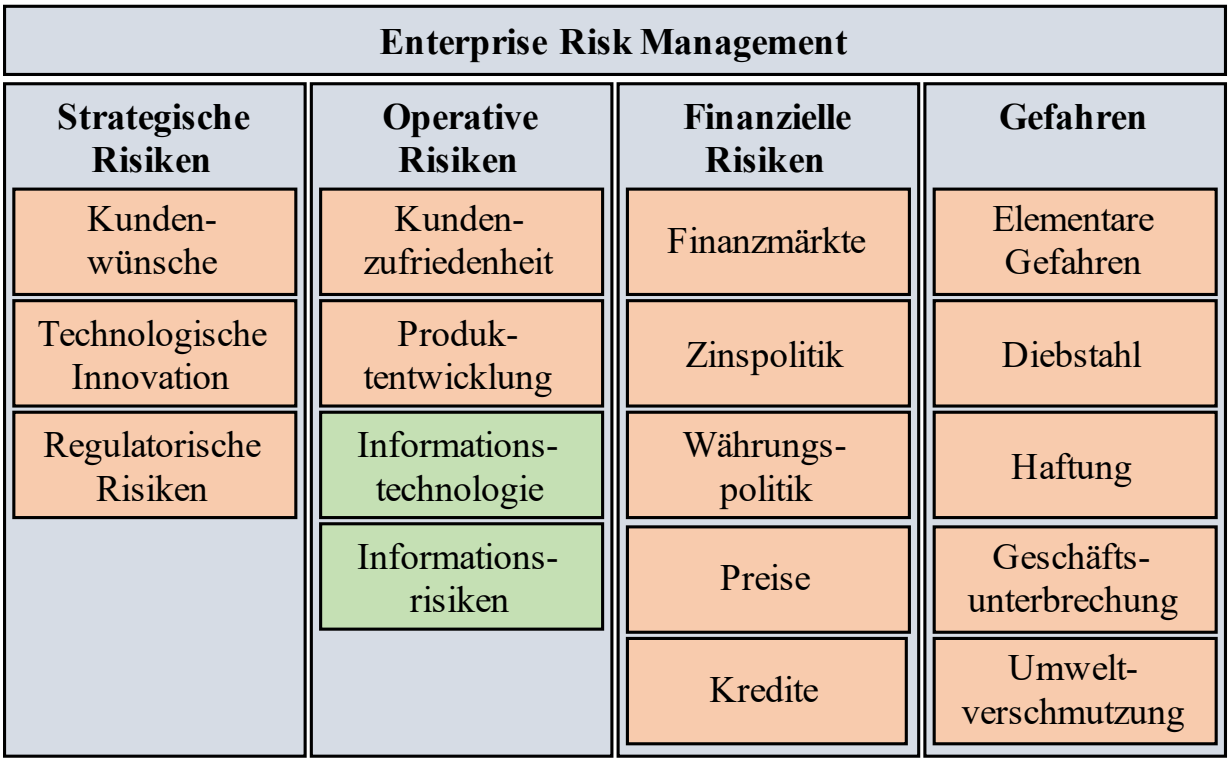
ERM Kategorien

Bereits vor dem Bekanntwerden des Begriffs ERM gab es ganzheitliche Ansätze, die unter den Namen *Corporate, Business, Holistic, Strategic oder Integrated Risk Management* geführt wurden. Das ERM lässt es sich grundsätzlich in die Kategorien *strategische, finanzielle und operative Risiken sowie Gefahren* unterteilen. Der initiale Fokus des klassischen RM lag konkret auf den Gefahren, welche eine Organisation als ganzes bedroht haben. Später entwickelte sich der Teilbereich Finanzen und die Bereiche der strategischen und operativen Risiken, welche inzwischen beliebig vielen Unterkategorien besitzen. Abbildung 2.5 zeigt eine nicht abschließende Übersicht der generischen Kategorien und Risikotypen des ERM. [47]

Scope des ERM

Das ERM kann helfen, einen risikobasierten Ansatz in allen Bereichen und Teilen der Organisation zu etablieren. Durch die zentrale Koordination der einzelnen Risikobereiche behält die Organisation den Überblick über alle relevanten Risiken. Ein Zusammenführen der Risiken aus verschiedenen Kategorien macht jedoch nur Sinn, wenn diese auch miteinander vergleichbar sind. Das setzt die Verwendung einer einheitlichen RM Methodik in allen Teilbereichen der Organisation voraus. Somit ist zum Etablieren des ERM zum einen eine starke Hierarchie innerhalb der Organisation erforderlich und zum anderen der Willen des Topmanagements, organisationsweite Prozessvorgaben zu machen. Während ersteres in den meisten Organisationsformen der Fall sein wird, ist letzteres nicht immer gegeben oder gewünscht. Es gilt also zu betrachten, ob das ERM in der jeweiligen Organisation sinnvoll etabliert werden kann. Unabhängig davon können RM Prozesse in den einzelnen Kategorien auch ohne übergeordnetes ERM aufgebaut werden.

Abbildung 2.5: Generische Kategorien und Risikotypen des ERM



2.2.3 Information Security Risk Management

Definition ISRM

Das ISRM beschreibt die Anwendung des RM auf Informationen und Technologie. Aus Sicht des ERM wäre das ISRM in der Kategorie der operativen Risiken anzusiedeln (Abbildung 2.5). Das ISRM beschäftigt sich konkret mit dem Management von Sicherheits- und Kontinuitätsrisiken für die Informationen und informationsverarbeitenden Systeme einer Organisation. Oftmals wird auch der Begriff *Cyber Risk Management* synonym zu ISRM verwendet. Dabei existiert keine klare Definition, Abgrenzung oder Einigung darüber, ob die Begriffe *Information Security* und *Cyber Security* tatsächlich das Gleiche bedeuten, ähnliche oder überlappende Themenkomplexe beschreiben [80]. Letztlich verbindet das ISRM die in Sektion 2.1 vorgestellten Konzepte (Asset, Schwachstelle, Bedrohung, Risiko, Maßnahme) zu einem sinnvollen, zusammenhängenden Ablauf.

Verbindung zum RM

Das ISRM ist für Organisationen ein kontinuierlicher Prozess, um die Information Assets und die Bedrohungen denen diese ausgesetzt sind besser zu verstehen. Es liefert die notwendigen Werkzeuge, um die potenzielle Risiken zu bewerten und mit diesen umzugehen. Dabei lassen sich die Prinzipien aus dem allgemeinen RM auch auf das ISRM übertragen [81]. Im Zentrum des ISRM stehen die Information Assets einer Organisation, welche mit angemessenem Ressourcenaufwand vor (Cyber) Bedrohungen geschützt werden sollen.

Struktur des ISRM

Unabhängig von der konkreten Ausgestaltung lässt sich das ISRM grundsätzlich aus vier Komponenten zusammensetzen: IS Risikoeinschätzung; Maßnahmen testen und überprüfen; IS Risikoreduktion; Operative IS. Die Risikoeinschätzung ist ein zentrales Element im ISRM. Sie beinhaltet eine objektive Überprüfung des Stands der IS der Organisation zur Ermittlung des aktuellen Risikoniveaus. Dabei wird der Verlust von Assets der Organisation im Rahmen einer BIA evaluiert und die Wirksamkeit existierender Maßnahmen analysiert. Anschließend wird die Bedrohungslage der Organisation betrachtet und potenzielle Schwachstellen identifiziert. Unter Berücksichtigung der Kritikalität und Werte der Assets wird die Risikohöhe ermittelt und bei Bedarf weitere Maßnahmen zur Reduktion vorgeschlagen. Eine weitere Komponente ist das Testen und Überprüfen von Maßnahmen. Dabei wird überprüft, ob die existierenden Maßnahmen den Sicherheitsanforderungen entsprechen. So kann die Wirksamkeit der Maßnahme überprüft werden, was wiederum Einfluss auf die Risikohöhe bzw. das spätere Restrisiko hat. In einem etablierten System läuft dies unabhängig bzw. parallel zur Risikoeinschätzung ab. Nach Prüfung der Maßnahmen und Einschätzung der Risiken muss das Management der Organisation entscheiden, wie mit den Risiken umgegangen werden soll. Entweder wird das Risiko akzeptiert oder es folgt eine Risikoreduktion, um die Risikohöhe zu reduzieren. Die Risikoeinschätzung liefert die notwendigen Daten, um eine faktenbasierte Entscheidung über die Investition von notwendigen Ressourcen zu treffen. Weiterhin stehen durch die kontinuierliche Prüfung der existierenden Maßnahmen Informationen über den Ist-Zustand bereit. Nach der Auswahl einer geeigneten Behandlungsoption müssen neue Maßnahmen als Teil der operativen IS umgesetzt werden. Die Implementierung muss letztlich in das Tagesgeschäft integriert und von vom Betriebspersonal durchgeführt werden. [62]

ISRM Prozess

Diese generischen Komponenten beschreiben die strukturellen Inhalte des ISRM unabhängig von einem spezifischen Vorgehen. In der Praxis wird das ISRM als Managementprozess dargestellt, für dessen konkretes Design sich verschiedene Frameworks etabliert haben. Einen allgemeinen ISRM Prozess definieren Shameli-Sendi et al. [73] mit vier aufeinanderfolgenden Aktivitäten (Abbildung 2.6):

1. **Risikokontext festlegen**
   Festlegen einer gemeinsamen Sicht auf Risiken innerhalb der Organisation, dem angestrebten Umgang mit Risiken und was die Grenzen des ISRM sind. Dazu gehört auch das Abstimmen der Risikokriterien in Abhängigkeit der Risikotoleranz und des Risikoappetits der Organisation. Nicht alle Bereiche oder Assets müssen im Rahmen des ISRM betrachtet werden, sondern basierend auf der Strategie der Organisation ein- oder ausgeschlossen werden. Das Ergebnis dieser Aktivität ist eine definierte Strategie für den Umgang mit IS-Risiken in der Organisation.

2. **Risiken einschätzen**
   Bereitstellen einer umfassenden Übersicht existierender Risiken, ihrer potenziellen Konsequenzen und möglichen Maßnahmen. Die Einschätzung besteht aus zwei Teilen, der Risikoanalyse und der Risikobewertung. In der Analyse werden zuerst wichtige Assets und deren Schwachstelle identifiziert, relevante Bedrohungen betrachtet und letztlich der potenzielle Schaden der resultierenden Risiken eingeschätzt. Anschließend werden die Risiken in der Bewertung anhand der festgelegten Risikokriterien eingestuft. Auf Basis dieser Einstufung werden die Risiken anhand der Risikohöhe priorisiert und eine angemessene Risikobehandlungsoption (Akzeptieren, Vermeiden, Transferieren, Reduzieren) ausgewählt.

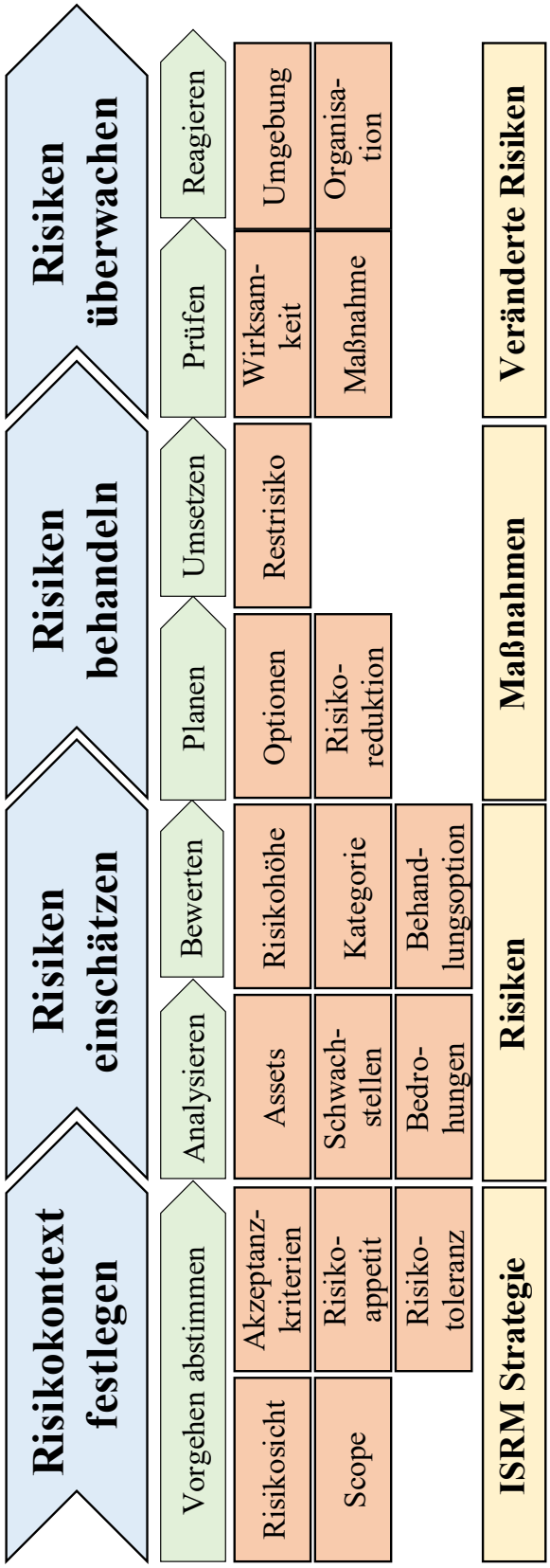
3. **Risiken behandeln**
   Umsetzen der gewählten Behandlungsoption, falls das betrachtete Risiko nicht akzeptiert wird. In den meisten Fällen ist ein Vermeiden oder Transferieren nicht möglich oder gewünscht, weshalb das Risiko reduziert werden soll. Dazu muss unter Berücksichtigung von Kosten und Nutzen eine angemessene Maßnahme ausgewählt und implementiert werden. Die Wirksamkeit der gewählten Maßnahme ist zu bewerten, um das verbleibende Restrisiko zu ermitteln.

4. **Risiken überwachen**
   Kontinuierliche Überprüfung der existierenden Risiken, um auf Änderungen zu reagieren. Die Risikohöhe ist nicht konstant, sondern veränderte Rahmenbedingungen können auch die Eintrittswahrscheinlichkeit oder Auswirkung des Risikos beeinflussen. Dieser Schritt ist besonders wichtig für die langfristige Effektivität des Prozesses und dessen Ausrichtung an den Zielen der Organisation.

Holistisches Vorgehen

Häufig wird die Risikoeinschätzung (risk assessment) als wichtigster Teil des ISRM angesehen, welche auch in der Literatur [62, 73, 82] besondere Aufmerksamkeit erhält. Für einen erfolgreichen Umgang mit IS-Risiken müssen jedoch alle Aktivitäten des Prozesses in der Organisation gleichermaßen etabliert werden. Nur durch ein holistisches ISRM können Risiken erfolgreich erkannt, bewertet und behandelt werden, um das Sicherheitslevel der Organisation bei optimalem Ressourceneinsatz zu erhöhen.

Abbildung 2.6: Darstellung eines generischen ISRM Prozesses



2.2.4 Supply Chain Risk Management

Scope des SCRM

In der heutigen globalisierten und vernetzten Welt werden auch die Verbindungen zwischen Organisationen zunehmend verflochtener. Dabei entstehen auch immer mehr Abhängigkeiten, welche neue externe Risiken für eine Organisation bedeuten. So führen kürzere Produktlebenszyklen, komplexe und internationale Partnerschaften, Unsicherheit bei der Nachfrage in globalen Märkten, Kostendruck, Outsourcing und Offshoring zu neuen Herausforderungen [83]. Mit dieser Thematik beschäftigt sich das sogenannte SCRM, eine weitere Form des RM. Dabei geht es um den Umgang mit von Lieferanten/Dienstleistern (engl. Supplier) ausgelösten Risiken, welche über die etablierte Supply Chain weitergetragen werden. Obwohl die heutigen Supply Chains immer länger und komplexer werden, begann die Entwicklung des SCRM erst Anfang der 2000er [31]. Seit etwa 2005 hat sich die Disziplin jedoch vom aufkommenden Trend in ein stark wachsendes Forschungsfeld verwandelt [84, 85].

Definition SCRM

Trotz der bereits langen Historie ist das SCRM noch immer ein aufstrebendes Feld [85], dessen Inhalt, Teilgebiete und die genaue Abgrenzung der Disziplin bisher nicht eindeutig definiert ist. Das Feld entwickelt sich kontinuierlich weiter, was zu einer Vielzahl an unterschiedlichen Definitionen führt, wie die Literaturanalyse von Gurtu und Johny [83] zeigt. Sie beschreiben das SCRM als „systematic and phased approach for recognizing, evaluating, ranking, mitigating, and monitoring potential disruptions in supply chains.“ In der einfachsten Variante geht es somit um die Identifikation von Risiken, die dazu geeignet wären, die Supply Chain zu stören und schlimmstenfalls zu unterbrechen. Durch die enge Verknüpfung und Abhängigkeit von Suppliern würde eine Störung innerhalb der Supply Chain einen direkten oder indirekten negativen Einfluss auf die Organisation bedeuten. Dabei ist zu beachten, dass je länger die Supply Chain ist, desto stärker wirkt sich eine Störung mit zunehmendem Abstand auf die Organisation aus, etwa durch den aus der Logistik bekannten Bullwhip-Effekt[2] [86]. Etwas weiter gehen Jüttner et al. [31], welche das SCRM als „the identification and management of risks for the supply chain, through a coordinated approach amongst supply chain members, to reduce supply chain vulnerability as a whole“ definieren. Diese Definition bringt noch eine zusätzliche Dimension in das RM ein. Während das klassische Vorgehen Risiken lediglich organisationsintern betrachtet hat, sollen diese im SCRM gemeinsam mit den in der Supply Chain involvierten Organisationen behandelt werden.

Supply Chain Networks

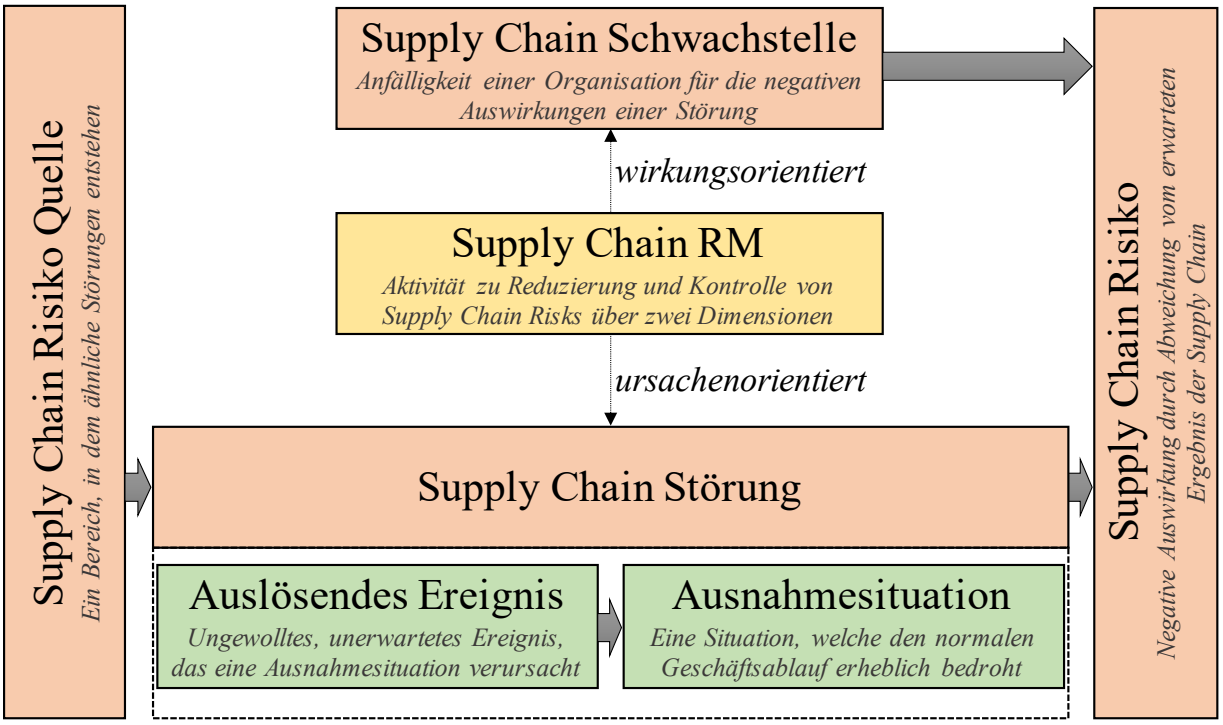
Supply Chains sind heute komplexe Strukturen, welche ein Netzwerk verschiedenster Organisationen bilden (teilweise auch Supply Chain Network genannt). Dabei geht es nicht mehr nur um die reine Lieferung von Produkten, sondern neue Kernziele wie Kostenminimierung, Wertmaximierung und dem Erschließen neuer Märkte durch die koordinierte Abstimmung zwischen den Teilnehmern. Diese Art der Partnerschaft kann viele Vorteile liefern und durch integrierte Koordinationsstrategien unerwünschten Ereignissen entgegenwirken. Mit zunehmender Partnerschaft wird die Supply Chain Struktur jedoch selbst zu Quelle und Medium von Risiken innerhalb des Netzwerks. [85]

[2] Der Peitscheneffekt beschreibt eine stufenweise zunehmende und durch fehlerhafte Kommunikation oder fehlende Information ausgelöste Störung der Lieferkette, z.B. Verzögerung bei Angebot und Nachfrage.

Supply Chain Risks

Das SCRM dient also dem Schutz einer Organisation durch die Koordination und Behandlung von Supply Chain Risks (SCRs). Ein SCR ist definiert als „any risks for the information, material and product flows from original supplier to the delivery of the final product for the end user“ [31]. Es lässt sich sagen, dass ein SCR ein unerwartetes, negatives Ereignis ist, welches unbehandelt zu einer Supply Chain Störung bzw. Unterbrechung (engl. Disruption) der Supply Chain führt (Abbildung 2.7). Wie auch im ISRM werden im SCRM üblicherweise nur *echte Risiken* betrachtet, da es um die ungewollten Konsequenzen auf die Organisation durch Störung der Supply Chain geht. Eine Supply Chain Disruption beeinträchtigt wiederum den Geschäftsbetrieb der Organisation, was letztlich zu einer negativen Konsequenz für das Business führt. Die Störung kann sowohl durch interne als auch externe SCRs ausgelöst werden, wodurch es teilweise schwierig wird, diese von anderen Geschäftsrisiken abzugrenzen. Eine mögliche Taxonomie ist die Aufteilung in nachfragebezogene, angebotsorientierte, regulatorische, rechtliche, katastrophale und Infrastruktur-Risiken. [86]

Abbildung 2.7: Supply Chain Risk Nomenklatur [In Anlehnung an 86]



Supply Chain Resilience

Nicht alle Supply Chains sind von den gleichen Risiken betroffen, da sich diese je nach Geschäftsbereich und Branche unterscheiden können, jedoch existieren einige allgemeingültige Risiken. Eine Strategie zum Umgang mit diesen Risiken zu planen und zu implementieren ist Aufgabe des SCRM, was nur durch eine kontinuierliche Beurteilung und Reduzierung der Schwachstellen erfolgen kann. Grundsätzlich existieren zwei mögliche Vorgehensweisen im SCRM: die vollständige Strategie zum RM oder der Fokus auf eine bestimmte Art von Störungen. Konkrete Störungen könnten laut Literatur Security [87], Lieferzeiten [88] oder Terrorismus [89] sein. Dabei wird jedoch üblicherweise von einer unabsichtlichen bzw. einer Störung von außen ausgegangen. Dem gegenüber stehen Störungen, durch vorsätzliche Handlungen eines Suppliers in der Supply Chain verursacht werden. Dazu zählen etwa (schadhafte) Qualitätsmängel an Produkten, um Kosten zu sparen. Gerade längere Supply Chains oder Netzwerke besitzen viele Teilnehmer, welche Risiken absichtlich oder unabsichtlich induzieren können. Diese zu managen und eine widerstandsfähige Supply Chain (Supply Chain Resilience) zu erhalten erfordert einen hohen Einsatz an Ressourcen. [83]

SCRM Konzepte

Die grundsätzlichen Konzepte im SCRM ist ähnlich zum allgemeinen RM, es kommt jedoch die organisationsübergreifende Perspektive hinzu. Dabei lassen sich insbesondere vier Konstrukte unterscheiden: Risikoquelle, Risikokonsequenz, Risikotreiber und Risikobehandlungsstrategie. Die Risikoquelle sind die Supply Chain spezifischen Variablen, deren Wert nur mit Unsicherheit bestimmt werden kann (Abbildung 2.7). Diese Quellen lassen sich konkret in drei Kategorien einteilen: Netzwerk-bezogen, umweltbezogen und organisatorisch. Analog zum allgemeinen RM beschreibt die Risikokonsequenz die Auswirkung des Risikos auf die Organisation. Dabei lassen sich betriebliche Unfälle, betriebliche Katastrophen und strategische Unsicherheiten unterscheiden, welche eine unterschiedliche Eintrittswahrscheinlichkeit und Schweregrad der Konsequenzen besitzen. Insbesondere im organisationsübergreifenden Kontext wird das Eingehen von Risiken als integraler Bestandteil des Managements angesehen, da jede strategische Entscheidung im Kontext einer Supply Chain ein kalkuliertes Risiko darstellt. Somit wird der Wettbewerbsdruck (Wettbewerbsfähigkeit, Kosten, Wirtschaftlichkeit) zum zentralen Risikotreiber, welcher die strategischen Entscheidungen in der Supply Chain beeinflusst. Solche Risikotreiber beeinflussen die Supply Chain und können zu Supply Chain Schwachstellen führen, welche dann von Risikoquellen betroffen sind. Letztlich bestimmt die Risikobehandlungsstrategie das strategische Vorgehen einer Organisation, um auf diese Risikoquellen und Schwachstellen zu reagieren. [31]

Cyber SCRs

Diese klassischen Konzepte und Vorgehensweisen des SCRM beziehen sich auf die allgemeinen Geschäftsziele einer Organisation, die durch Supply Chain Störungen negativ beeinflusst werden. Natürlich lässt sich die Kaskadierung in der Supply Chain auch auf IS-Risiken übertragen, wodurch sich eine Schnittmenge von SCRM und ISRM bildet, welche im folgenden als Cyber SCRM bezeichnet wird. Eine traditionelle Supply Chain befasst sich mit der Übertragung physischer Produkte, Finanzen oder Informationen, wohingegen eine Cyber Supply Chain ein Netzwerk von IT-Infrastruktur und Technologien zur Erstellung virtueller Güter darstellt [90].

SCR Sichtbarkeit

Der Standard *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* [91] definiert Cyber Supply Chain Risks, in ihrem Wording als *Information and Communications Supply Chain Risks* bezeichnet, als „Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.“[3] Es geht also um den potenziellen Schaden für die eigene Organisation durch den Verlust der Schutzziele (CIA) bei anderen Teilnehmern der Supply Chain. Ausfälle von Servicekomponenten (Verfügbarkeit), kompromittierte Software (Integrität) oder die Offenlegung von Informationen durch Supplier (Vertraulichkeit) sind Beispiele für Bedrohungen, welche zu direkten Risiken für die Organisation werden. Technische und organisatorische Schwachstellen über Organisationsgrenzen hinweg zu identifizieren und zu beheben stellt eine besondere Herausforderung dar. Dabei sind Schwachstellen in der Cyber Supply Chain besonders schwierig zu entdecken, da diese oftmals über Jahre etabliert und deren Ausnutzen schwer zurückverfolgt werden kann [91]. Die verschiedenen Ebenen einer Cyber Supply Chain, dargestellt in Abbildung 2.8, sind für die einzelne Organisation schwer zu Durchdringen und Sub-Supplier sowie deren Risiken damit schwer zu kontrollieren. Im Kontext des Cyber SCRM müssen Organisationen daher versuchen, den Anwendungsbereich des klassischen ISRM zu erweitern und externe Risiken so zu betrachten, als ob diese eigene IS-Risiken wären.

2.2.5 Collaborative SCRM

Scope des SCRM

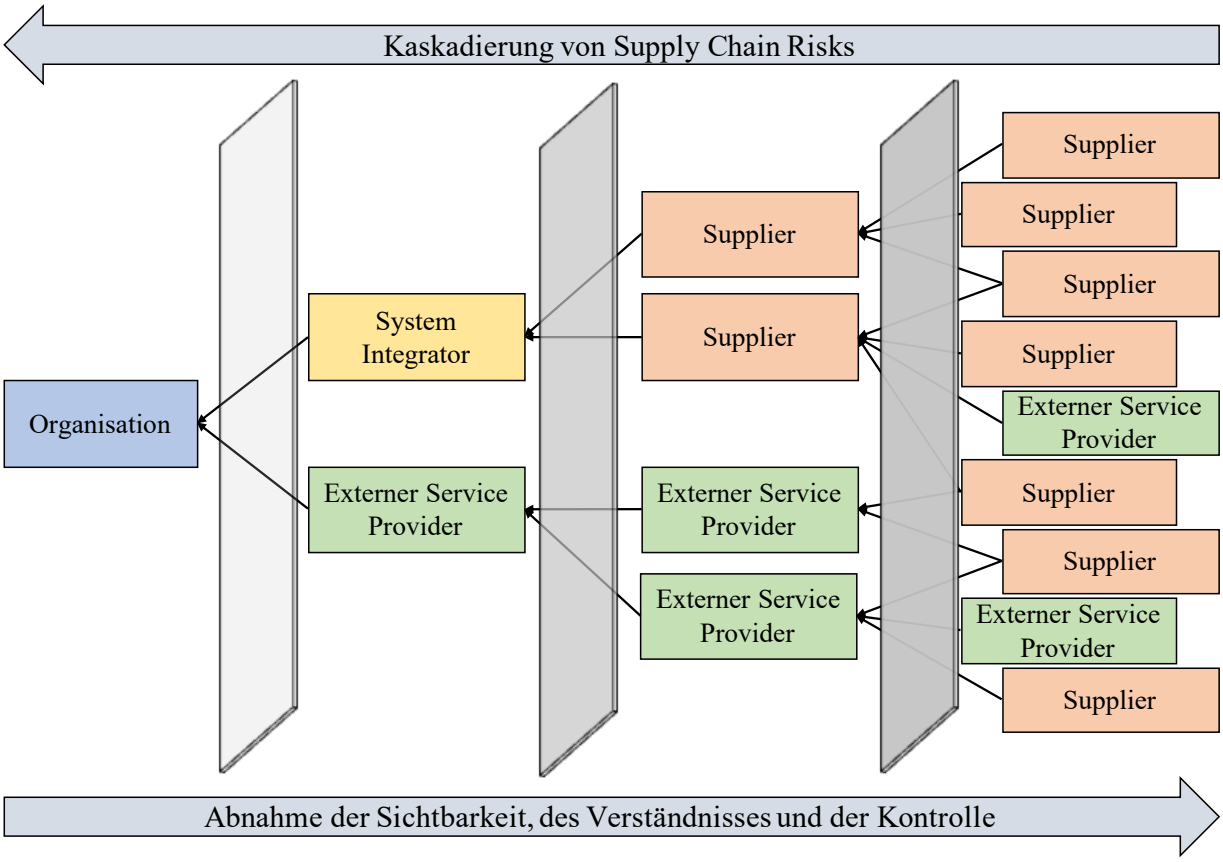
Das (Cyber) SCRM liefert bereits einen ersten Ansatz für eine organisationsübergreifende Risikobetrachtung. Allerdings ist die Zusammenarbeit dabei minimal und nicht auf Kollaboration ausgelegt. Supplier werden als zusätzliche Risikoquellen betrachtet und jegliche Form der Kooperation als Risikotreiber. Auch die Art der Analyse ist auf die eigene Organisation ausgerichtet, wobei SCRs lediglich zusätzliche Risiken sind, welche über die Supply Chain vererbt werden. Diese Risiken sollen identifiziert und einseitig behoben werden, eine engere Zusammenarbeit zur Bewertung oder Behandlung ist generell nicht vorgesehen. In der heutigen Geschäftswelt wird Kollaboration jedoch zum zentralen Element, wobei zwischen der Koordination und den damit verbundenen Risiken sorgfältig abgewogen werden muss [85].

Joint SCRM

Die traditionelle ERM Perspektive zielt lediglich auf Behandlungsmethoden ab, welche unternehmensintern umgesetzt werden können. Auch das angegliederte SCRM liefert damit wenig Möglichkeiten zur gemeinsamen Bewältigung von Risiken. Dabei sind SCRs deutlich komplexer als klassische interne Risiken, da sie von deutlich mehr Effekten betroffen sind. Durch die Übertragung entlang der Supply Chain über Organisationsgrenzen hinweg, werden Eintrittswahrscheinlichkeit und Auswirkung beeinflusst und damit sehr schwer abschätzbar. Um organisationsübergreifenden Risiken besser begegnen zu können, sollten Organisationen jedoch eine kooperative Perspektive einnehmen und ihr Vorgehen in Rich-

[3] Abgeleitet von der allgemeinen Risikodefinition aus FIPS 200 [92]

Abbildung 2.8: Cyber Supply Chain Intransparenz [In Anlehnung an 91]



tung eines gemeinsamen Prozesses erweitern, welches als Joint SCRM bezeichnet werden kann. SCRs müssen von diesen Organisationen als gemeinsame Risiken erkannt werden, denen auch gemeinsam begegnet werden sollte. Dazu ist es nötig, dass die Teilnehmer der Supply Chain dem Teilen von risikobezogenen Informationen gegenüber aufgeschlossen sind. Die Bereitschaft zur Weitergabe dieser Informationen und etablierte Methoden für die Weitergabe sind essenzielle Techniken für ein erfolgreiches Joint SCRM. [30]

Kollaboration

Durch eine noch intensivere Kollaboration im SCRM, also die weitergehende Zusammenarbeit zur Erreichung gemeinsamer Ziele, können die Organisationen insgesamt erfolgreicher bei der Bewältigung von SCRs sein. Dabei nimmt auch die Widerstandsfähigkeit der Supply Chain durch kollaborative Aktivitäten stetig zu. Neben den zwei bereits genannten Aktivitäten zum *Kommunizieren und Teilen von Informationen* kommen dabei noch *gemeinsame Ziele, abgestimmte Entscheidungen, gegenseitige Anreize, geteilte Ressourcen und ein gemeinsamer Wissensaufbau* hinzu. Diese kollaborativen Aktivitäten schaffen die notwendige Sichtbarkeit und Transparenz, um Supply Chain Störungen sowohl Upstream[4]

[4]Der Supply Chain Pfad zur Organisation hin, d.h. vom Supplier zur Organisation

als auch Downstream[5] erkennen zu können. Dies ermöglicht es, deutlich schneller auf Supply Chain Störungen zu reagieren bzw. potenzielle Störungen zu verhindern. Wenn Organisationen aufeinander angewiesen sind, führt das letztlich dazu, dass sie auch ihren Erfolg voneinander abhängig machen und eine gemeinsame Problemlösung und Planung anstreben. Insbesondere ein hoher Grad an Abhängigkeiten innerhalb eines Supply Chain Netzwerks erhöht auf diese Art die Supply Chain Resilience. Es zeigt sich insgesamt, dass Kollaboration ein sinnvoller Ansatz zur Erhöhung der *Sichtbarkeit, Geschwindigkeit und Flexibilität* des SCRM ist. [93]
Diese Formen der Zusammenarbeit im SCRM zielen hauptsächlich auf eine bessere Transparenz in der Supply Chain ab, um die Sichtbarkeit von SCRs zu erhöhen. Dies ist extrem wichtig ist, da mangelnde Sichtbarkeit in Supply Chains als Hauptproblem im SCRM [93, 91, 30, 85, 94] angesehen wird. Joint SCRM und vertiefende Zusammenarbeit können somit ein effektives Vorgehen zum Umgang mit SCRs sein.

[5]Der Supply Chain Pfad von der Organisation weg, d.h. von der Organisation zum Kunden

2.3 Etablierte Rahmenwerke und Methoden

ISRM Frameworks

Nachdem nun die Grundlagen des RM und dessen relevante Teilbereiche betrachtet wurden, sollen im Folgenden die existierenden Ansätze betrachtet werden, um ISRM in der Praxis zu implementieren. Dazu werden nationale und internationale Rahmenwerke vorgestellt, welche den State-of-the-Art in der angewandten Praxis des ISRM definieren. Die Analyse bezieht sich auf praxisrelevante Rahmenwerke, da diese Standards in allen Industriesektoren weltweit wesentlich sind und somit die Grundlage für praktisches ISRM in Organisationen bilden [73]. Die überwiegende Mehrheit der Literatur bezieht sich dabei auf dieselben Rahmenwerke. Auch die Praxis zeigt, dass ISRM in Organisationen durch die genannten Rahmenwerke sehr gut abgedeckt ist. Darüber hinaus konzentriert sich diese Übersicht speziell auf ISRM und vernachlässigt allgemeine RM oder SCRM Rahmenwerke. Es erfolgt jeweils eine Beschreibung des Frameworks, seines Anwendungsbereichs, der Struktur und des enthaltenen Risikokonzeptes. Dabei zeigen sich zwei generelle Ansätze in ISRM Frameworks. Diese sind entweder organisationsbasiert, d.h. der RM-Prozess betrachtet die Organisation als Ganzes, oder systembasiert, d.h. der RM-Prozess betrachtet jeweils ein einzelnes System/Asset.

Weitere Methoden

Darüber hinaus gibt es viele Methoden, die sich speziell mit bestimmten Tätigkeiten befassen, wie CORAS [95] oder CRAMM [96] für die Risikobewertung. Da diese nur einen Teilbereich abdecken oder spezifische Methoden definieren, wurden sie nicht weiter betrachtet. Auch wurden nicht alle potenziellen ISRM Frameworks untersucht, sondern nur solche, die entsprechende Praxisrelevanz aufweisen, d.h. eine entsprechende Anwendbarkeit und Verbreitung in der Industrie aufweisen. Eine umfassende Liste mit weiteren hier nicht genannten ISRM Methoden wurde im *Compendium of Risk Management Frameworks with Potential Interoperability* [37] veröffentlicht. Weiterhin präsentieren Wangen et al. [82] eine komplette Liste von Methoden zur Risikoeinschätzung, die im ISRM verwendet werden können.

2.3.1 ISO 31000 und ISO/IEC 27005

Die International Organization for Standardization (ISO) stellt einige international anerkannte Standards zum RM bereit, für den Bereich IS oftmals in Zusammenarbeit mit der International Electrotechnical Commission (IEC).

Anwendungsbereich

Der allgemeine Standard zum RM ist die *ISO 31000* [35], von welchem sich die Themenspezifischen Standards (e.g. IS, Qualität, Umwelt) ableiten. Obwohl dieser ein allgemeines und kein ISRM spezifisches Vorgehen beschreibt, soll das Framework besonders erwähnt werden, da die ISO 31000 heute de facto das Standardwerk zum RM darstellt. Der darin beschriebene Prozess (Abbildung 2.4) wurde weitläufig in Literatur und Praxis aufgegriffen, andere ISO und nicht ISO Rahmenwerke nutzen oder adaptieren inzwischen das grundlegende Vorgehen.

Auch die 27000er Reihe der ISO ist ein allgemein anerkannter Standard in Bezug auf IS. Die bekanntesten Teile sind die ISO/IEC 27001 [12], welche die Anforderungen an ein Information Security Management System (ISMS) definiert und die ergänzende *ISO/IEC 27002* [97], welche konkrete Sicherheitsmaßnahmen erläutert. Der relevante Standard für das ISRM ist die ISO/IEC 27005 [98].

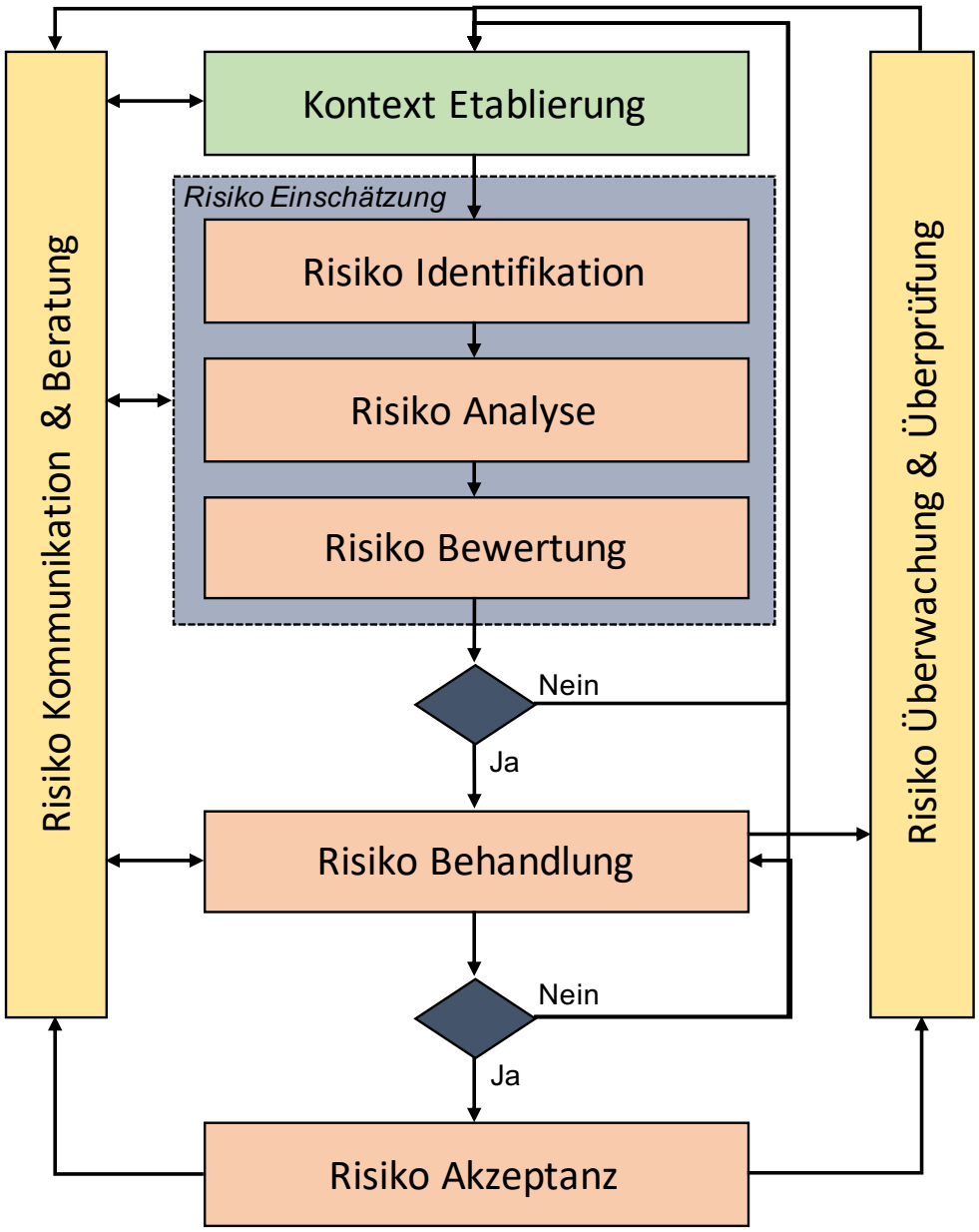
Dokumente & Struktur

Die ISO 31000 Standardfamilie besteht aus mehreren einzelnen Dokumenten, welche das allgemeine RM oder bestimmte Teilbereiche behandeln. Das Hauptdokument *ISO 31000* [35] enthält das organisatorische RM Framework sowie das Prozessmodell (Abbildung 2.4). Ersteres besteht aus den Teilen *Integration, Design, Implementation, Evaluation und Improvement*, letzteres beschreibt das allgemeine Vorgehen beim RM in Organisationen. Das genaue Vorgehen zur Risikoeinschätzung wird im Dokument *ISO/IEC 31010* [99] beschrieben. Zur einfachen Integration hilft die *IWA 31* [100] bei der Nutzung des Vorgehens in ISO Managementsystemen.
Ein solches kompatibles Managementsystem ist etwa ein ISMS gemäß *ISO/IEC 27001* [12]. Die übergeordnete 27000er Standardfamilie ist eine sehr umfangreiche Serie mit aktuell etwa 63 Veröffentlichungen. Das Hauptdokument *ISO/IEC 27000:2018* [49] selbst liefert eine Terminologie für das IS, die weiteren Veröffentlichungen behandeln spezifische Teilbereiche. Im Dokument *ISO/IEC 27005:2018* [98] wird eine Methode für das ISRM definiert. Das Vorgehen ist von der ISO 31000 abgeleitet, legt aber einen speziellen Fokus auf IS und definiert einen adaptierten Prozess.

Inhalt & Vorgehen

Abgeleitet vom generischen RM Modell der ISO 31000 (Abbildung 2.4) liefert die ISO 27005 ein für das ISRM einen leicht angepassten Prozess, wie in Abbildung 2.9 dargestellt. Dieser lässt sich in die drei Bereiche Planung, Durchführung und Unterstützung aufteilen. Wie auch beim generischen RM Prozess enthält die Planung das Definieren des Kontexts, d.h der Festlegung, in welchen Rahmen und mit welchen Methoden das ISRM in der Organisation durchgeführt werden soll. Die Durchführung enthält das Information Security Risk Assessment (ISRA), die Risikobehandlung und die Risikoakzeptanz. Der Teilprozess ISRA gliedert sicher wiederum in die Aktivitäten Identifikation, Analyse und Behandlung von Risiken. Letztlich enthält der Bereich Unterstützung Aktivitäten zur kontinuierlichen Überwachung des Prozesses sowie der Kommunikation relevanter Ergebnisse innerhalb der Organisation.

Abbildung 2.9: ISO/IEC 27005 RM Prozessmodell [In Anlehnung an 98]



2.3.2 BSI Grundschutz

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt ein nationales Rahmenwerk für die Absicherung von IT-Systemen und Organisationen bereit.

Anwendungsbereich

Als nationales Rahmenwerk des BSI richten sich die Standards in erster Linie an Behörden und angegliederte Organisationen, welche zum Teil verpflichtet sind, das Vorgehen umzusetzen. Die Vorgaben sind jedoch allgemein anwendbar und können grundsätzlich von jeder Art von Organisation eingesetzt werden. Das ISRM ist ein expliziter Teil des Rahmenwerks und ein essenzieller Bestandteil des definierten ISMS.

Dokumente & Struktur

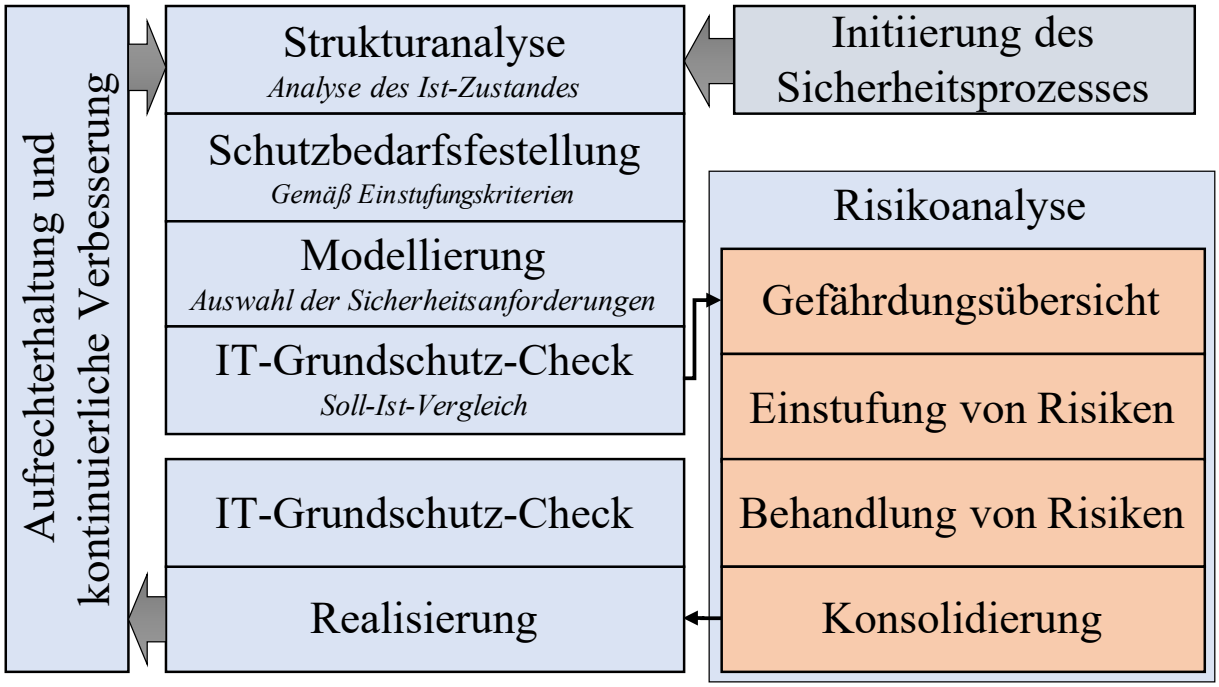
Das allgemeine Rahmenwerk zur IS ist der IT-Grundschutz [52]. Diese werden ergänzt durch verschiedene spezifische Standards und technische Richtlinien. Im Kontext eines ISMS definiert die 200er Reihe Anforderungen [13] und Methodik [56] basierend auf dem IT-Grundschutz. Speziell für das ISRM wird ein Vorgehen für die Risikoanalyse [101] und das Business Continuity Management [102] bereitgestellt.

Inhalt & Vorgehen

Das Vorgehen nach BSI beschreibt einen definierten RM-Prozess (Abbildung 2.10), der in den Kontext des IT-Grundschutzes eingebunden ist. Das konkrete RM Vorgehen orientiert sich allerdings wieder an der ISO 31000. Dabei ist zu beachten, dass das BSI andere Begriffe verwendet und den gesamten RM-Prozess als *Risikoanalyse* bezeichnet. Dieser Prozess zur Risikoanalyse besteht aus vier Schritten. Im ersten Schritt wird eine Gefährdungsübersicht erstellt, wobei elementare und spezifische Gefährdungen[6] ermittelt werden. Anschließend ist eine Risikoeinstufung durchzuführen, bei der Eintrittswahrscheinlichkeit und Auswirkung ermittelt wird, wobei die konkreten Kategorien für eine quantitative Bewertung vorgegeben sind. Aus den ermittelten Werten kann anschließend eine Risikokategorie abgeleitet werden, welche somit eine quantitative Risikohöhe darstellt. Basierend auf dieser Einstufung wird in der nachfolgenden Risikobehandlung eine angemessene Behandlungsoption ausgewählt: Risikovermeidung, Risikoreduktion, Risikotransfer oder Risikoakzeptanz. Letztlich erfolgt die Integration in den Sicherheitsprozess, indem eventuell zusätzlich definierte Maßnahmen (Risikoreduktion) in das Sicherheitskonzept aufgenommen werden.

[6] Gefährdungen sind ein BSI spezifischer Begriff, der eine Vermischung von Bedrohungen und Schwachstellen beschreibt

Abbildung 2.10: BSI Sicherheitsprozess mit Risikoanalyse [In Anlehnung an 101]



2.3.3 NIST SP 800-37 und RMF

Das National Institute of Standards and Technology (NIST) ist eine Standardisierungsbehörde der USA. In dieser Funktion stellt sie nationale Standards, unter anderem für IT und IS, bereit.

Anwendungsbereich

Der Fokus der NIST Standards liegt, wie auch das Wording zeigt, auf der Absicherung von US-Behörden und Informationssystemen. Viele Standards beziehen sich auf Vorgaben in den Federal Information Processing Standards (FIPS), welche für Behörden verpflichtend sind. Trotzdem haben die NIST Dokumente internationale Relevanz und werden weltweit von Organisationen verwendet. Im Gegensatz zu anderen vorgestellten Standards bezieht sich das Risk Management Framework (RMF) nicht auf die gesamte Organisation, sondern auf Informationen und Informationsverarbeitende Systeme. Somit ist der ISRM Prozess zwar ähnlich, jedoch immer mit Fokus auf einzelne Systeme.

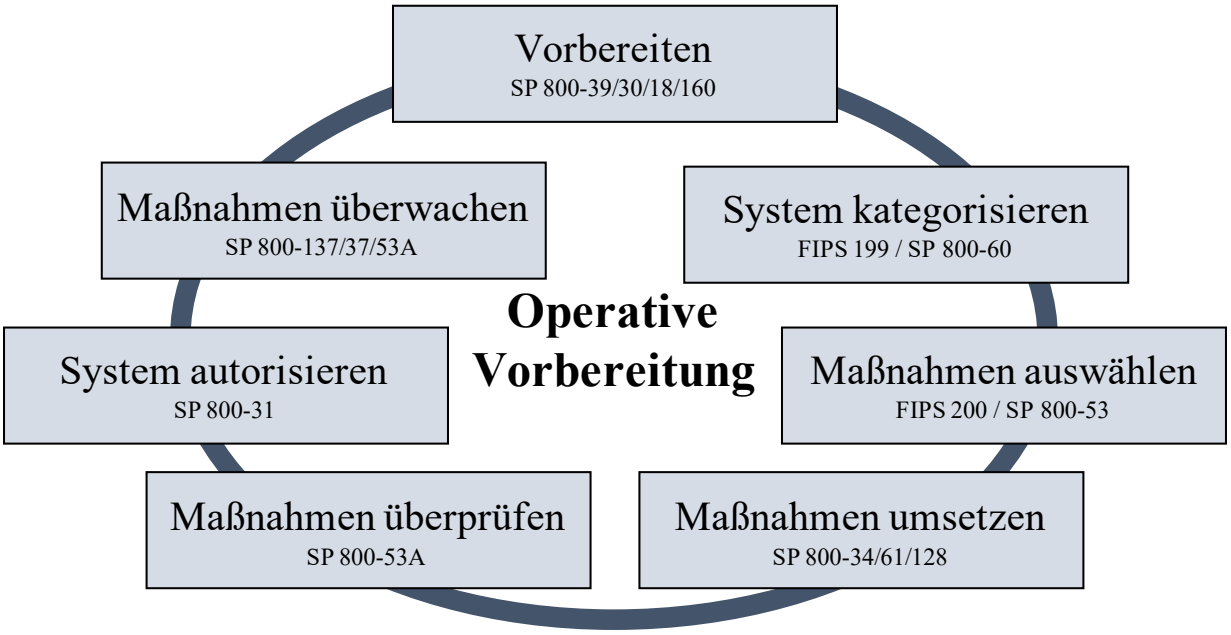
Dokumente & Struktur

Alle Standards zum Thema IS finden sich in der Reihe *NIST Special Publications 800*. Dazu gehört insbesondere das *Risk Management Framework for Information Systems and Organizations* [103]. Dabei handelt es sich um ein Sammelwerk, welches auch viele andere Veröffentlichungen aus der 800er Reihe logisch verknüpft. Dazu gehören unter anderem *Managing Information Security Risk* [104] zum Umgang mit IS-Risiken sowie der *Guide for Conducting Risk Assessments* [105] mit Methoden zur Risikoeinschätzung. Weiterhin zu erwähnen ist die mit dem Fokus auf Sicherheitsmaßnahmen ausgelegte Veröffentlichung *Security and Privacy Controls for Federal Information Systems and Organizations* [106] und die Erweiterung *Contingency Planning Guide for Federal Information Systems* [107] zum Continuity Management. Die bereits genannte aber unabhängige Veröffentlichung *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* [91] beschäftigt sich mit dem Thema Cyber SCRM. Aufbauend auf diesen Veröffentlichungen entstand das übergreifende online *NIST Risk Management Framework* [108].

Inhalt & Vorgehen

Der RMF Prozess ist in sieben Schritte aufgeteilt, wie im Prozessmodell in Abbildung 2.11 dargestellt. Da das RMF systembezogen aufgebaut ist, ist das Vorgehen iterativ und wird pro System durchgeführt. Jeder Schritt verweist auf bestimmte NIST Dokumente, welche das konkrete Vorgehen beschreiben. Der Prozess beginnt mit einem Vorbereitungsschritt zur Ausarbeitung der organisatorischen Rahmenbedingungen wie Rollen, RM Strategie, Risikotoleranz und Appetit der Organisation und eine Definition von Standardsicherheitsmaßnahmen. Auch die komplette Aktivität zur Risikoeinschätzung ist bereits Teil der Vorbereitungsphase. Im zweiten Schritt sollen alle Informationen und Systeme der Organisation basierend auf den FIPS Sicherheitskategorien kategorisiert werden, was quasi eine BIA darstellt. Anschließend wird für jede der drei Sicherheitskategorien (Gering, Mittel, Hoch) eine Auswahl von Sicherheitsmaßnahmen festgelegt, welche jeweils die Control-Baseline bilden. Die Baseline besteht aus allgemeinen Maßnahmen, basierend auf der Sicherheitskategorie, sowie spezifischen Maßnahmen, basierend auf der Risikoeinschätzung. Anschließend sollen die auf diesem Weg geplanten Maßnahmen implementiert werden. Nach erfolgreicher Umsetzung wird ein Review der neu implementierten Maßnahmen durchgeführt, um sicherzustellen, dass diese wie geplant eingeführt wurden. Bevor ein System in die Produktion überführt wird, muss dieses formal freigegeben werden. Letztlich wird die Funktionalität aller Maßnahmen kontinuierlich überwacht, um deren Wirksamkeit zu überprüfen und den aktuellen Risikostatus zu kontrollieren.

Abbildung 2.11: NIST RMF Schritte und Publikationen [In Anlehnung an 108]



2.3.4 COBIT und COBIT5 for Risk

Die ISACA Organisation (ursprünglich die Abkürzung für Information Systems Audit and Control Association) stellt verschiedene Frameworks und Anleitungen im Bereich IT-Governance, Management und IS bereit.

Anwendungsbereich

COBIT bezeichnet sich selbst als Framework für das I&T Governance im Unternehmen. Dabei wurde bewusst von IT zu I&T gewechselt, was in diesem Kontext für Information and Technology steht. Damit wurde hervorgehoben, dass das Framework grundsätzlich in jeder Organisation anwendbar ist und nicht nur im klassischen IT-Kontext. COBIT ist ein high-level Framework, welches das Management der IT auf Geschäftsebene ausrichtet.

Dokumente & Struktur

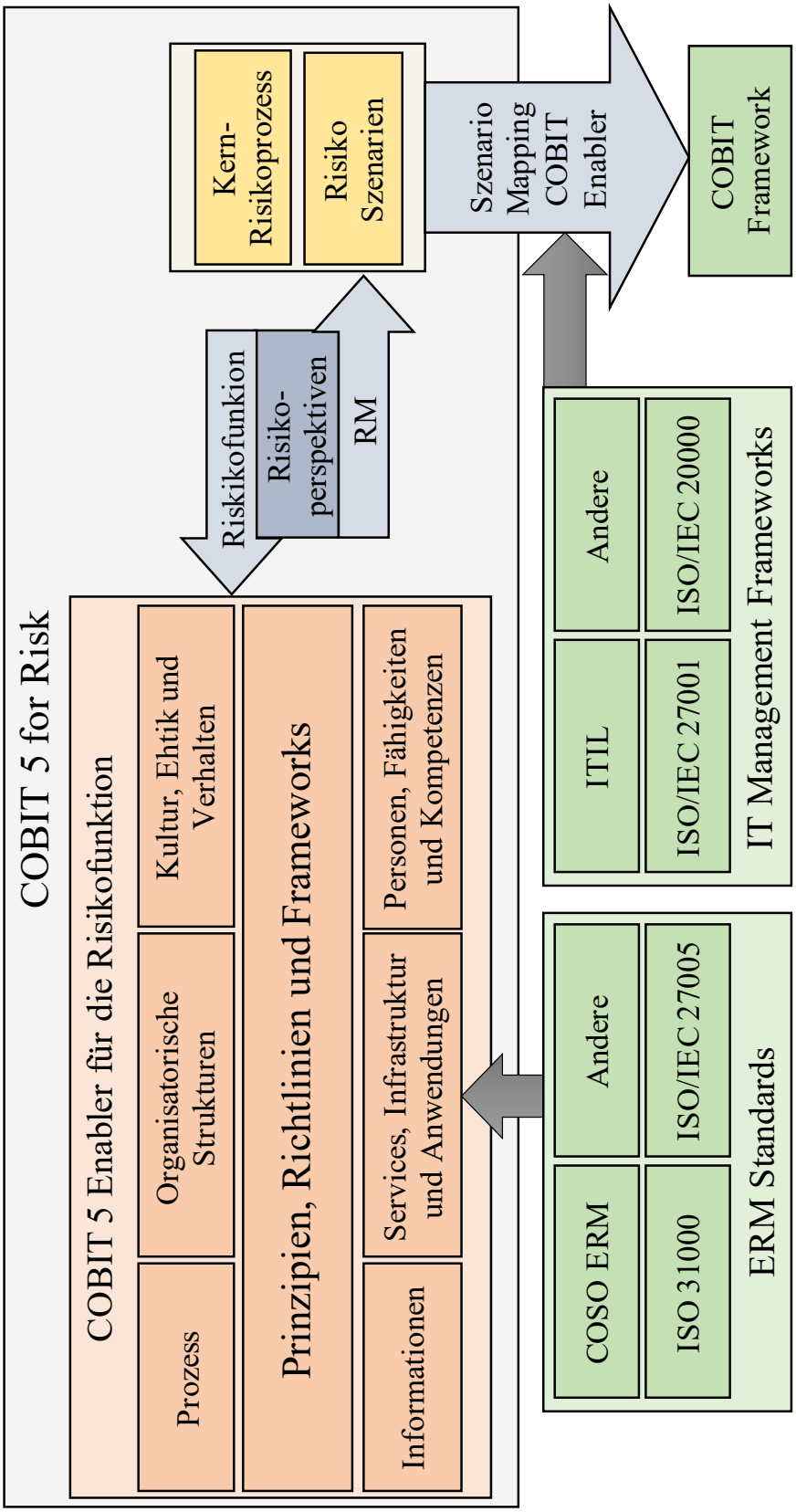
Lange Zeit war COBIT 5 [109] der Hauptteil der Reihe, welcher über die Jahre um verschiedenste Aspekte erweitert, darunter *COBIT 5 for Information Security* [110] und *COBIT 5 for Risk* [111]. Diese wurde durch die aktuelle Version [112, 113] ersetzt. Die neue Version versucht die Themen IS und RM von Anfang an stärker in das Framework zu integrieren.

Trotzdem setzt das Framework auf Erweiterungen, sogenannte Fokus Areas. In diesem Zusammenhang sind bereits *COBIT Focus Area: Information Security* [114] und *COBIT Focus Area: Information and Technology Risk* [115] erschienen.
Da sich das Framework selbst als Umbrella-Framework bezeichnet referenziert es wiederum auf andere Frameworks. Dies sind für RM die bereits genannten Frameworks ISO/IEC 27005 und NIST SP 800-37 sowie außerdem COSO ERM. *COSO Enterprise Risk Management* [116] ist ein Business-Framework zum allgemeinem RM in Unternehmen. Es ist ein anerkanntes und weit verbreitetes Framework, beschäftigt sich jedoch nicht im Speziellen mit dem Teilbereich IS. Aus diesem Grund wurde es in dieser Veröffentlichung nicht weiter betrachtet.

Inhalt & Vorgehen

COBIT 5 for Risk [111] integriert das ISRM in die COBIT Umgebung, indem es die notwendigen Rahmenbedingungen und Schnittstellen definiert. Dabei bezieht sich das Framework konkret auf die Module *EDM03 Ensured Risk Optimisation* and *APO12 Managed Risk* des übergeordneten COBIT Frameworks [112, 113], welches die Ziele für den Umgang mit IS-Risiken definieren. Das ISRM wird im Framework aus zwei Perspektiven betrachtet (Abbildung 2.12). Eine Perspektive beschreibt, wie eine Organisation die sieben COBIT Enabler nutzen kann, um die notwendigen Risikofunktionen aufzubauen. Die enthaltenen Themengebiete umfassen Grundlagen, Ressourcen und organisatorische Rahmenbedingungen des ISRM. Es wird jedoch kein konkreter Prozess definiert, sondern die notwendigen Module und Prozessziele aus COBIT referenziert, welche zur Vollständigkeitsprüfung genutzt werden können. Somit definiert die Perspektive Risikofunktion die allgemeinen Voraussetzungen für das ISRM. Die andere Perspektive beschreibt, wie der Managementprozess genutzt werden kann, um auf spezifische Szenarien zu reagieren. Dabei liefert das Framework 112 Risikoszenarien in 20 Risiko-Kategorien, welche zur Planung genutzt werden sollen. COBIT gibt lediglich den Rahmen und die Ziele für das ISRM vor, schreibt jedoch keine konkrete Methode für die Risikoeinschätzung vor, sondern orientiert sich dabei an existierenden Methoden.

Abbildung 2.12: COBIT ISRM Prozess [In Anlehnung an 111]



2.3.5 Risk IT Framework

Das Risk IT Framework wird ebenfalls von der ISACA Organisation herausgegeben. Ursprünglich als Erweiterung zu COBIT herausgebracht, laufen die beiden Frameworks nun parallel, insbesondere da mit COBIT for Risk ein eigenes Risikodokument entstand.

Anwendungsbereich

Mehr als andere zielt das Risk IT Framework darauf ab, dass ISRM als organisationsweite Herausforderung zu begreifen und in das ERM zu integrieren. Dabei soll das ISRM nicht nur als Teilbereich der operativen Risiken angesehen werden, sondern essenzieller Bestandteil aller ERM Bereiche, die letztlich mit I&T zusammenhängen. In diesem Zusammenhang wird insbesondere versucht, auch die Risikobehandlung im ganzheitlichen Kontext der Organisation zu betrachten.

Dokumente & Struktur

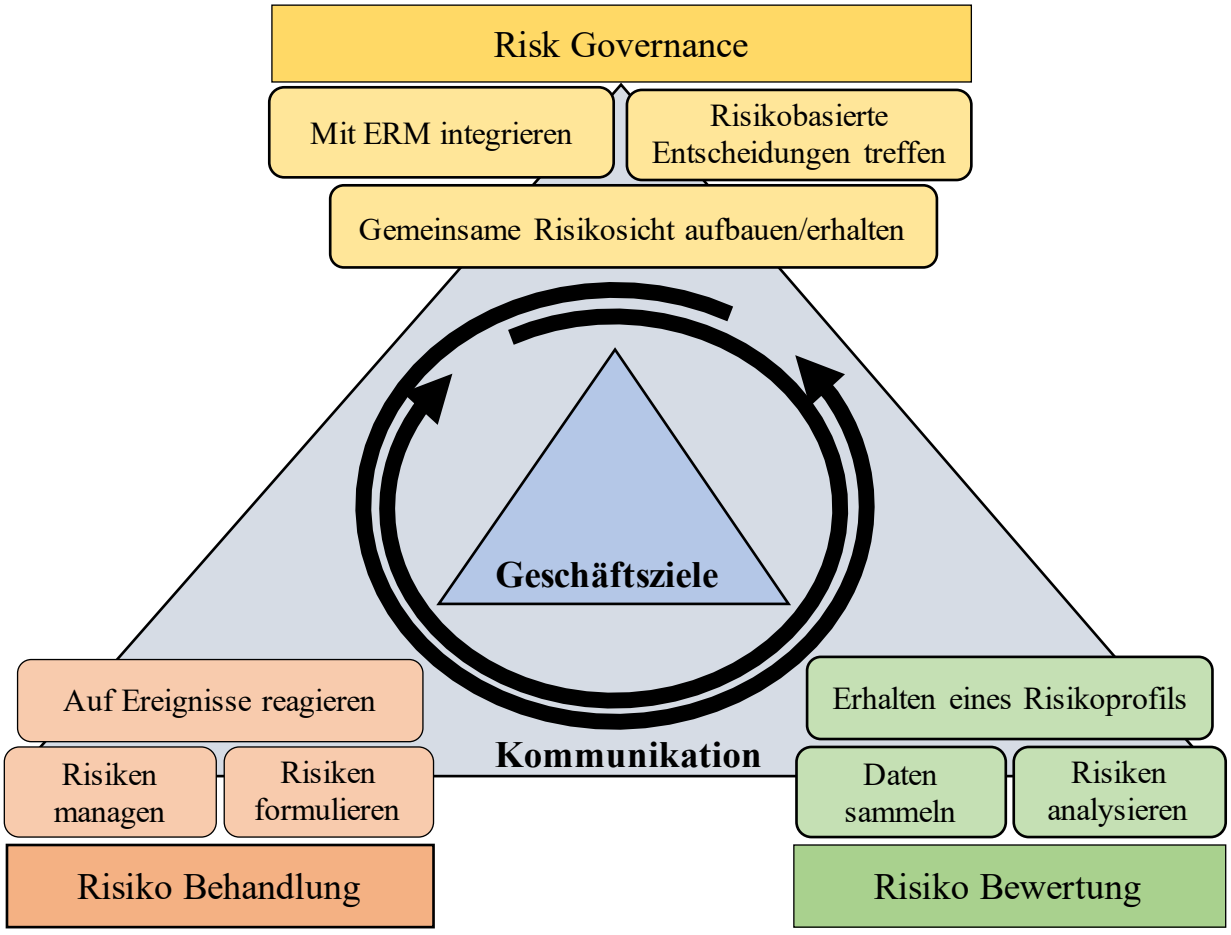
Das *Risk IT Framework* [117] stellt ein umfassendes Kompendium für das ISRM bereit. Es wird durch den Praxisleitfaden *Risk IT Practitioner Guide* [118] ergänzt, welcher Umsetzungsanleitungen liefert. In der aktualisierten zweiten Version [119] wurde das Framework weitgehend überarbeitet und umstrukturiert. Besonders die neue Version bezieht sich direkt auf die Module *EDM03 Ensured Risk Optimization* und *APO12 Managed Risk* aus dem COBIT Framework.

Inhalt & Vorgehen

RiskIT liefert einen Überblick über Prinzipien, Grundlagen und Vorgehen beim ISRM. Wie auch COBIT for Risk ist das Vorgehen mit COBIT kombinierbar und bezieht sich auf die gleichen Module (EDM03, AP012), jedoch kann das Framework auch komplett eigenständig eingesetzt werden. Das Framework liefert einen kompletten ISRM Prozess (Abbildung 2.13) mit Governance, Einschätzung, Behandlung und Bewertung von Risiken. Der Prozess beginnt mit dem übergeordneten Thema Risiko Governance. Wie auch in anderen Frameworks wird zuerst der Kontext etabliert und eine gemeinsame Sicht auf das ISRM definiert. Allerdings wird hier bereits die Schnittstelle zum ERM als wichtiges Element einbezogen. Im Rahmen der Risikoeinschätzung werden Risiken analysiert und bewertet. Zur Analyse wird ein szenario-basiertes Vorgehen eingesetzt, entweder Top-Down (Ableiten von Szenarien von den Geschäftszielen) oder Bottom-Up (Definieren von Szenarien und anschließende Reduktion). Als Grundlage der Bewertung wird eine BIA auf Basis der Unternehmenswerte (Assets) durchgeführt.

Auf Basis der Bewertung erfolgt anschließend die Risikobehandlung durch akzeptieren, vermeiden, teilen, transferieren oder reduzieren des Risikos. Dabei wird zusätzlich noch das Aggregieren von Risiken als Option genannt, bei der das Risiko mit anderen Risiken aus dem ERM zusammengeführt und integriert behandelt werden kann. Weiterhin nimmt das Thema Awareness, Reporting und Kommunikation eine wichtige Rolle im Prozess ein. Dabei sollen die Ergebnisse des Prozesses kontinuierlich an relevante interne und externe Stakeholder kommuniziert werden.

Abbildung 2.13: RiskIT ISRM Prozess [In Anlehnung an 119]



2.3.6 FAIR

Factor Analysis of Information Risk (FAIR) ist ein Ansatz für die quantitative Risikoeinschätzung des FAIR Instituts.

Anwendungsbereich

Es handelt sich genau genommen nicht um ein vollständiges ISRM Framework, da es sich speziell auf die Bewertung von IS-Risiken konzentriert. Als einzige quantitative Methode zur Analyse von IS-Risiken, die auch einen hohen Verbreitungsgrad besitzt, hat das Framework trotzdem eine hohe Relevanz. Das Konzept basiert auf der bekannten Risiko-Messmethode *Value at risk*[7]. Damit liefert es eine detaillierte Methode zur Berechnung der Risikohöhe, welche grundsätzlich in jeder Organisation eingesetzt werden kann.

Dokumente & Struktur

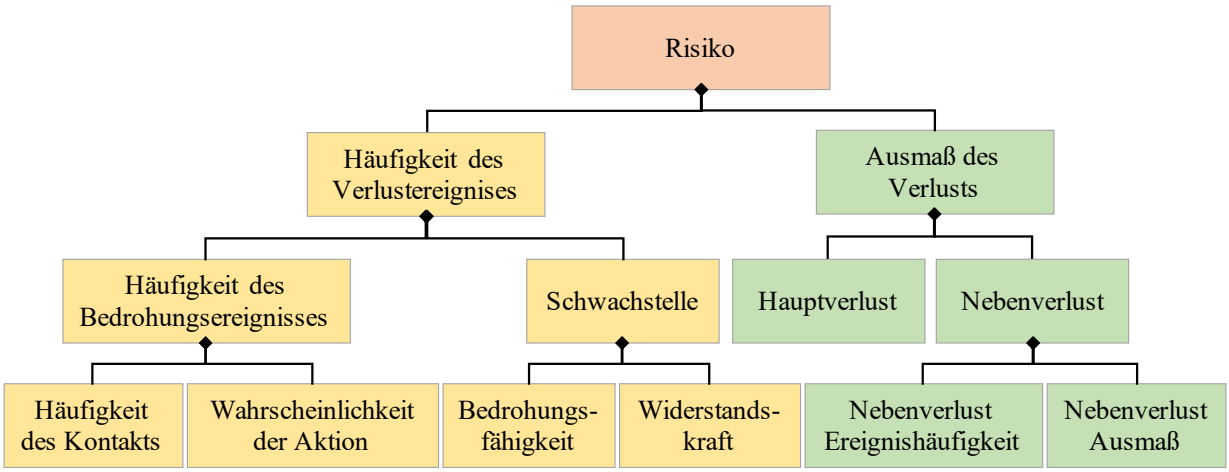
Es existiert das Hauptdokument *Measuring and Managing Information Risk* [120], welches das komplette Framework enthält. Die Grundsätze von FAIR wurden vom Konsortium *The Open Group* in zwei Veröffentlichungen standardisiert. Dabei wurden die Methodik [121] sowie die Terminologie [122] gemeinsam als OpenFAIR veröffentlicht. Im Rahmen dieser Arbeit wird das OpenFAIR Framework der Open Group herangezogen. Insbesondere, da hier auch eine Terminologie definiert wird, welche das ISRM in Organisationen beeinflusst, hat das Framework für die weitere Arbeit Relevanz.
Die Open Group hat versucht, die Konzepte möglichst allgemeingültig und kompatibel zu gestalten. So fließt etwa Input aus OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [123] ein, während eine Verbindung zu anderen Methoden genauso möglich ist. Das Framework betont seine Kompatibilität zu anderen ISRM Standards und hat daher Guides zur Verbindung von ISO/IEC 27005 [124] sowie dem NIST Framework [125] herausgebracht.

[7] Maximaler Wertverlust über einen bestimmten Zeitraum bei definierter Verlustwahrscheinlichkeit

Inhalt & Vorgehen

Das FAIR Modell, dargestellt in Abbildung 2.14, stellt Begriffe und Struktur für eine quantitative Risikoanalyse bereit. Der Prozess zur Risikoeinschätzung startet mit der Festlegung des Anwendungsbereichs, bei der Verantwortlichkeiten, betrachtete Assets und relevante Bedrohungen festgelegt werden. Anschließend beginnt die modellbasierte Risikoanalyse, bei welcher der aktuelle Risikozustand der Organisation ermittelt wird. Dazu wird das FAIR Modell verwendet, welches die einzelnen Faktoren zur Modellierung eines Risikos und Ermittlung der Risikohöhe darstellt.
Davon ausgehend werden Alternativen modelliert und evaluiert, die einen verbesserten Stand der Organisation beschreiben. Die Ergebnisse werden dem Entscheidungsträger vorgelegt, um über die Risikobehandlung zu entscheiden. Die Risikobehandlung und nachfolgende Schritte sind nicht mehr Teil von FAIR. Auch in diesem Vorgehen spielt die kontinuierliche Kommunikation mit Stakeholdern und Entscheidungsträgern eine zentrale Rolle.

Abbildung 2.14: FAIR Risiko Konzept [In Anlehnung an 122]



2.3.7 MoR

Das Framework Management of Risk (MoR) ist ein Rahmenwerk zum praxistauglichen ISRM. Obwohl das Framework lange Zeit nicht mehr aktualisiert wurde[8], hat es in der Praxis nicht an Popularität verloren haben.

Anwendungsbereich

MoR ist ein anwendungsorientiertes Framework, das sich auch gezielt an Praktiker richtet. Es ist deutlich kompakter als andere Frameworks und fokussiert sich auf praxisrelevante Aspekte des RM. Die beschriebenen Konzepte basieren auf den Prinzipien der ISO 31000. MoR wird von Axelos publiziert, der gleichen Organisation die auch das sehr bekannte Service Management Framework Information Technology Infrastructure Library (ITIL) herausgibt, was wahrscheinlich zur Bekanntheit beigetragen hat. Eventuell hat auch diese Nähe dafür gesorgt, dass MoR im Bereich ISRM populär geworden ist, obwohl es eigentlich ein allgemeines RM Framework darstellt.

Dokumente & Struktur

Das Framework besteht aus nur einem Dokument: *Management of Risk: Guidance for Practitioners* [127]. Damit ist es deutlich kompakter als andere der vorgestellten Frameworks. MoR basiert auf vier Kernkonzepten, welche auch die Struktur des Frameworks definieren: Prinzipien; MoR Ansatz; Prozesse; Einbetten und Überprüfen. Für jedes Konzept werden Anleitungen, Techniken und Ressourcen bereitgestellt.

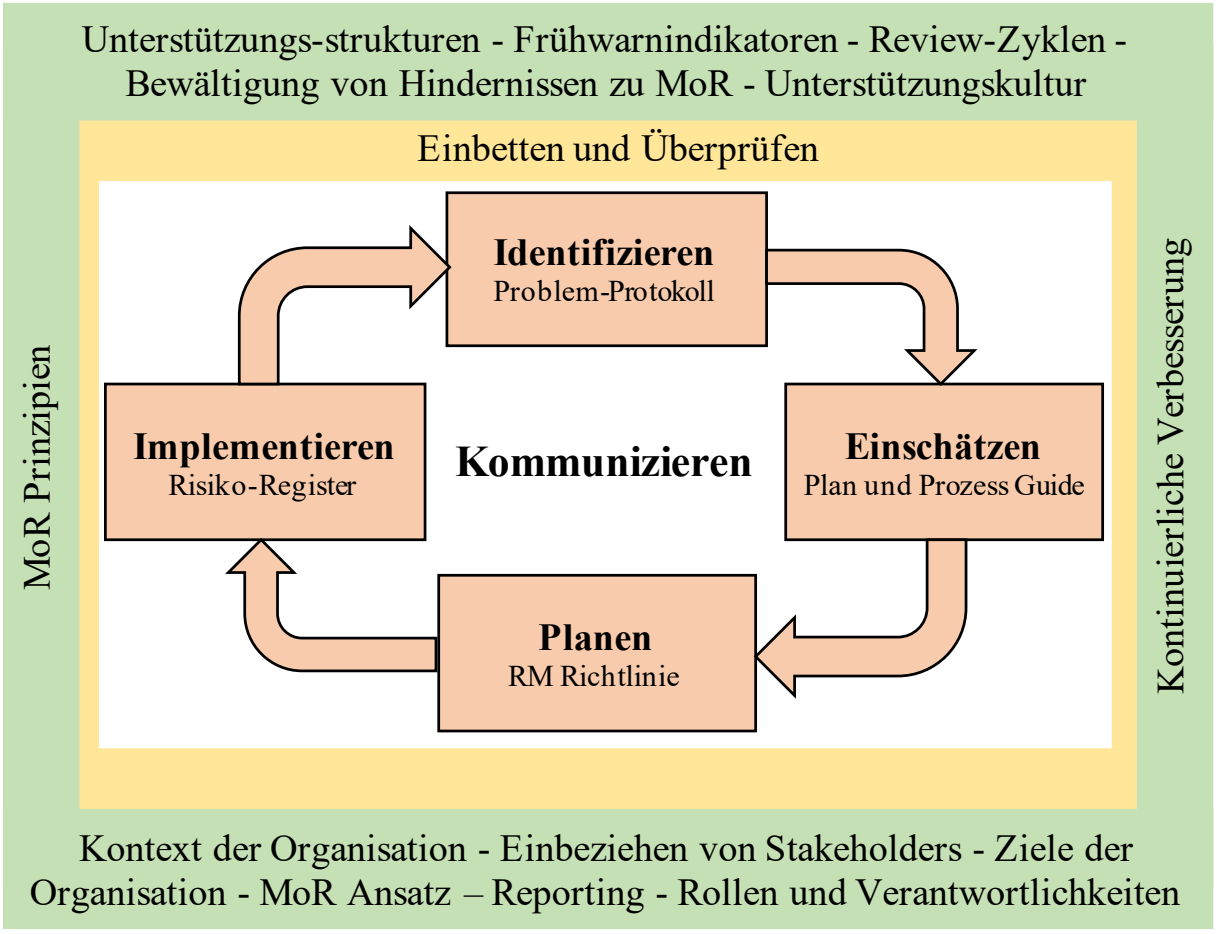
Inhalt & Vorgehen

Die genannten Kernkonzepte (Abbildung 2.15) bilden die Basis für das gesamte RM Vorgehen und beinhalten letztlich den Prozess. Die 12 Prinzipien, abgeleitet von übergeordneten Governance-Prinzipien, beschreiben grundlegende Leitsätze, welche den Rahmen für das gesamte RM bilden. Der MoR Ansatz beschreibt, wie das Vorgehen zum RM innerhalb einer Organisation implementiert werden sollte. Dazu nennt das Framework fünf allgemeine Praktiken, welche jede Organisation angemessen adaptieren muss.
Der Prozess beschreibt die vier Aktivitäten zu Durchführung des RMs, sowie deren Inputs und Outputs. Die erste Aktivität Identifizieren beinhaltet sowohl das Etablieren des organisatorischen Kontexts als auch die Risikoidentifikation. Potenzielle Bedrohungen für die Organisation sollen ermittelt und verstanden werden, um darauf aufbauend ein angemessenes Risiko-Register erstellen zu können. Diese wird in der nächsten Aktivität genutzt, um die Risikoeinschätzung durchzuführen und die Risikohöhe zu ermitteln. Dabei setzt MoR ebenfalls auf eine Bewertung basierend auf Eintrittswahrscheinlichkeit und Auswirkung, ohne dabei eine konkrete Methode vorzugeben. Basierend auf dieser Bewertung wird ein Plan erstellt, wie die Risiken konkret behandelt werden sollen. Anschließend wird der

[8] Inzwischen ist eine neue Version [126] erschienen, die allerdings in dieser Arbeit nicht verwendet wurde.

durch das Topmanagement freigegebene Plan implementiert und die neuen Maßnahmen überwacht. Das letzte Kernkonzept, Einbetten und Überprüfen, soll das RM Vorgehen konsistent in der gesamten Organisation etablieren. Dabei liegt der Fokus darauf, das risikobasierte Denkweise in die Unternehmenskultur zu integrieren.

Abbildung 2.15: MoR Kernkonzepte [In Anlehnung an 127]



2.3.8 ENISA Risk

Die ENISA betreibt Forschung für die EU im Kontext IS. Mit dem ENISA Risk Framework wurde eine Sammlung verschiedener Risikodokumente bereitgestellt.

Anwendungsbereich

Die Aktivitäten der ENISA sind an den Bedürfnissen der Mitgliedsstaaten ausgerichtet und fokussieren sich oftmals auf den Anwendungsbereich von Staaten und staatlicher Organisationen. Die Inhalte sind jedoch allgemein zugänglich und für alle Organisationen anwendbar.

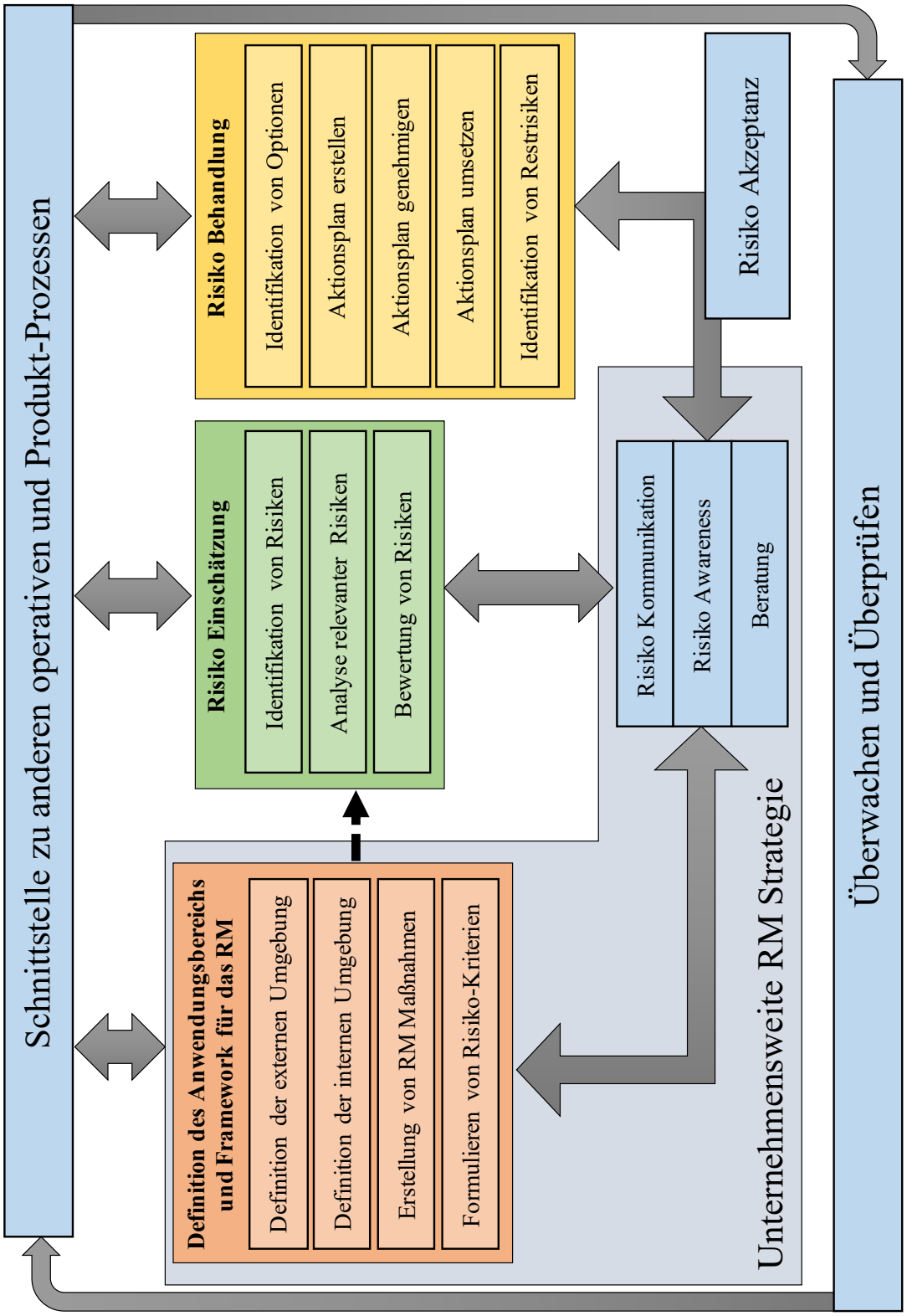
Dokumente & Struktur

Das *ENISA RM/RA Framework* [128] ist eine Sammlung von ISRM Dokumenten auf der ENISA Website. Dies enthält einen ISRM Prozess, ein Vorgehen zum Einbinden in ein ISMS, Methoden zur Risikoeinschätzung [43] und unterstützende Ressourcen (Terminologie und Templates). Weitere relevante ENISA Veröffentlichungen sind *Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment Methods and Tools* [129] zur Umsetzung des Frameworks und *Cloud Computing* [130] im Kontext SCRM. Die *Threat Landscape and Good Practice Guide for Internet Infrastructure* [131] schafft einen Überblick über die aktuelle Bedrohungslage und Risikosituation.

Inhalt & Vorgehen

Das ENISA Frameworks definiert einen ISRM Prozess bestehend aus zwei unterstützenden und drei Hauptaktivitäten, dargestellt in Abbildung 2.16. Der Prozess beginnt mit der *Definition des Anwendungsbereichs und des Frameworks*, wobei interne und externe Faktoren zur Etablierung der organisationsweiten Rahmenbedingungen berücksichtigt werden. Die nächste Aktivität beschreibt die Risikoeinschätzung, bestehend aus der Identifikation, Analyse und Bewertung von Risiken. ENISA gibt keine konkreten Methoden vor, nennt jedoch ein Asset-basiertes Vorgehen und eine Bewertung auf Basis der Eintrittswahrscheinlichkeit und Auswirkung von Ereignissen. Anschließend folgt die Risikobehandlung zum strukturierten Umgang mit Risiken. Dabei wird die Planung und Implementierung im Framework zusammengefasst. Letztlich wird ein Aktionsplan erstellt und umgesetzt, sowie alle nicht enthaltenen Risiken akzeptiert. Als unterstützende Aktivität soll eine kontinuierliche Überwachung und Kommunikation innerhalb der Organisation etabliert werden. Die dazu notwendigen Aspekte sollten bereits als Teil der unternehmensweiten RM Strategie berücksichtigt werden. Weiterhin ist es möglich, zusätzliche Schnittstellen in andere Prozesse zu etablieren.

Abbildung 2.16: ENISA ISRM Prozess [In Anlehnung an 128]



2.4 Resümee zur Kollaboration im ISRM

Existierende Ansätze

In diesem Kapitel wurden die Grundlagen des RM, relevante Teilbereiche und Rahmenwerke vorgestellt. Dabei wurde insbesondere das Thema der organisationsübergreifenden Zusammenarbeit im Kontext des RM angesprochen. Als Erweiterung des klassischen SCRM geht der vorgestellte Ansatz des Joint SCRM zur Kollaboration in Supply Chains in diese Richtung. Weitere Überlegungen für ein kollaboratives SCRM existieren bereits, sind allerdings noch nicht ausreichend stark formalisiert.

Fehlende Ansätze

Obwohl das Teilen von Informationen (*(risk) information sharing*) und entsprechende Kommunikation (*communication mechanisms*) in der Supply Chain bzw. mit den Partnern insgesamt als essenziell für das Joint (Cyber) SCRM erkannt wurde [30, 32, 132, 133, 94, 85, 86, 91, 134], existieren so gut wie keine Details zur Kollaboration oder konkrete Konzepte zur Umsetzung. Weiterhin bezieht sich die bisherige Forschung hauptsächlich auf SCRs, jedoch nicht auf Risiken innerhalb einer Allianz. Die Betrachtung der Risiken erfolgt wie beim klassischen RM aus einer organisationszentrierten Perspektive. Das bedeutet, dass SCRs zwar als zusätzliche Risiken erkannt, dabei allerdings nur die Auswirkung auf die eigene Organisation betrachtet werden. Allianzen können zwar auch im Kontext einer Supply Chain entstehen, bilden sich allerdings nicht zwangsläufig auf Basis einer Supplier-Beziehung. Insbesondere für Organisationen, welche eine engere Partnerschaft als ein klassisches Supply Chain Netzwerk eingehen, bieten sich weitere Möglichkeiten zur Zusammenarbeit. Dabei entsteht die Möglichkeit, Risiken für die Allianz als Ganzes zu identifizieren und diese gemeinsam zu behandeln.

ISRM im speziellen

Weiterhin existieren die vorgestellten Ansätze bisher hauptsächlich im Bereich des allgemeinen RM. Wenige Veröffentlichungen beschäftigen sich tatsächlich mit dem Cyber SCRM. Die Verbindung eines kollaborativen Vorgehens mit dem ISRM bzw. Cyber SCRM ist bisher noch nicht verbreitet. Nachdem sich im klassischen SCRM gezeigt hat, dass sich die Supply Chain Resilience durch engere Kollaboration erhöht, so sind diese Vorteile auch im Kontext der IS zu erwarten. Zum jetzigen Zeitpunkt existiert jedoch kein Modell dafür, wie Kollaboration oder organisationsübergreifende Zusammenarbeit im ISRM aussehen könnte.

ENISA Ressourcen

Zwar sind die bereits genannten Ansätze der ENISA zur Interoperabilität von ISRM Frameworks [37, 38] ein Schritt in diese Richtung, jedoch geht es auch hier nicht um eine Zusammenarbeit von Organisationen. Die bereitgestellten Ressourcen können dabei helfen, die Ergebnisse verschiedener Prozesse vergleichbar zu machen. Sie liefern allerdings nicht die notwendigen Grundlagen zum Aufbau eines gemeinsamen Prozess zwischen mehreren Organisationen im Sinne eines CRM.

Weitere Forschung

Zum jetzigen Zeitpunkt besteht daher weiterer Bedarf, die Forschung im Bereich kollaboratives ISRM zu vertiefen. Die vorgestellten RM Frameworks zeigen, dass die heute etablierten Konzepte und Prozesse sich zwar in der Implementierung unterscheiden, jedoch grundsätzlich nichts dagegen spricht, sie im Kontext eines kollaborativen Ansatzes zu integrieren. Im nächsten Kapitel wird daher grundlegend der Anwendungsbereich für ein solches Konzept diskutiert. Es gilt zu definieren, was die Anforderungen an ein wirksames kollaboratives Framework sind und in welchem Kontext bzw. für welche Organisationen die Kollaboration im ISRM sinnvoll ist.

Kapitel 3

Anforderungen an ISRM in strategischen Partnerschaften

Inhaltsangabe

Im vorherigen Kapitel wurden die Grundlagen der IS, des RM und der davon abgeleiteten, spezialisierten Bereiche beschrieben. Das heute in Organisationen etablierte ERM und als Teilbereich damit auch das ISRM betrachtet nur die eigene Organisation und die Risiken innerhalb dieses Geltungsbereichs. Dabei werden nur organisationsinterne Prozesse und Werte betrachtet, während alles außerhalb der Organisation als externe Bedrohungen in das RM eingeht. Die eigene Organisation steht damit im Zentrum des Bedrohungsmodells, andere Organisationen werden lediglich als Risikoquellen wahrgenommen. Eine kooperative Schnittstelle zu Dritten, etwa Lieferanten oder Partnerorganisationen, ist nicht vorgesehen.

Supply Chain Risks

Eine Weiterentwicklung bildet das genannte SCRM, bei dem zusätzlich Supplier, die Supply Chain und damit zusammenhängende Risiken (SCRs) betrachtet werden. Allerdings wird auch hier eine innere Sicht eingenommen, bei dem Drittorganisationen aus der Perspektive der Kundenorganisation betrachtet werden. Beispielsweise führt der Ausfall eines Lieferanten dazu, dass die Organisation aufgrund fehlender Hardware nicht mehr in der Lage ist, ein Produkt herzustellen. Ein Risiko, das die Organisation durch alternative Lieferanten und Lieferwege mitigieren kann. Die Frage, warum der alte Lieferant ausgefallen ist, spielt für die Risikobehandlung keine Rolle. Schließlich hat jede an der Supply Chain beteiligte Organisation nur soweit Interesse an der IS der anderen Teilnehmer, insofern sie die eigene Produktion/Dienstleistung betrifft und ein Ausfall diese gefährden würde. Somit werden nicht die Risiken der anderen Organisation berücksichtigt, sondern nur die durch den Supplier verursachten Bedrohungen bewertet.

Kollaboratives ISRM

Als Erweiterung des klassischen ISRM soll daher ein Ansatz für ein kollaboratives Vorgehen entwickelt werden, welches einen gemeinsamen Umgang mit IS-Risiken über organisatorische Grenzen hinweg ermöglicht. Die Grundidee ist es, durch Etablieren entsprechender Kommunikationsschnittstellen und Definition geteilter Prozessartefakte einen verteilten Prozess zu realisieren. Ein solcher Ansatz kann eine Lösung für die vorgestellte Problematik (Kapitel 2.4) der fehlenden kooperativen Möglichkeiten im ISRM liefern, welche auf die Limitierungen im Anwendungsbereich des klassischen ERM zurückzuführen ist. Diese Erweiterung des klassischen ISRM und Weiterentwicklung des SCRM zu einem verteilten Prozess wird im Folgenden als Collaborative Information Security Risk Management (CISRM) bezeichnet.

Szenarien

In diesem Kapitel wird nun genauer auf die konkrete Zusammenarbeit eingegangen und welche Szenarien bei der Zusammenarbeit von Organisationen in der Praxis existieren. Dazu werden verschiedene Szenarien vorgestellt, die zwar alle enge Partnerschaften sind, aber eine unterschiedliche Dynamik in der Zusammenarbeit aufweisen (Abschnitt 3.1). Der Hauptunterschied liegt dabei in den verschiedenen Organisationsstrukturen, die gewählt wurden, um die Allianz zu etablieren. Dadurch ergeben sich auch andere Konstellationen von Macht und Vertrauen. Die beschriebenen Allianzen bilden organisatorische Prototypen, in denen das in dieser Arbeit entwickelte kollaborative Framework zum Einsatz kommen soll.

GÉANT

Anschließend wird das GÉANT Projekt vorgestellt, welches in dieser Arbeit als Fallbeispiel dienen soll (Abschnitt 3.2). Dabei handelt es sich um eine existierende Kollaboration unabhängiger Organisationen in ganz Europa. Es wird sowohl der Aufbau des Projektes erklärt als auch dessen relevante Eigenschaften genauer beschrieben. Ein Ausblick zeigt,

wie diese Gemeinschaft von einem gemeinsamen CISRM profitieren könnte.

Eigenschaften des CRM

Es folgt ein Blick in übergeordneten Themenbereich des RM. Auf dieser Ebene gibt es bereits Untersuchungen, wie mehrere Organisationen im RM oder SCRM im Kontext eines CRM enger zusammenarbeiten können. Sie liefern damit allgemeine Rahmenbedingungen, die auch im ISRM adaptiert werden könnten.

Anforderungen

Die identifizierten Kerneigenschaften des CRM sollen somit als Erfolgsfaktoren für das CISRM genutzt werden (Abschnitt 3.3). Dazu werden ihnen zugrunde liegende Ziele abgeleitet und auf das ISRM angewendet. Diese führen mit Hilfe der vorgestellten Kollaborationsformen letztlich zu Anforderungen an ein kollaboratives Framework und bilden die Grundlage für das weitere Vorgehen.

Konzept

Letztlich wird am Ende des Kapitels ein Konzept zu Erstellung des geplanten Meta-Frameworks vorgestellt (Abschnitt 3.4). Ziel ist es ein Vorgehen für den Aufbau eines CISRM zu beschreiben, welches alle für einen kollaborativen Prozess notwendigen Komponenten enthält und dabei die zuvor definierten Anforderungen berücksichtigt. In den nachfolgenden Kapiteln wird das Framework gemäß diesem Konzept entwickelt.

Definitionen

Die Vielzahl von Begriffen für Kooperationen und ähnliche partnerschaftliche Beziehungen zwischen Organisationen und deren Vermischung führt schnell zu unübersichtlichen Formulierungen. Daher wird als generische Bezeichnung für alle Formen von organisationsübergreifenden Beziehungen nachfolgend der Begriff Interorganisational Relationship (IOR) verwendet (Def. 3.1). Weiterhin werden die Teilnehmer einer solchen Beziehung zukünftig als Partnern bezeichnet (Def. 3.2), unabhängig davon, ob es sich um eine kurz- oder langfristige Partnerschaft handelt.

Definition 3.1: Interorganisationale Beziehung

Eine Interorganisational Relationship (IOR) bezeichnet eine allgemeine Beziehung zwischen zwei oder mehr Organisationen, unabhängig von der Art oder Ausprägung der organisationsübergreifenden Zusammenarbeit.

Definition 3.2: Partner

Ein Partner bezeichnet eine an einer IOR (Def. 3.1) teilnehmende Organisation.

3.1 Kollaborationsszenarien im ISRM

Auf höchster Ebene lassen sich IORs auf Basis der vorherrschenden Beziehungsform typisieren. Klassische Beziehungen gehen dabei jedoch nur von einer begrenzten Interaktion zwischen den Organisationen aus. Möglich wäre eine abstrakte Einteilung der Beziehung in eine Solidaritätsgemeinschaft, Hierarchie oder eine Art freien Markt. Als direkte Ausprägungen von Allianzen werden die Föderation und das Unternehmensnetzwerk mit Variationen wie dem Konsortium, dem Joint Venture, der Fusion und dem Unternehmenssystem genannt. Auch können Organisationsformen dazwischen angesiedelt sein. [135]

Ausprägungen

Im Folgenden werden drei in der Industrie verbreitete IOR Szenarien beschrieben, die grundsätzlich geeignet erscheinen, in verschiedenen Bereichen wie auch dem ISRM zusammenarbeiten zu können. Neben diesen drei Beispielen existieren in der Industrie noch weitere Anwendungsfälle zu den Kollaborationsszenarien, wie die oben genannten Varianten. Trotz mancher Unterschiede bei der Struktur oder Ausprägung bestimmter Aspekte, lassen sich die meisten davon jedoch als einer der drei generischen Typen klassifizieren. Dabei handelt es sich um Joint Ventures als projektbasierte Zusammenarbeit, Verbünde als Bund unabhängiger Organisationen im Kontext einer strategischen Initiative und Konzerne als Verbund wirtschaftlich zusammenhängender aber unabhängig agierender Unternehmen. Jede dieser Kollaborationsformen wird kurz erklärt und anschließend auf ihre Besonderheiten bei der Anwendung eines CISRM eingegangen.

Gemeinsame Risiken

Cropper et al. [136] betrachten in IORs zwei verschiedene Ebenen, die der individuellen Organisation und dem Kollektiv aller Organisationen. Sie nutzen die Begriffe Mikro-Kontext für alles unterhalb einer Organisationen (Gruppen, Individuen) und Makro-Kontext für alles oberhalb der Beziehung (z.B. Recht, Politik, Wirtschaft). In Bezug auf das RM existiert bereits eine ähnliche Unterscheidung in Makro- und Mikro-Risiken. Dabei betreffen Mikro-Risiken eine einzelne Organisation und Makro-Risiken eine ganze Industrie, Branche oder geopolitische Region. In dieser Einteilung könnten die Allianz betreffende Risiken dann konsequent als Meso-Risiken bezeichnet werden. Beide Ebenen, Mikro-Risiken der Organisation und Meso-Risiken der Allianz sollten im CISRM betrachtet werden. Da in dieser Arbeit nur diese zwei klar definierten Risiken relevant sind, werden im Folgenden die Abkürzungen Risiko der Allianz (RA) und Risiko der Organisation (RO) verwendet.

Definition 3.3: Risiko der Organisation (RO)

Bezeichnet ein IS-Risiko, welches Auswirkungen auf eine einzelne Organisation innerhalb der Allianz (Def. 4.9) hat.

Definition 3.4: Risiko der Allianz (RA)

Bezeichnet ein IS-Risiko, welches die Allianz (Def. 4.9) bzw. alle Partner (Def. 3.2) betrifft.

3.1.1 Joint Venture

Definition

Ein *Joint Venture* bezeichnet einen „Zusammenschluss von Unternehmen zum Zweck der gemeinsamen Durchführung von Projekten“ [137]. Die Grundidee dieser Kollaboration ist es, dass verschiedene Organisationen einen Teil ihrer Aktivitäten in eine gemeinsame Unternehmung auslagern. Durch diese können sich die Beteiligten entweder Aufwände sparen, da sie nicht selbst die kompletten Kosten tragen müssen oder jeweils das Wissen der Anderen benutzen, welches nicht in der eigenen Organisation vorhanden ist. Diese Zusammenarbeit ist damit ein gutes Beispiel für den Vorteil der geteilten Ressourcen zur Durchführung von großen oder komplexen Projekten. Das Joint Venture ist auch gleichzeitig die schwächste Form der kollaborativen Beziehung, da sich die Zusammenarbeit auf die Durchführung eines konkreten Projektes beschränkt.

Arten von Join Ventures

Grundsätzlich ist jedes Joint Venture eine rechtlich und organisatorisch selbständige Unternehmung (Projekt oder Organisation) mehrerer unabhängiger Organisationen. Allerdings lassen sich diese noch einmal anhand der Art der Zusammenarbeit unterscheiden. Beim *Equity Joint Venture* wird ein eigenständiges Unternehmen gegründet, welches zukünftig bestimmte Aufgaben für alle Beteiligten übernimmt. Dabei sind die Partner finanziell an der gemeinsamen Organisation beteiligt, wodurch sich unterschiedliche Abhängigkeits- und Machtverhältnisse ergeben können. Das *Contractual Joint Venture* stellt dagegen kein eigenes Unternehmen dar, sondern bezeichnet lediglich eine Zusammenarbeit der Partner zur gemeinsamen Durchführung bestimmter Aktivitäten. Eine Sonderform ist auch das *Internationale Joint Venture*, an dem die Partner aus verschiedenen Staaten beteiligt sind. [138]

Beispiel Joint Venture

Ein gutes Beispiel für beide Formen des Joint Ventures liefert der Automobilhersteller Mercedes-Benz. So hat dieser mit der BMW Group eine gemeinsame Unternehmung im Bereich Car-Sharing gestartet und dazu die gemeinsame Firma Share Now [139] gegründet. Diese Gründung einer kollaborativen Organisation stellt ein Equity Joint Venture dar. Weiterhin hat der Konzern auch ein Beispiel für ein Contractual Joint Venture. Dazu zählt der Zusammenschluss mit dem Technologiekonzern Google zur gemeinsamen Herstellung von Hightech-Autos [140], bei dem die Unternehmen eine strategische Partnerschaft eingegangen sind, jedoch keine neue Firma gegründet haben.

CISRM in Joint Ventures

Egal, ob es sich nun um ein kapital- oder vertragsbasiertes Joint Venture handelt, arbeiten die Partner kollaborativ an bestimmten Aktivitäten. Sie sind damit direkt von den Risiken betroffen, die diese gemeinsame Unternehmung mit sich bringt. Dies unterscheidet sich allerdings noch nicht von normalen Projektrisiken, die im Kontext des Projektmanagements betrachtet werden sollten. Da jedoch alle Partner finanziell und organisatorisch an der Durchführung beteiligt sind, haben Risiken jedes Partners auch indirekt Auswirkungen auf die Zusammenarbeit. Es ist jedoch anzunehmen, dass dies beim Equity Joint Venture weniger relevant ist, da die gegründete Organisation grundsätzlich unabhängig agiert und nicht direkt von den Partnern beeinflusst ist. Somit macht CISRM vor allem in einem Contractual Joint Venture Sinn, egal ob national oder international.

Zusammenspiel

Per Definition sind die Teilnehmer des Joint Ventures bereits an der Führung und Steuerung der Unternehmung beteiligt, wobei jeder Partner über Einfluss und Entscheidungskompetenz verfügt. Die Organisationen selbst sind jedoch unabhängig und arbeiten nur in bestimmten Aktivitäten zusammen. Sie werden ihre internen Managementprozesse daher nicht aneinander anpassen wollen oder können. Somit besteht die Möglichkeit, durch ein übergeordnetes CISRM alle Partner in den Umgang mit Risiken einzubinden.

3.1.2 Verbund

Definition

Verbünde sind eine weitere Art der Zusammenarbeit, wobei der Begriff nur sehr wenig Informationen darüber gibt, wie diese tatsächlich stattfindet. Tatsächlich beschreibt der Verbund nur eine Gruppe von unabhängigen Organisationen, die sich zur wirtschaftlichen Kooperation zusammenschließen. Der Begriff wird jedoch nicht eindeutig definiert oder einheitlich verwendet. Eine deutlich konkretere Beschreibung liefert die Föderation. Sie bezeichnet ein „Bündnis zwischen Staaten [oder einen] Zusammenschluss von Organisationen“ [141]. Eine Föderation ist damit ein Beispiel für einen Verbund von wirtschaftlich unabhängigen Organisationen zu einer strategischen Allianz, bei der gleichberechtigt und weitgehend autonom gearbeitet wird. Föderationen können vielfältig sein und sehr große, internationale Allianzen bilden. Eine weitere bekannte Bezeichnung für einen Verbund von Organisationen ist das Konsortium, ein „vorübergehender Zusammenschluss von Unternehmen, besonders Banken, zur gemeinsamen Durchführung eines größeren Geschäfts“ [142]. Die Konditionen dieser Verbindung sind formaljuristisch definiert und werden im Weiteren nicht genauer betrachtet.

Bildung eines Verbunds

Entschließen sich Organisationen zu dieser Form der Kollaboration, dann geschieht dies normalerweise freiwillig. Die Organisationen haben bereits eine Beziehung zueinander, die entsprechende Nähe für eine Kollaboration aufweist. Soll nun insbesondere die Innovationskraft gesteigert und das Teilen von Informationen gefördert werden, ist die Gründung eines Verbunds sinnvoll. Eine weitere Möglichkeit, warum Organisationen einen Verbund eingehen, ist das Mandat. Dabei wird die Zusammenarbeit der Unternehmen einer bestimmten Branche von staatlicher Stelle erzwungen. Im Unterschied zum Joint Venture ist es die deutlich breitere Kollaboration mit Interaktionen in verschiedenen Bereichen. Da ein Joint Venture sich eher auf eine bestimmte Aktivität beschränkt, scheint es für eine branchenübergreifende Zusammenarbeit eher ungeeignet. Es ist also denkbar, dass die Organisationen sich zu einem Verbund zusammenschließen.

CISRM in Verbünden

Föderationen als Zusammenschluss unabhängiger Organisationen, mit dem Ziel gemeinsam Produkte oder Dienstleistungen zu erbringen, sind prädestiniert für das kooperative Management von Risiken. Die Teilnehmer sind mindestens von Risiken betroffen, welche die gemeinsamen Aktivitäten betreffen. Da diese allerdings vielfältig sein können und sich über diverse Interaktionen im ganzen Unternehmen erstrecken, können verschiedenste Risiken der Partner direkten und indirekten Einfluss auf die eigene IS haben. Wie auch beim Contractual Joint Venture fehlt in Föderationen allerdings eine übergeordnete, steuernde Instanz. Daher ist es grundsätzlich schwierig ein gemeinsames ISRM zu implementieren, welches auf einer Angleichung der Vorgehensweisen beruht.

Beispiel Verbund

Ein Beispiel für eine staatliche Föderation ist die Europäische Union als Bündnis unabhängiger Nationalstaaten mit einer gemeinsamen Vision, Mission und der Kollaboration bei der Zielerreichung. Deutlich relevanter für diese Arbeit sind jedoch Verbünde als Zusammenschluss von Organisationen. Hier könnte man etwa Kooperationen öffentlicher Institutionen betrachten, die als unabhängig agierende Organisationen trotzdem gemeinsame Ziel verfolgen. Ein gutes Beispiel sind auch regionale Verkehrsverbünde als Zusammenschluss unabhängiger privater und öffentlicher Verkehrsgesellschaften. Die spezialisierten Leistungen und Produkte der Partner werden dem Kunden als kombinierte Dienstleistung angeboten, häufig unter einem gemeinsamen Markenkern. Im Großraum München werden diese Produkte etwa vom Münchner Verkehrs- und Tarifverbund (MVV) angeboten, welcher als Verbund (Allianz) nur koordinierende Aufgaben übernimmt, während die Leistungen von unabhängigen Verkehrsunternehmen (Partnern) erbracht werden [143]. Die Zusammenarbeit ist dabei sehr umfangreich und betrifft viele der von den Organisationen bereitgestellten Leistungen wie Fahrzeuge oder IT-Services. Dabei bleiben alle Organisationen unabhängig bei der Erbringung ihrer Dienstleistungen, müssen sich allerdings an gemeinsam aufgestellte Richtlinien orientieren.

3.1.3 Konzern

Als drittes Szenario ist ein Konzern bestehend aus verschiedenen Unternehmen denkbar, welche zwar zusammengehörig sind, jedoch unabhängig voneinander auftreten und agieren. Per Definition ist ein Konzern ein „Zusammenschluss von Unternehmen zu einer wirtschaftlichen Einheit, bei der die jeweilige rechtliche Selbstständigkeit nicht aufgegeben wird“ [144]. Für die einzelnen Unternehmen ist die Konzernstruktur damit nichts anderes als eine Form der Partnerschaft. Im Gegensatz zu den Verbünden existiert bei Konzernen grundsätzlich eine hierarchische Beziehung. Eine übergeordnete Muttergesellschaft, auch Dachorganisation oder Holding, steht dabei an der Spitze und hält einen Mehrheitsanteil an untergeordneten Tochtergesellschaften.

Abhängigkeiten

Durch die Konstellation ergibt sich ein formales Abhängigkeitsverhältnis zwischen den Tochtergesellschaften und der Muttergesellschaft. Obwohl es eine hierarchische Struktur im Konzern gibt, stehen die einzelnen Tochtergesellschaften erst einmal in keinem direkten Verhältnis zueinander. Die Dachorganisation kann jedoch jederzeit verbindliche Vorgaben machen und Richtlinien oder Prozesse für den gesamten Konzern einführen. So ist es grundsätzlich möglich, eine ähnlich starke Koordinationsstruktur wie bei einem Einzelunternehmen zu etablieren. So stärker die Dachorganisation jedoch ihre Kompetenzen ausnutzt, desto schwächer werden die Vorteile einer solchen verteilten Unternehmensstruktur, bei der die entkoppelten Unternehmen eigentlich flexibel und eigenverantwortlich agieren sollten. Damit gibt es grundsätzlich verschiedene Möglichkeiten, ein konzernweites ISRM zu gestalten. Letztlich ist der Konzern direkt von allen Risiken der Tochtergesellschaften betroffen und hat ein starkes Interesse daran, diese zu koordinieren.

Klassisches ISRM im Konzern

Durch die klaren Hierarchien, die von einer Dachorganisation gesteuert werden, bietet sich ebenso die Etablierung eines zentralen RM. Die Grundvoraussetzung dafür ist, dass die Muttergesellschaft dafür notwendige strategische und operative Vorgaben an die Tochterunternehmen macht. Dabei könnten entweder strikte Vorgaben für das ERM der einzelnen Organisationen festgelegt werden oder ein einziges konzernweites ERM etabliert werden, welches das RM für alle Teile des Konzerns übernimmt. Auch eine Mischform beider Ansätze ist denkbar, bei der jede Organisation weiterhin ein eigenes, unabhängiges ERM betreibt und ausgewählte Risiken in einem zentralen ERM für den Konzern verwaltet werden. Es ist zu erwarten, dass ein solches Vorgehen effizienter ist als ein lose gekoppeltes CISRM, da alle notwendigen Methoden, Prozesse und Verfahren identisch und optimal aufeinander abgestimmt sind. Durch die Auswahl und Festlegung eines einzelnen RM Frameworks im Konzern ist sichergestellt, dass alle Organisationen die gleiche Vorgehensweise und Terminologie verwenden. Allerdings bringt ein solches Vorgehen auch Nachteile mit sich. So ist ein zentrales Management der RM Vorgaben erforderlich, was einen administrativen Overhead erzeugt. Durch die Vorgabe aller Komponenten des RM ist dieses, abhängig von der Heterogenität innerhalb des Konzerns, eventuell nicht optimal an die Bedürfnisse der einzelnen Organisationen angepasst.

CISRM im Konzern

Auf der anderen Seite besteht auch hier die Möglichkeit, ein konzernweites CISRM einzuführen. Dabei können die Tochtergesellschaften weiterhin unabhängig voneinander agieren und trotzdem ein gemeinsames ISRM etablieren. Ob und wie stark dabei die Rolle der Muttergesellschaft ausgeprägt sein soll, kann je nach Bedarf entschieden werden. Auf diese Weise bleiben die Vorteile der unabhängigen Unternehmen erhalten und trotzdem die Risikobehandlung im Konzern abgestimmt werden.

3.2 Fallbeispiel: Das GÉANT Projekt

Die drei vorgestellten Typen, das Joint Venture, der Verbund und der Konzern decken ein breites Spektrum an Kollaborationsszenarien in der Wirtschaft ab. Im Folgenden wird eine weitere IOR vorgestellt, bei der es sich ebenfalls um ein reales Beispiel aus der Praxis handelt. Dabei wird im Detail auf die Struktur der Allianz, deren Eigenschaften und die Möglichkeiten für gemeinsames ISRM zwischen den Partnern. Die Allianz wird im Kontext dieser Arbeit als Fallbeispiel verwendet, an dessen Beispiel später der Aufbau des CISRM skizziert werden soll (Kapitel 8.2).

GÉANT

Die für das Fallbeispiel ausgewählte IOR ist das *GÉANT Projekt*, welches dem Autor aus der eigenen Praxiserfahrung bekannt ist[1]. Dabei handelt es sich um eine internationale Allianz aus dem Bereich Research & Education (R&E). Das *GÉANT Projekt* [145] ist dabei ein Zusammenschluss von nationalen Institutionen in Europa, den sogenannten National Research and Education Networks (NRENs). Innerhalb dieser Allianz arbeiten die Partner in verschiedenen Bereichen zusammen, entwickeln gemeinsam Produkte und betreiben übergreifende Services. Es liefert damit potenziell eine sehr gute Umgebung für verschiedenste interorganisationale Aktivitäten.

Aktivtäten

Aktuell kollaborieren die Partner im Kontext von GÉANT bereits bei mehreren Aktivitäten. Ein großer Bereich ist der Aufbau und die Pflege eines europäischen Forschungsnetzes, das Hochleistungsverbindungen zwischen den einzelnen NRENs etabliert. Der andere Bereich ist die Entwicklung und Bereitstellung von Dienstleistungen auf Basis dieses Netzes. Dazu gehören sowohl konkrete Software-Services, sowie gemeinsame Initiativen in den Bereichen Marketing, Infrastruktur und Security. Formal sind das physische Netz und die gemeinsamen Dienstleistungen zwar separate Teilprojekte (aktuell GN5-1 und GN5-1N), das spielt für die Zusammenarbeit an sich jedoch keine Rolle, weshalb im Weiteren nicht zwischen diesen unterschieden wird.

ISRM

Das GÉANT Projekt bietet sich als IOR zur genaueren Betrachtung an, da es bereits erste interorganisationale Aktivitäten in Bezug auf die IS gibt. Diese beschränken sich jedoch größtenteils auf den Bereich Training und Awareness, insbesondere auf gemeinsame Veranstaltungen und die Bereitstellung von Schulungsmaterial. Weiterhin werden gemeinsame Softwareprodukte entwickelt, welche die Sicherheit der Partner verbessern sollen. Im ISM existieren auch erste Ansätze einer Zusammenarbeit, etwa durch die Erstellung gemeinsamer Standards oder einer übergreifenden Kommunikation von Schwachstellen.

Überblick

Dieser Abschnitt liefert einen Überblick über das GÉANT Projekt. Dabei werden dessen Aufbau und Struktur erklärt, um zu verstehen, wie die Partner (NRENs) zusammenarbeiten. Anschließend werden die Eigenschaften und Besonderheiten der Allianz beschrieben, die sich aus dieser Struktur ergeben. Letztlich wird diskutiert, welche Perspektiven eine Kollaboration im ISRM einer interorganisationalen IOR wie dem GÉANT Projekt bieten könnte.

[1] Der Autor ist seit 2017 selbst aktives Mitglied des GÉANT-Projektes (GN4-2, GN4-3, GN5-1) und arbeitet seitdem als Vertreter von DFN/LRZ in den Bereichen Trust & Identity sowie Security.

3.2.1 Aufbau und Struktur

Das GÉANT Projekt, im weiteren nur GÉANT, setzt sich aus verschiedenen Teilen und Organisationen zusammen. Diese nehmen verschiedene Rollen innerhalb der IOR ein. Dazu gehören die NRENs als Partner, deren nationale Institutionen als Kunden und der GÉANT Assoziation als Koordinator.

NREN

Die NRENs sind die Partner innerhalb der IOR. Bei ihnen handelt es sich um Organisationen verschiedenster Art und Größe, die je nach Staat verschiedene Rechtsformen annehmen können. Meist sind es jedoch gemeinnützige (non-profit) Organisationen, die sich aus ihren Mitgliedern oder staatlichen Förderungen finanzieren. Ein NREN stellt die nationale Forschungsinfrastruktur eines Landes bereit. In Deutschland ist dies der „Verein zur Förderung eines Deutschen Forschungsnetzes“ [146], kurz als Deutsches Forschungsnetz (DFN) bezeichnet. Mit Ausnahme weniger Spezialfälle existiert in jedem Land genau ein NREN. Diese liefern die Infrastruktur und zugehörigen Services an ihre Mitglieder, d.h. die Institutionen in ihrem Land. Viele der von den NRENs genutzten und gelieferten Services werden wiederum gemeinsam mit den Partnern in GÉANT entwickelt und betrieben.

Institutionen

Zu den Institutionen zählen Organisationen aus dem Bereich der Lehre (Schulen und Hochschulen) und Forschung (öffentliche und private Forschungseinrichtungen). Welche Organisationen genau von den NRENs versorgt werden unterscheidet sich von Land zu Land. Die Institutionen sind letztlich die Kunden der NRENs und nutzen die von ihnen bereitgestellten Services, wie etwa das nationale Forschungsnetz. Abhängig von der Organisationsform sind die Institutionen oftmals auch Teil oder Teilhaber der NRENs. Der DFN ist etwa als gemeinnütziger Verein strukturiert und die Mitgliedschaft steht allen deutschen Hochschulen sowie forschungsnahen Wirtschaftsunternehmen offen [146]. Durch diese einheitliche Kundengruppe ergibt sich eine weitere Gemeinsamkeit der NRENs.

Projekt

Das GÉANT Projekt selbst stellt die Allianz dar. Die NRENs arbeiten in diesem Kontext gemeinsam an Leistungen für sie selbst und ihre Kunden, wodurch sich eine starke Beziehung zwischen den Partnern ergibt. Wie bereits der Name impliziert, ist diese IOR projektbasiert strukturiert, d.h. die Laufzeit der Zusammenarbeit ist fest definiert. Jede Projektphase wird finanziert durch die Europäische Kommission im Rahmen der „Horizon“ Förderprogramme [147, 148]. Dies kann jedoch eher als Besonderheit der Finanzierung gesehen werden. Da GÉANT in verschiedenen Phasen bereits seit über 20 Jahren läuft, kann durchaus von einer langfristigen Zusammenarbeit im Sinne einer strategischen Allianz gesprochen werden. Zusätzlich wurde eine gemeinsame, projektübergreifende Organisation gegründet, was für eine intensive Beziehung spricht.

Association

Diese Organisation ist die GÉANT Association [149] mit Sitz in Amsterdam. Dabei handelt es sich um einen Verein, dessen Mitglieder wiederum die Europäischen NRENs sind. Er wurde genau aus dem Grund gegründet, um eine von der Projektstruktur unabhängige Kollaboration zu ermöglichen. Die Association agiert als juristische Person übernimmt die Verantwortung für den Betrieb der GÉANT Services. Somit könnte man das Projekt und die Association grundsätzlich als zwei unabhängige IORs betrachten (was im nächsten Teilabschnitt genauer besprochen wird). Im Kontext des GÉANT Projektes ist die Association wiederum ein Partner und nimmt aktiv an der Zusammenarbeit teil.

3.2.2 Eigenschaften der Allianz

Bei GÉANT handelt es sich demnach um eine strategische Allianz aus nationalen NRENs. Die internationale IOR dient dazu, den Partnern gemeinsame Aktivitäten zu ermöglichen, um den gemeinsamen Zielbereich R&E und deren Kunden zu unterstützen.

Organisationsform

Gemäß den vorher vorgestellten Szenarien (Abschnitt 3.1) kann das GÉANT Projekt als ein *Contractual Joint Venture* betrachtet werden. Die NRENs haben dieses als gemeinsame Unternehmung gegründet, um zusammen Aktivitäten durchführen und sich gegenseitig bei der Zielerreichung unterstützen zu können. Trotzdem bleiben die einzelnen NRENs wirtschaftlich unabhängige Organisationen, diese treten weiterhin selbständig auf (kein Verbund) und es wird keine gemeinsame Organisation gegründet. Davon getrennt zu betrachten ist die GÉANT Association, bei der es sich tatsächlich um einen *Verbund* handelt. Die Association ist im vollständigen Besitz seiner Kernmitglieder, d.h. der 36 EU NRENs [149]. Dies ist ein Vorteil, da in einem *Contractual Joint Venture* kein Partner als vertretende, juristische Person auftreten kann. Mit Hinblick auf das Projekt ist die Association jedoch auch wiederum nur als koordinierender Partner zu betrachten, da dieses vollständig von der EU finanziert und von den NRENs ausgeführt wird. Im Folgenden liegt daher der Fokus auf dem GÉANT Projekt als IOR.

Eigenschaften

Im Gegensatz zu einer einzigen Organisation oder einer einfachen Lieferantenbeziehung ergeben sich aus der Struktur der Allianz verschiedene Einschränkungen. Diese sind nicht speziell für das GÉANT Projekt, sondern sind repräsentativ für diese Art der interorganisationalen Zusammenarbeit. Zu den besonderen Eigenschaften der IOR gehören:

- **Autorität:** Es gibt keine übergreifende Autorität, d.h. eine Organisation die für alle Partner verbindliche Entscheidungen treffen könnte.
- **Aktvitäten:** Die Partner können sich an den gemeinsamen Aktivitäten beteiligen, müssen das allerdings nicht.
- **Freiheit:** Die Partner unterliegen keinem Zwang, die in der Allianz produzierten Ergebnisse auch zu nutzen.
- **Beziehung:** Jeder Partner hat zu jedem Zeitpunkt die Möglichkeit, die Allianz auch wieder zu verlassen.

Auswirkung

Aufgrund der fehlenden übergreifenden Autorität können keine zentralen Vorgaben gemacht werden. Alle Regelungen, die innerhalb der Allianz gelten sollen, müssen auch von allen Partnern akzeptiert und mitgetragen werden. Weiterhin basiert die Beziehung darauf, dass die Partner zusammenarbeiten wollen, sie müssen dies jedoch nicht. Das heißt, es kann nicht davon ausgegangen werden, dass sich jeder Partner an gemeinsamen Aktivitäten beteiligen will, insbesondere wenn ihm diese keinen Mehrwert liefern (dies könnte in anderen IORs jedoch vertraglich festgelegt sein). In diesem Zusammenhang sind die Partner auch frei bei der Entscheidung, ob sie gemeinsam erstellte Produkte oder von der Allianz bereitgestellte Services nutzen möchten. Letztlich bleiben die Partner wirtschaftlich unabhängige Organisationen, somit kann jeder Partner die Beziehung einseitig beenden, falls ihn nicht vertragliche oder gesetzliche Regelungen davon abhalten.

3.2.3 Kollaboration im ISM

Vor dem Hintergrund dieser IOR stellt sich nun die Frage, wie die NRENs im ISRM zusammenarbeiten können. Dabei sind die genannten Eigenschaften der Allianz zu berücksichtigen, die sich von den Anforderungen einer einzelnen Organisation unterscheiden.

Abhängigkeit

Innerhalb von GÉANT besteht eine besondere Abhängigkeit zwischen den Partnern, da diese alle auf die gemeinsam entwickelten und betriebenen Services angewiesen sind. Neben dem physischen Netz, das die NRENs zum Aufbau des eigenen nationalen Forschungsnetzes benötigen, gehören dazu insbesondere die gemeinsamen IT-Services. Dabei entwickelt und betreibt die Allianz viele verschiedene Services die direkt von den Partnern genutzt oder an deren Kunden weitergegeben werden. Einige dieser Services, wie beispielsweise eduGAIN [150] oder eduroam [151], sind fester Bestandteil des Serviceportfolios der NRENs und können ohne die Allianz nicht erbracht werden. Somit besteht eine starke, gegenseitige Abhängigkeit zwischen den Partnern.

Security

Wie beschrieben existieren aktuell bereits erste Initiativen innerhalb der Allianz, auch im ISM zusammenzuarbeiten. So werden gemeinsame Security Awareness Kampagnen und Trainings erstellt [152, 153], die allen Partnern zur Verfügung stehen und das Sicherheitsniveau jeder einzelnen Organisation verbessern sollen. Weiterhin wurden best practices zum Aufbau eines Security Operations Centers in R&E sowie interoperable Werkzeuge für Security Operations und Schwachstellenanalysen bereitgestellt [154, 155]. Auch im Bezug auf die IS Governance gab es bereits Anstrengungen, gemeinsame Sicherheitsstandards und Frameworks [156, 157, 158] für die Allianz zu definieren. Somit gibt es zwar einige Aktivitäten zur Kooperation im ISM, aber diese gehen meist nicht über die Bereitstellung von Werkzeugen, Anleitungen oder anderer gemeinsamer Ressourcen hinaus. Konkrete ISM Prozesse, die von mehreren NRENs übergreifend etabliert werden, gab es bisher nicht.

ISRM

Dabei scheint die Allianz durchaus geeignet, um interorganisationale Prozesse zu etablieren. In Bezug auf das ISRM gibt es bereits viele Gemeinsamkeiten zwischen den Partnern. So besteht die Allianz aus Organisationen mit einer vergleichbaren Struktur, welche alle derselben Branche (R&E) angehörigen. Somit sollte auch die Bedrohungslage der Partner durchaus miteinander vergleichbar sein. Auch besitzen diese mit den übergreifenden Services auch gemeinsame Assets, die von diesen Bedrohungen betroffen sein können. Gleichzeitig sind die Partner durch die gegenseitige Abhängigkeit auch von Störungen der Anderen betroffen. Dies geht über reine SCRs hinaus, da die Partner sowohl als Lieferanten als auch als Kunden in der Allianz auftreten und ein NREN nicht einfach ‚ausgetauscht' werden kann, was im SCRM eine übliche Maßnahme wäre. Die Partner haben somit ein intrinsisches Interesse daran, dass alle Teilnehmer der Allianz über ein möglichst hohes Sicherheitsniveau verfügen. Da in der Allianz bereits einige gemeinsame Projekte und Aktivitäten realisiert werden, insbesondere bei technischen Sicherheitsmaßnahmen, ist die Ausweitung auf die gemeinsame Risikobehandlung naheliegend.

CISRM

Was dazu jedoch fehlt, ist erst einmal ein Prozessmodell für das gemeinsame Vorgehen im ISRM. Hier kommt das CISRM und das kollaborative Framework ins Spiel, welches alle dazu notwendigen Komponenten bereitstellen soll. Ob das und wie das erfolgreich sein kann, wird am Ende der Arbeit am Beispiel des GÉANT Projektes detailliert beschrieben.

3.3 Erfolgsfaktoren für ein CISRM-Framework

Nachdem nun drei potenzielle Szenarien (Abschnitt 3.1) identifiziert und ein Fallbeispiel (Abschnitt 3.2) beschrieben wurden, in denen CISRM sinnvoll anwendbar wäre, sollen nun dessen Rahmenbedingungen dafür spezifiziert werden. Dazu werden im Folgenden die generellen Eigenschaften des kollaborativen RM, dem CRM, untersucht. Diese sollen Aufschluss darüber geben, welche organisatorischen Fähigkeiten das ISRM im Kontext einer IOR liefern muss. Letztlich wird diese Arbeit alle Bausteine zum Aufbau eines CISRM liefern, um Organisationen bei der Etablierung eines gemeinsamen Prozesses unterstützt. Somit bilden die identifizierten Fähigkeiten die Grundlage für das, was ein dazu geeignetes Framework liefern muss.

3.3.1 Eigenschaften des kollaborativen RM

Friday et al. [29] untersuchen in ihrem umfassenden Literaturreview Veröffentlichungen über 20 Jahre hinweg zum Thema CRM. Dabei wurden verschiedenste Anwendungsgebiete betrachtet und domainübergreifend verglichen, um eine grundsätzliche Definition des CRM zu finden. Insbesondere sollte herausgefunden werden, wie sich das CRM vom SCRM abgrenzt bzw. dieses erweitert. Obwohl festgestellt wurde, dass keine einheitliche Definition gefunden werden kann, so existiert zumindest ein ähnliches Verständnis für das CRM als Anwendung des RM in IORs. Dabei wurden in der Veröffentlichung 6 Fähigkeiten (Capabilities) identifiziert, die das CRM auszeichnen bzw. ermöglichen: Teilen von Risikoinformationen (risk information sharing), Standardisierung der Vorgehensweisen (standardisation of procedures), Prozessintegration (process integration), Teilen von Risiken und Vorteilen (risk and benefit sharing), Gemeinsame Entscheidungen (joint decision making), Kollaborative Leistungssysteme (collaborative performance systems).

Anwendbarkeit ISRM

Friday et al. [29, S. 242–243] sprechen beim CRM von einem „higher order construct“ sagen dazu: „CRM capabilities include routines, practices, and predictable patterns of activity, employed to increase capacity in reshaping and reconfiguring assets to enhance a supply chain's ability to mitigate disruptions and their spillover effects through sequences of coordinated interfirm actions“. Diese Fähigkeiten liefern letztlich eine fundierte Ausgangslage für das, was ein kollaborativer Ansatz im RM grundsätzlich leisten sollte, um erfolgreich zu sein. Obwohl bei der Ermittlung Eigenschaften des CRM das klassische SCRM im Fokus des Literaturreviews steht, so sind die identifizierten Fähigkeiten doch so generisch, dass sie auch eine Grundlage zur Machbarkeit in anderen Anwendungsbereichen sein können. Es ist anzunehmen, dass das, was in diesem Zusammenhang für das SCRM ermittelt wurde, auch einen sinnvollen Rahmen für das CISRM liefern kann. Auch dort soll der Anwendungsbereich des existierenden ISRM von einer Organisation auf eine Allianz erweitert werden.

Adaption ISRM

Da viele der untersuchten Kollaborationen jedoch aus anderen RM Bereichen stammen, bei denen oftmals die gemeinsame Produktion von Gütern in Vordergrund steht, sind nicht alle Erkenntnisse direkt zu übertragen. Grundsätzlich lassen sich hier jedoch im Kern wichtige Praktiken erkennen, die im CRM berücksichtigt werden sollten. Dahinter steht auch immer

ein übergeordnetes Ziel, das es zu erreichen gilt. Durch Abstrahieren der Ziele sollten sich diese auch für das ISRM adaptieren lassen. Im Folgenden werden die von Friday et al. [29] genannten Fähigkeiten gelistet und mit Blick auf das ISRM interpretiert. Die Ergebnisse sind in Tabelle 3.1 mit den abgeleiteten Zielen zusammengefasst.

Fähigkeit 1: Teilen von Risikoinformationen

Das Teilen von Informationen über Risiken bezeichnet den Austausch von Daten, die Aktivitäten innerhalb der Supply Chain sind. Dies soll die Partner dabei unterstützen, Risiken frühzeitig zu erkennen. Wichtige Rahmenbedingungen dazu sind, dass die Partner ihren Wissensstand synchronisieren, die Sichtbarkeit von Informationsflüssen und Aktivitäten innerhalb der Supply Chain erhöhen, SCRs bei anderen Partnern zu verhindern, sowie opportunistisches Verhalten vermeiden. Das Ziel ist also der Austausch von Informationen zum Aufbau einer gemeinsamen Wissensbasis, um damit langfristig Störungen zu vermeiden. Dies ist genauso im ISRM gültig, bei dem die Partner Informationen über für die Allianz relevante IS-Risiken austauschen sollten.

Fähigkeit 2: Standardisierung der Vorgehensweise

Bei der Standardisierung der Vorgehensweise geht es um die Einhaltung von strukturierten Verfahren. Dadurch wird die Nachvollziehbarkeit des SCRM Prozesses erhöht, wodurch die Konsistenz und Stabilität der Abläufe gesichert wird. Nur so kann sichergestellt werden, dass die Zusammenarbeit im CRM langfristig funktioniert. Das übergeordnete Ziel ist es daher, die Kontinuität der Zusammenarbeit im RM sicherzustellen. Auch dies ist direkt auf das ISRM übertragbar, insofern die Partner ein einheitliches Verständnis über die Begriffe und Konzepte des ISRM haben müssen, um überhaupt zusammenarbeiten zu können.

Fähigkeit 3: Gemeinsame Entscheidungen

Die gemeinsame Entscheidungsfindung beschreibt die Fähigkeit der Partner, sich innerhalb der Allianz auf eine gemeinsame Risikobehandlung zu einigen. Dadurch sollen insbesondere die internen Entscheidungsprozesse angepasst werden, um die Auswirkungen der Risikoakzeptanz eines Partners für die Allianz zu reduzieren. Hier ist das Ziel also die übergreifende Koordination eines Entscheidungsprozesses, um Gefahren aufgrund von Einzelentscheidungen zu vermeiden. Im ISRM kann dies analog über ein Abstimmen der Risikobehandlungsoptionen innerhalb der Allianz geschehen.

Fähigkeit 4: Teilen von Risiken und Vorteilen

Das Teilen von Risiken und Vorteilen ist essenziell, um die Partner am CRM zu beteiligen. Das erfordert die Entwicklung formeller Strategien und Vereinbarungen zur Aufteilung von Haftung und Vorteilen aus den gemeinsamen Aktivitäten. Dies stellt sicher, dass die Partner vom gemeinsamen RM profitieren und die Auswirkungen von Risiken auf die Allianz verteilen können. Letztlich ist das Ziel, gemeinsame Verbindlichkeiten und Erfolge zu

etablieren. Aus dem ISRM heraus ist es schwer vorstellbar, eine gemeinsame Verantwortlichkeit für Nachteile und Vorteile der Risikobehandlung zu etablieren. Vielmehr scheint es so, dass dies eine Grundbedingung der Beziehung ist, welche sich durch die gegenseitige Abhängigkeit und die gemeinsamen Ziele ergibt.

Fähigkeit 5: Prozessintegration

Prozessintegration beschreibt die Tatsache, dass die Partner ihre internen und externen Prozess aneinander angleichen müssen. Nur wenn diese aufeinander abgestimmt sind, kann ein sinnvoller Informationsaustausch erfolgen. Das Ziel ist, es die RM Verfahren intern und extern zu synchronisieren, um einen durchgängigen Prozess zu etablieren. Für das ISRM bedeutet das, dass die Prozesse der Partner grundsätzlich kompatibel zueinander sein müssen.

Fähigkeit 6: Kollaborative Leistungssysteme

Das kollaborative Leistungssystem ist ein Begriff für ein Kennzahlensystem, welches zur Überwachung von Störungen in Betriebsprozessen dient. Dadurch sollen Probleme in der Supply Chain für alle Partner transparent dargestellt werden. Es liefert damit eine wichtige Grundlage für das Teilen von Risikoinformationen und die gemeinsame Entscheidungsfindung. Dieser Aspekt ist stark auf die Produktion innerhalb des SCRM zugeschnitten. Trotzdem lässt sich daraus das Ziel abstrahieren, dass die Partner die transparente Messbarkeit des Risikoniveaus sicherstellen müssen. Übertragen auf das ISRM kann das einfach bedeuten, dass die Ergebnisse des ISRM innerhalb der Allianz vergleichbar sein müssen.

Tabelle 3.1: Adaption von CRM-Prinzipien aus der Literatur für das CISRM

CRM Prinzip	Abgeleitetes Ziel	Adaptierung CISRM
Teilen von Risikoinformationen	Austausch von Informationen zur Behandlung von Risiken	Austausch über IS-Risiken zwischen den Partnern
Standardisierung der Vorgehensweisen	Kontinuität der Zusammenarbeit sicherstellen	Einheitliches Verständnis des ISRM
Gemeinsame Entscheidungen	Übergreifende Koordination des Entscheidungsprozesses	Abstimmung der Risikobehandlungsoptionen
Teilen von Risiken und Vorteilen	Gemeinsame Verbindlichkeit und Erfolge etablieren	Gemeinsames Interesse der Partner am Erfolg der Allianz
Prozessintegration	Angleichen von Prozessen zur Vermeidung von Störungen	Kompatibilität verschiedener ISRM Prozesse
Kollaborative Leistungssysteme	Messbarkeit des Risikoniveaus der Partner	Vergleichbarkeit der IS-Risiken in der Allianz

3.3.2 Ableitung von Anforderungen

Die oben gelisteten Fähigkeiten sind das Ergebnis aus verschiedensten kollaborativen Anwendungsbeispielen des SCRM, die als abstrakte Kompetenzen für die erfolgreiche Zusammenarbeit in Partnerschaften gesehen werden können. Die daraus abgeleiteten Ziele für das ISRM (Tabelle 3.1) zeigen, dass sie auch einen sinnvollen Rahmen in diesem Anwendungsbereich liefern können. Durch Adaptieren der Fähigkeiten und anpassen an das CISRM können sie den Ausgangspunkt für die Durchführung des RM Prozesses als gemeinsame Managementfunktion definieren. Daher werden sie im Kontext dieser Arbeit als Critical Success Factors (CSFs)[2] definiert, welche das CISRM erfüllen muss. Es wird davon ausgegangen, dass ein kollaboratives Vorgehen im ISRM nur erfolgreich ist, wenn sie alle berücksichtigt wurden.

Anforderungen

Somit sollte auch ein entsprechendes Prozessframework mindestens diese sechs CSF etablieren, um wirksam anwendbar zu sein. Ausgehend von den speziellen Eigenschaften der Kollaborationsszenarien (Abschnitt 3.1) und dem Fallbeispiel ((Abschnitt 3.1)) lassen sich wiederum einzelne Anforderungen ableiten. Diese lassen sich den CSF zuordnen, um einen Anforderungskatalog zu erstellen. Ziel ist es, die Voraussetzungen für ein möglichst kompaktes Meta-Framework zu definieren, dass das Zusammenwirken mehrerer ISRM Prozesse in verschiedenen Organisationen ermöglicht. Im Folgenden werden die oben beschriebenen Fähigkeiten auf das CISRM angewendet und daraus weitere Anforderungen abgeleitet. Sie werden im Text mit [R]*equirement* und einer fortlaufenden Nummer markiert.

Teilen von Risikoinformationen

Ein erster Schritt, um das eigene ISRM zu verbessern, ist es, Informationen über Risiken mit anderen Organisationen zu teilen. Dies ist keine spezielle Eigenschaft von kollaborativen Beziehungen, sondern findet bereits in anderen IORs und mit Hilfe von Plattformen und offenen Communitys statt. So entwickelt sich das Teilen von IS Informationen über Schwachstellen oder Incidents zunehmend zu einem essenziellen Faktor zur Abwehr von Angriffen [45]. Trotzdem ist die Allianz hier in einer optimalen Position, um diesen Austausch zu intensivieren und so den Partnern einen Vorteil zu verschaffen. Während es bei andern Communitys meist eher um den Austausch von Informationen über aktuelle Bedrohungen und Schwachstellen geht, könnten Allianzen tatsächlich auf ihre realen Risiken verweisen. Das ist natürlich nur nützlich, wenn das ISRA der Partner zu vergleichbaren Risiken führt, welche auch Relevanz für die Partner haben, da diese sonst nur einen geringen Informationsgehalt hätten [R1.1]. Weiterhin gilt es vorher die Risiken zu identifizieren, welche Risiken überhaupt für die Partner relevant sind [R1.2]. Das können auf der einen Seite ROs sein, welche nur eine Information für die Partner darstellen und diesen als Eingabe für das eigene ISRM dienen können. Auf der anderen Seite existieren die RAs, welche für die Allianz als Ganzes relevant sind. Um diese Risikoinformationen sinnvoll zwischen den Partnern austauschen zu können, muss innerhalb der Allianz ein strukturiertes Vorgehen definiert werden [R1.3].

[2] CSFs sind Kernaspekte die funktionieren müssen, um ein Ziel zu erreichen [159].

CSF 1: Teilen von Risikoinformationen

Ein unkomplizierter Austausch von relevanten IS-Risiken innerhalb der Allianz ist möglich.

R1.1 Die Risikoeinschätzung der Partner muss zu vergleichbaren Risiken führen.

R1.2 Es muss geregelt sein, welche Risiken innerhalb der Allianz relevant sind.

R1.3 Es muss ein strukturiertes Vorgehen existieren, um Risikoinformationen zwischen den Partnern auszutauschen.

Standardisierung der Vorgehensweisen

Für ein CISRM ist es grundlegend notwendig, dass die Partner sich innerhalb der Allianz inhaltlich Austauschen können [R2.1]. Im ISRM existieren heute jedoch sehr viele verschiedene Vorgehensmodelle, die von Organisationen zur Etablierung eines Prozesses genutzt werden können (siehe Kapitel 2.3). Eine Allianz besteht immer aus unabhängigen Organisationen. Bei vertikalen Allianzen stammen diese sogar aus unterschiedlichen Branchen, bei internationalen Allianzen nicht einmal aus dem gleichen Land. Es daher kann nicht davon ausgegangen werden, dass alle die gleichen Standards verwenden oder das gleiche Verständnis für ISRM besitzen. Das bedeutet unter anderem, dass sich die Partner auf die Bedeutung von Kernelementen des ISRM (z.B. Risiken, Assets und Schwachstellen) sowie deren Zusammenhang einigen müssen [R2.2]. Gleichzeitig darf dies nicht dazu führen, dass die Partner ihre internen Standards anpassen müssen, da dies die Akzeptanz des CISRM reduzieren würde [R2.3]. Es ist davon auszugehen, dass die Sprache ein Teil der Unternehmenskultur ist und nicht ohne erheblichen Aufwand angepasst werden kann.

CSF 2: Standardisierung der Vorgehensweisen

Innerhalb der Allianz herrscht ein einheitliches Verständnis des ISRM und seiner Inhalte.

R2.1 Die Partner müssen im CISRM über eine einheitliche Sprache verfügen.

R2.2 Die Kernelemente des ISRM müssen innerhalb der Allianz standardisiert sein.

R2.3 Die internen Prozesse der Partner dürfen nicht durch die einheitliche Sprache [R2.1] oder standardisierten Elemente [R2.2] beeinträchtigt werden.

Gemeinsame Entscheidungen

Neben dem bloßen Teilen von Risikoinformationen ist es ein Hauptziel der Kollaboration, das Risikoniveau der gesamten Allianz zu senken. Das kann nur funktionieren, wenn die Partner sich bei der Auswahl einer geeigneten Risikobehandlungsoption miteinander abstimmen. Es gilt also zu definieren, wie über relevante Risiken innerhalb der Allianz entschieden werden kann [R3.1]. Es ist zu bedenken, dass die Partner freiwillig an der Allianz und dem CISRM teilnehmen. Um die Akzeptanz der getroffenen Risikobehandlung zu gewährleisten ist es notwendig, dass alle Partner auch Einfluss auf die Entscheidung haben [R3.2]. Zusätzlich wird es jedoch auch Risiken geben, die zwar für die Allianz relevant sind, welche eine Organisation jedoch intern adressiert. Die Partner dürfen daher nicht zur Zusammenarbeit gezwungen werden, sondern müssen selbst entscheiden können, ob sie ein Risiko selbständig oder gemeinsam behandeln wollen [R3.3].

CSF 3: Gemeinsame Entscheidungen

Die Risikobehandlung von für die Allianz relevanten IS-Risiken wird zwischen den Partnern abgestimmt.

R3.1 Über relevante Risiken [R1.2] muss innerhalb der Allianz entschieden werden.

R3.2 Jeder Partner muss Einfluss auf die Freigabe der Risikobehandlung haben.

R3.3 Die Entscheidungsfindung muss die Autonomie der Partner bei der Risikobehandlung gewährleisten.

Teilen von Risiken und Vorteilen

Ein Hauptgrund für die Implementierung eines CISRM innerhalb einer Allianz ist die Erwartung, dass eine gemeinsame Ausführung des ISRM jedem Partner einen Mehrwert bietet. Wie bereits etabliert sind dabei die zwei Ebenen der ROs und RAs zu betrachten. Das heißt, es ergeben sich Vorteile aus einer gemeinsamen Betrachtung und Behandlung für die einzelne Organisation oder die gesamte Allianz. RAs sind für eine Organisation dabei nur relevant, wenn sie auch ein Interesse am Erfolg der Allianz hat [R4.1]. Gleichzeitig führt das dazu, dass jeder Partner am Wohlergehen der anderen Partner interessiert sein muss, da dies sonst den gemeinsamen Erfolg gefährden könnte [R4.2]. Beide Anforderungen hängen offensichtlich bereits von der Auswahl der Partner ab und ergeben sich aus den Eigenschaften einer Beziehung. Somit scheinen bereits Einschränkungen bei der Wahl der Teilnehmer zu geben, die den Anwendungsbereich des CISRM eingrenzt. Dabei ist einer der wichtigsten Gründe, warum sich Partnerschaften überhaupt formen, gemeinsame Probleme effizient zu lösen. Auch dazu muss die Allianz organisatorisch überhaupt in der Lage sein, unabhängig von der Zusammenarbeit im Bereich der IS. Übertragen auf das ISRM ist damit der große Vorteil, dass die Partner gemeinsam Maßnahmen ergreifen können, die zu komplex für jede einzelne Organisation wären [R4.3].

CSF 4: Teilen von Risiken und Vorteilen

Aus einer gemeinsamen Risikobehandlung ergeben sich Vorteile für die Allianz oder jede einzelne Organisation.

R4.1 Die Partner müssen ein Interesse am Erfolg der Allianz haben.

R4.2 Jeder Partner muss einen Vorteil durch die Reduktion von IS-Risiken haben.

R4.3 Die Allianz muss das gemeinsame Umsetzen von Maßnahmen ermöglichen.

Prozessintegration

Wie bereits erwähnt können die Teilnehmer einer Allianz aus verschiedensten Organisationen bestehen. Nachdem keine verbindlichen Standards oder eine einheitliche Vorgehensweise zum ISRM existiert, kann nicht davon ausgegangen werden, dass alle Partner dabei das gleiche Prozessmodell etablieren. Grundsätzlich ist das Verfahren zum ISRA zwar oft einheitlich definiert und von bekannten Rahmenwerke abgeleitet, jedoch werden insbesondere Struktur und Inhalt der Risiken individuell erfasst [131, 65]. Jede Organisation wird potenziell ein Modell etablieren, dass am besten zu ihrer Struktur, Kultur oder Branche passt. Durch eine Standardisierung der Vorgehensweisen (CSF 2) wird zumindest ein gemeinsames Verständnis für das ISRM geschaffen. Der Versuch, ein übergreifendes ISRM zu etablieren lässt damit zwei Alternativen zu: Entweder alle Teilnehmer der Allianz verwenden das gleiche Prozessmodell oder die unterschiedlichen Prozessmodelle müssen zueinander kompatibel sein. Es scheint eher unwahrscheinlich, dass sich innerhalb einer Partnerschaft (insbesondere bei mehr als zwei Organisationen) immer alle Partner innerhalb einer Allianz auf ein Prozessmodell einigen können [R5.1]. Aufgrund der Unabhängigkeit der Organisationen kann die Verwendung eines bestimmten Prozessmodells außerdem im Normalfall nicht erzwungen werden[3]. Das bedeutet allerdings auch, dass ein bereits implementierter Prozess einfach um die für die Kollaboration notwendigen Elemente erweiterbar sein muss, um eine einfache Schnittstelle zu den Prozessen anderer Organisationen zu schaffen [R5.2]. Weiterhin muss sichergestellt sein, dass die internen Prozesse der Partner nicht blockiert werden, da diese weiterhin unabhängig voneinander arbeiten wollen [R5.3]. Schließlich bleiben alle Organisationen im Kern selbständige Einheiten, die nur in einem Teilbereich zusammenarbeiten, dies jedoch nicht ihre anderen Geschäftsaktivitäten beeinflussen soll.

[3]Im Falle eines Konzerns besteht zwar grundsätzlich die Möglichkeit zentrale Vorgaben zu machen, jedoch würde die Konformität einen hohen organisatorischen Aufwand verursachen und die Selbständigkeit der Tochtergesellschaften gefährden. Dies repräsentiert eine machtbasierte Beziehung, während hier von Vertrauen als dominierender Eigenschaft ausgegangen wird (siehe Kapitel 4).

CSF 5: Prozessintegration

Ein kollaborativer Prozess innerhalb der Allianz integriert existierende ISRM Implementierungen, ohne das ERM der Partner negativ zu beeinflussen.

R5.1 Ein Prozessmodell für das CISRM muss kompatibel zu etablierten ISRM Standards und Frameworks sein.

R5.2 Ein bereits implementierter Prozess muss einfach erweiterbar sein.

R5.3 Das CISRM muss den Partnern weiterhin die Ausführung ihrer internen Prozesse ermöglichen und darf diese nicht beeinträchtigen.

Kollaborative Leistungssysteme

Für eine erfolgreiche Zusammenarbeit im ISRM ist es wichtig, relevante Aspekte innerhalb der Allianz transparent darzustellen. Das Ziel des CISRM ist es letztlich nicht nur Ressourcen zu verwalten, sondern auch durch gemeinsame Maßnahmen das Sicherheitsniveau der Allianz zu verbessern [R6.1]. Dabei existieren im ISRM zwei Kernelemente, welche eine Aussage über IS-Risiken zulassen: Assets und Bedrohungen. Diese sind eine Voraussetzung, wenn ein Austausch von Risikoinformationen (CSF 1) und eine gemeinsame Entscheidungsfindung (CSF 3) realisiert werden soll. Da es sich bei den Partnern um unabhängige Organisationen handelt, haben alle davon unterschiedliche Assets, die sie schützen wollen. Im Zuge des ISRM müssen sie jedoch herausfinden, welche davon relevant für die Allianz sind um entsprechende Risiken zu teilen. Gleichzeit müssen andere Partner die Möglichkeit haben, Risikoinformationen auf ihre eigenen Assets abzubilden, um diese nutzen zu können [R6.2]. In diesem Zusammenhang sind auch die Bedrohungen relevant, welche auf die Assets wirken. Die Partner sollten einen Überblick über das Bedrohungsmodell der Allianz haben, um ihre Risiken nachvollziehbar zu bewerten [R6.3]. Schließlich bietet ihnen dieses einen Einblick in das übergreifende Sicherheitsniveau und relevante Bedrohungen.

CSF 6: Kollaborative Leistungssysteme

Das Risikoniveau der Allianz ist für alle Partner transparent und die Auswirkungen von Bedrohungen sind nachvollziehbar.

R6.1 Das Sicherheitsniveau der Allianz muss sich durch das CISRM langfristig verbessern lassen.

R6.2 Die IS-Assets der Partner müssen miteinander vergleichbar sein.

R6.3 Die Partner müssen das Bedrohungsmodell der Allianz verstehen.

3.3.3 Zusammenfassung der Anforderungen

Durch die Analyse der sechs CSF wurden insgesamt 18 Anforderungen an das CISRM identifiziert. Es wurde sich dazu entschieden, jeweils maximal drei Anforderungen zu definieren, um ein Ziel zu erfüllen. Obwohl unter jedem CSF damit noch weitere Anforderungen denkar wären, sind die existierenden für eine Evaluation ausreichend. Eine größere Anzahl oder ein höherer Detailgrad würde nicht automatisch zu einem besseren Ergebnis führen, aber die Auswertung erschweren. Die vollständige Liste mit CSFs und den übergeordneten Zielen aus Tabelle 3.1, sowie den einzelnen Anforderungen ist in Tabelle 3.2 zu sehen.

CSF 1 Im ersten CSF geht es darum, ein System zu etablieren, dass die Kommunikation zwischen den einzelnen Prozessen, den verteilten Prozessaktivitäten und den für diese zuständigen Personen ermöglicht. Dazu ist es erforderlich, dass die Partner vergleichbare Daten liefern, um diese im CISRM auszutauschen. Weiterhin muss klar festgelegt werden, welche Informationen überhaupt relevant sind und wie die Partner sie austauschen können.

CSF 2 Im zweiten CSF soll sichergestellt werden, dass die Partner ein ähnliches Verständnis für das ISRM aufweisen. Der gemeinsame Prozess muss eine Sprache verwenden, den alle Teilnehmer unabhängig von ihrem Hintergrund verstehen können. Somit müssen auch die in diesem Prozess verwendeten Elemente für alle Partner verständlich sein, damit sie einheitlich verwendet werden. Diese innerhalb der Allianz getroffenen Abstimmungen dürfen letztlich nicht mit dem internen Vorgehen der Organisationen kollidieren.

CSF 3 Im dritten CSF wird auf eine gemeinsame Risikobehandlung innerhalb der Allianz abgezielt. Das bedeutet, dass alle relevanten Risiken auch untereinander besprochen und deren Behandlung gemeinsam entschieden wird. Dabei müssen alle Partner den gleichen Einfluss auf die Entscheidung haben, wenn es die Allianz als Ganzes betrifft. Trotzdem sollten die Organisationen nicht in ihrem eigenen Vorgehen eingeschränkt oder von der Behandlung eines Risikos abgehalten werden.

CSF 4 Im vierten CSF sollen die Grundlagen einer Verteilung von Risiken und Vorteilen zwischen den Partnern errichtet werden. Dies setzt im Grundsatz voraus, dass die Partner miteinander verbunden sind und gemeinsam erfolgreich sein wollen. Ist dies der Fall, dann sollten auch die Konsequenzen einer Zusammenarbeit positive Auswirkungen auf alle Organisationen haben. Das gemeinsame Umsetzen von Maßnahmen hilft den Partnern von der Zusammenarbeit zu profitieren.

CSF 5 Im fünften CSF steht die Entwicklung eines kollaborativen Prozesses im Vordergrund. Dieser muss verbreitete Industriestandards unterstützen und die auf ihnen basierenden Prozesse einfach erweitern können. Dabei muss trotz der Zusammenarbeit sichergestellt sein, dass die Partner ihre existierenden Prozesse unabhängig voneinander weiterhin nutzen können.

CSF 6 Im sechsten CSF geht es letztlich um die Transparenz innerhalb des CISRM. Am Ende sollte erkennbar sein, dass das gemeinsame Vorgehen das Sicherheitsniveau der Partner verbessert. Weiterhin sollten die Assets innerhalb der Allianz vergleichbar und die darauf abzielenden Bedrohungen nachvollziehbar sein.

Umsetzung Nachfolgend wird beschrieben, wie die das geplante Framework erstellt werden soll, um alle Anforderungen an das CISRM zu erfüllen.

Tabelle 3.2: Anforderungen an das CISRM

CSF 1: Teilen von Risikoinformationen	
R1.1	Die Risikoeinschätzung der Partner muss zu vergleichbaren Risiken führen.
R1.2	Es muss geregelt sein, welche Risiken innerhalb der Allianz relevant sind.
R1.3	Es muss ein strukturiertes Vorgehen existieren, um Risikoinformationen zwischen den Partnern auszutauschen.
CSF 2: Standardisierung der Vorgehensweisen	
R2.1	Die Partner müssen im CISRM über eine einheitliche Sprache verfügen.
R2.2	Die Kernelemente des ISRM müssen innerhalb der Allianz standardisiert sein.
R3.3	Die internen Prozesse der Partner dürfen nicht durch die einheitliche Sprache [R2.1] oder standardisierten Elemente [R2.2] beeinträchtigt werden.
CSF 3: Gemeinsame Entscheidungen	
R3.1	Über relevante Risiken [R1.2] muss innerhalb der Allianz entschieden werden.
R3.2	Jeder Partner muss Einfluss auf die Freigabe der Risikobehandlung haben.
R3.3	Die Entscheidungsfindung muss die Autonomie der Partner bei der Risikobehandlung gewährleisten.
CSF 4: Teilen von Risiken und Vorteilen	
R4.1	Die Partner müssen ein Interesse am Erfolg der Allianz haben.
R4.2	Jeder Partner muss einen Vorteil durch die Reduktion von IS-Risiken haben.
R4.3	Die Allianz muss das gemeinsame Umsetzen von Maßnahmen ermöglichen.
CSF 5: Prozessintegration	
R5.1	Ein Prozessmodell für das CISRM muss kompatibel zu etablierten ISRM Standards und Frameworks sein.
R5.2	Ein bereits implementierter Prozess muss einfach erweiterbar sein.
R5.3	Das CISRM muss den Partnern weiterhin die Ausführung ihrer internen Prozesse ermöglichen und darf diese nicht beeinträchtigen.
CSF 6: Kollaborative Leistungssysteme	
R6.1	Das Sicherheitsniveau der Allianz muss sich durch das CISRM langfristig verbessern lassen.
R6.2	Die IS-Assets der Partner müssen miteinander vergleichbar sein.
R6.3	Die Partner müssen das Bedrohungsmodell der Allianz verstehen.

3.4 Konzept zur Erstellung des Frameworks

Das Ziel dieser Arbeit ist es, ein allgemeines Vorgehen für das CISRM zu beschreiben und zusammen mit den für dessen Aufbau benötigten Werkzeugen als Framework bereitzustellen (siehe Forschungsfrage in Kapitel 1.2). Dieses soll verschiedene Typen von IORs, wie in den vorgestellten Szenarien (Abschnitte 3.1 und 3.2), unterstützen und ihnen eine prozessbasierte Zusammenarbeit im Bereich der IS ermöglichen. Dabei wird nicht das ISRM an sich oder die Grundlagen des ISRA verändert, da sich diese in der Industrie inzwischen weitgehend etabliert haben. Das Ergebnis stellt somit ein Meta-Framework dar, welches auf existierenden ISRM Frameworks aufsetzt und entsprechende Prozesse verschiedener Organisationen miteinander verknüpft.

Framework Komponenten

Um die Wirksamkeit des CISRM sicherzustellen, wurden zuvor sechs CSF mit 18 Anforderungen definiert (Tabelle 3.2). Das geplante Framework muss damit verschiedene Komponenten enthalten, welche geeignet sind, diese Anforderungen zu erfüllen. Die Bestandteile des Frameworks ergeben sich aus den zur Zusammenarbeit notwendigen Rahmenbedingungen, die Schritt für Schritt abgeleitet werden. Die vier Module des kollaborativen Frameworks sind in Abbildung 3.1 dargestellt. Diese bauen inhaltlich teilweise aufeinander auf und unterstützen jeweils genau einen Aspekt beim Aufbau eines interorganisationalen Prozesses.

Modul 1

Dabei gilt es zuerst herauszufinden, in welchem Kontext das CISRM wirksam anwendbar ist (Modul 2: Anwendbarkeit des CISRM). Nicht alle IORs sind überhaupt dazu geeignet, übergreifende ISM Prozesse zu etablieren und insbesondere IS Risiken gemeinsam zu behandeln. Die Organisationsstruktur und auch die Partnerschaft werden in erster Linie auf Basis der Geschäftsstrategie gesteuert und sind aus dem ISM heraus kaum zu beeinflussen. Somit hilft das Modul den Organisationen festzustellen, ob ihre IOR die Voraussetzungen für ein CISRM erfüllt.

Modul 2

Als Nächstes soll das zweite Modul, eine einheitliche Terminologie für das CISRM, entwickelt werden (Modul 2: Terminologie des ISRM). Dazu werden die in Kapitel 2.3 vorgestellten ISRM Frameworks genauer untersucht. Basierend auf diesen wird eine allgemeingültige Terminologie definiert, welche Kernbegriffe und Schlüsselkonzepte des ISRM beschreiben. Diese bilden nicht nur eine Komponente des Frameworks, sondern auch die Grundlage für den kollaborativen Prozess und dessen Ressourcen.

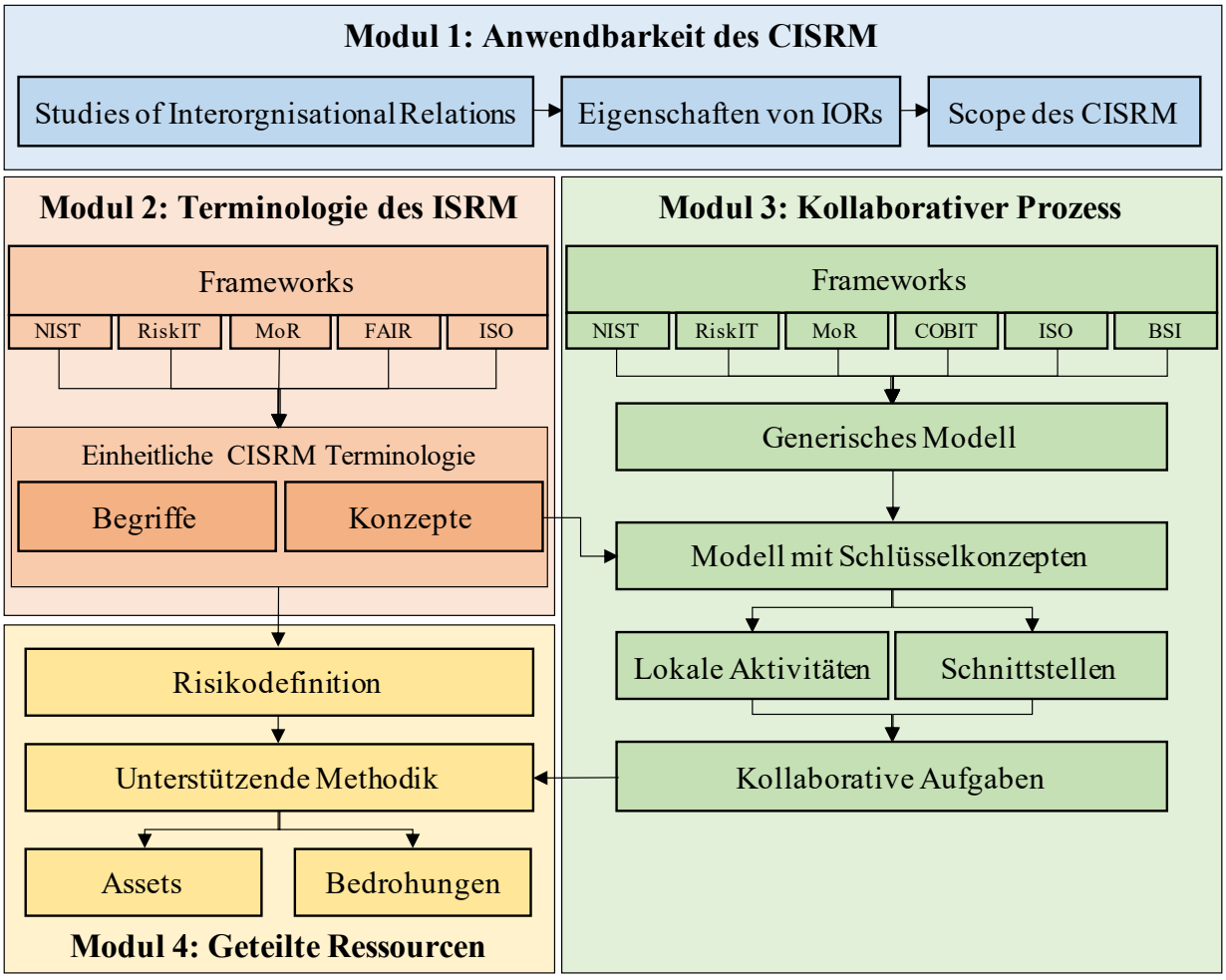
Modul 3

Das dritte Modul des Frameworks bildet ein kollaborativer Prozess, welcher von den Aktivitäten der bereits vorher betrachteten Frameworks abgeleitet wird (Modul 3: Kollaborativer Prozess). Durch eine Analyse der Aktivitäten des ISRM werden diese in lokale (begrenzt auf die Organisation) und Schnittstellenaktivitäten (Schnittstelle in den gemeinsamen Prozess) aufgeteilt werden. Daraus ergibt sich ein Prozessmodell für das CISRM, welches die Interaktionen und Verantwortlichkeiten im Prozess darstellt. In Kombination mit den Schlüsselkonzepten liefert dieser die Ausgangslage für die Beschreibung gemeinsam genutzter Ressourcen, die in den Prozess eingehen sollten.

Modul 4

Die während der Framework-Analyse identifizierten Inputs für den kollaborativen Prozess werden im vierten Modul schematisch beschrieben (Modul 4: Geteilte Ressourcen). Dazu gehört eine generische Methodik basierend auf der im Terminologie-Review erstellten

Abbildung 3.1: Konzept zur Erstellung eines kollaborativen Frameworks



Risikodefinition. Weiterhin werden die für das ISRM wichtigen Elemente Assets und Bedrohungen im Kontext des CISRM beschrieben. Diese Ressourcenbeschreibungen unterstützen den Aufbau des in Modul 4 beschriebenen Prozesses innerhalb der IOR.

Ausblick

Die vorgestellten Module liefern Organisationen die nötigen Hilfsmittel, um ein CISRM innerhalb ihrer Allianz aufzubauen. In den nächsten Kapiteln wird nun der genannten Reihenfolge nach jeweils ein Modul des Frameworks entwickelt. Anschließend werden die in diesem Kapitel definierten Anforderungen (Abschnitt 3.3) auf das erstellte Framework angewendet und der Aufbau eines Prozesses auf Basis des Fallbeispiels (Abschnitt 3.2) beschrieben. Den Anfang macht eine Untersuchung der Anwendbarkeit des CISRM, bei der insbesondere die verschiedenen Arten von IORs betrachtet werden.

Kapitel 4

Anwendungsbereich des CISRM

Inhaltsangabe

Hypothese Im vorherigen Kapitel wurden die Anwendungsfälle für eine Kollaboration im ISRM und die Anforderungen an ein potenzielles CISRM beschrieben. Die Anwendbarkeit eines kollaborativen ISRM, bei dem die individuellen Prozesse innerhalb einer IOR synchronisiert werden, ist insbesondere davon abhängig, wie die teilnehmenden Organisationen zusammenarbeiten. Die Hypothese ist, dass nur solche IORs, welche eine intensive Zusammenarbeit erlauben und deren Partnerschaft einen entsprechenden Reifegrad aufweist, grundsätzlich dafür geeignet sind.

Ausgangslage Als Ausgangslage schließen sich unabhängige Organisationen aufgrund gemeinsamer Interessen zu einer Allianz zusammen. Die einzelnen Partner nehmen an der Allianz teil, da sie dadurch einen strategischen Vorteil erwarten, den sie alleine nicht hätten. Nun besteht die Möglichkeit, im Kontext dieser Allianz zusätzlich noch die Kollaboration in anderen Bereichen zu betrachten, die über den Geschäftszweck der Partnerschaft hinausgehen. Beispiele dafür finden sich heute bereits häufig im Teilen von Ressourcen [160, 22] und Wissen [161, 162] zwischen Organisationen in verschiedenen Geschäftsbereichen. Dabei zeigt sich, dass diese langfristig von engen Kollaborationen profitieren, die mehr sind als ein bloßes Vertragsverhältnis [163].

Status quo Im Bereich der IS gibt es Kooperation etwa bereits bei Themen wie *Security Information Sharing* [41] oder *Security Incident Management* [45], bei denen Informationen über relevante Ereignisse in einem Netzwerk von Organisationen [42, 44, 164] ausgetauscht werden. Dabei handelt es sich jedoch meist nicht um ein kollaboratives Vorgehen, da jede Organisation weiterhin ihre eigenen Ziele verfolgt, und zwar unabhängig von den anderen Partnern. Es werden Informationen ausgetauscht, aber der Umgang damit bleibt jedem Teilnehmer selbst überlassen. Denken wir die Zusammenarbeit einen Schritt weiter, dann ist eine intensivere Form der Kooperation vorstellbar. Bei einem kollaborativen Vorgehen im ISM gehen die Partner über den reinen Austausch von Informationen hinaus und arbeiten auch koordiniert an gemeinsamen Schwächen und Problemen. Das setzt natürlich ein besonderes Interesse der einzelnen Organisationen aneinander und der Allianz als ganzes voraus, weshalb ein kollaboratives Vorgehen nur in einer engen, strategischen Partnerschaft sinnvoll sein kann. In einer solchen Allianz ist die Verbindung zwischen den Partnern stark genug, damit ein gemeinsames Vorgehen erfolgreich sein kann.

CISRM Übertragen auf das ISRM heißt das, dass die Partner erkannt haben, dass Risiken eines Partners auch Risiken für alle anderen darstellen können. Gleichzeitig wurde die Allianz aufgrund einer vertikalen oder horizontalen Nähe gegründet, weshalb bestimmte Risiken direkt die gesamte Allianz betreffen und von den Partnern gemeinsam behandelt werden können, z.B. umgebungsbezogene Risiken wie ein regionaler Blackout. Betrachtet man dabei lokale Allianzen (geografische Nähe), dann wären alle Partner gleichermaßen von einem regionalen Stromausfall betroffen. Es stellt sich an dieser Stelle die Frage, was eine Allianz gemeinsam dagegen tun kann, im Vergleich dazu, was jede Firma für sich alleine tun würde? Eine gemeinsame Risikobehandlung kann an dieser Stelle schneller und effizienter sein, da auf die Ressourcen der anderen Partner zugegriffen werden kann. Im oberen Beispiel wären das möglicherweise die gegenseitige Bereitstellung von Infrastruktur (Risiko teilen), der gemeinsame Aufbau einer unabhängigen Stromversorgung (Reduktion der Auswirkung) bzw. eines Ausweichstandortes (Reduktion der Eintrittswahrscheinlichkeit). Alle drei Maßnah-

men sind für eine einzelne Organisation in vielen Fällen zu ressourcenintensiv. Das CISRM kann den Partnern dabei helfen, gemeinsame Risiken zu behandeln, deren Reduktion ansonsten zu komplex wäre. Weiterhin kann die Allianz durch die Kollaboration im ISRM auch ihre Informationen über Bedrohungen und Risiken deutlich besser koordinieren und so gemeinsam eine höhere Widerstandsfähigkeit gegen IS-Risiken aufbauen.

Framework

Nachdem die Partner jedoch unabhängige Organisationen darstellen, besitzen sie unterschiedliche Voraussetzungen und haben eventuell verschiedene Prozesse etabliert. Das Ziel des kollaborativen Frameworks ist es nun, einen Rahmen zu definieren, der es den Organisationen trotzdem ermöglicht, ohne tiefgreifende interne Änderungen ein gemeinsames Vorgehen zu etablieren. Es soll die grundsätzlichen Elemente definieren, die in der Allianz etabliert bzw. in den Organisationen angepasst werden müssen, um die notwendige Kommunikation zu ermöglichen. Wie die Allianz den kollaborativen Prozess letztlich anwendet, um gemeinsamen Risiken zu begegnen, bleibt wie beim ERM am Ende den Partnern selbst überlassen. Dadurch ergeben sich bestimmte Einschränkungen im Vergleich zum Aufbau eines ISRM Prozesses innerhalb einer einzigen Organisation. Insbesondere kann nicht davon ausgegangen werden, dass sie die Dynamik der Beziehung verändert, nur um einen gemeinsamen Managementprozess zu etablieren. Stattdessen muss die IOR als statisches System gesehen werden, das nicht verändert werden kann.

Anwendungsbereich

Aufgrund dieser Voraussetzungen, die sich auch in den zuvor definierten Anforderungen widerspiegeln (Tabelle 3.2), ist das Konzept des CISRM nicht in jeder IOR anwendbar. So ist es etwa notwendig, dass die Partner ein Interesse am Erfolg der Allianz haben und von der gemeinsamen Risikobehandlung profitieren können (CSF 4), sowie deren Struktur gemeinsame Entscheidungen ermöglichen (CSF 3). Somit stellt sich die Frage, welche Beziehungen dafür geeignet sind, welche nicht und was diese Beziehungsformen auszeichnet. Aus der Forschung zum interorganisationalen Wissensaustausch und der wissensbasierten Kollaboration zwischen Organisationen geht hervor, dass die Rahmenbedingungen der Zusammenarbeit und die Faktoren, die für eine solche Beziehung essenziell sind oftmals nicht berücksichtigt werden [162]. Daher wird in diesem Kapitel zunächst die Frage nach den notwendigen Eigenschaften einer Allianz für das CISRM beantwortet und dabei ein allgemeines Werkzeug erstellt, um verschiedene Beziehungen und deren Eignung zur Zusammenarbeit (im ISRM Bereich) zu beschreiben.

Vorgehen

Dazu wird als Erstes der aktuelle Stand der Wissenschaft auf Basis der Literatur zu IORs untersucht (Abschnitt 4.1). Daraus werden die Kerneigenschaften einer solchen Zusammenarbeit abgeleitet, welche die Basis für die Klassifikation von Partnerschaften liefert. Dazu werden generische Beziehungstypen definiert, welche bestimmte Eigenschaften bündeln, die eine solche Beziehung erfüllen muss (Abschnitt 4.2). Anschließend wird ein Partnerschaftsmodell erstellt, das zur Festlegung des Anwendungsbereiches des CISRM genutzt werden kann (Abschnitt 4.3). Mit Hilfe dieser Beziehungstypen und des Partnerschaftsmodells soll es möglich sein zu bewerten, ob eine IOR für das CISRM geeignet ist.

Veröffentlichung

Das vorgestellte Partnerschaftsmodell wurde ursprünglich im Kontext dieser Arbeit als Teil des kollaborativen Frameworks entwickelt. Die Inhalte und Ergebnisse aus diesem Kapitel wurden bereits im Forschungsartikel „Opportunities of Interorganizational Collaboration in Information Security Management“ [165] beschrieben und veröffentlicht.

4.1 Interorganisationale Beziehungen

Neben dem klassischen, hierarchischen Unternehmen existieren heute viele verschiedene Formen von Organisationen. Deren Strukturen sind dabei heterogen und umspannen teilweise mehrere Tochtergesellschaften, Subunternehmen oder Partnerorganisationen. Über verschiedene Länder und Branchen hinweg haben sich dabei in den letzten Jahrzehnten interorganisationale Beziehungen etabliert, welche komplexe und langfristige Netzwerke aus unabhängigen Firmen formen [166, 24]. Netzwerke können dabei als sich selbstorganisierende Systeme angesehen werden, bei denen es nicht zwangsweise eine übergreifende Führung gibt, aber deren Aktivitäten miteinander verbunden sind, um die Zielerreichung der Akteure zu ermöglichen [167]. Diese Zusammenarbeit liefert den Teilnehmern Zugang zu einer größeren Ressourcenbasis, zu der insbesondere auch Wissen gehört [168]. Damit erlauben es diese Beziehungen gemeinsam mehr oder größere Vorhaben durchzuführen, als es jede einzelne Organisation alleine könnte.

ISM

Warum sich Organisationen für eine Zusammenarbeit entscheiden, hat dabei grundsätzlich nichts mit Technologie oder IS zu tun. Die Kooperation dient in erster Linie dem Erreichen der eigenen Geschäftsziele und wird von der Unternehmensstrategie und Bedürfnissen geleitet [169]. Haben sich zwei Organisationen jedoch für eine Partnerschaft entschieden, dann ist es denkbar, dass sie neben den angestrebten Geschäftsaktivitäten auch im Bereich ISM zusammenarbeiten. Dabei ist dies nicht auf Technologiefirmen beschränkt, da Technologien und Informationen in allen Branchen und Organisationen eine zentrale Rolle einnehmen. Durch die intensive Kollaboration überschreiten Sicherheitsrisiken einzelner Organisationen plötzlich organisatorische Grenzen und werden zum Risiko für andere Teilnehmer der Beziehung, wodurch IS eine gemeinschaftliche Aufgabe für die gesamte Partnerschaft wird [24]. Somit bringt der kontinuierlich fortschreitende Trend zur organisationsübergreifenden Zusammenarbeit auch neue Herausforderungen für das ISM und ISRM.

Ausblick

Im Folgenden werden im ersten Schritt die theoretischen Grundladen beschrieben, die für eine interorganisationale Beziehung relevant sind. Dazu gehört ein kurzer Einblick in die Organisationstheorie, sowie ein Überblick über die Kerneigenschaften von Beziehungen. Anschließend folgt eine Erklärung warum Organisationen überhaupt eine Beziehung eingehen und welche besonderen Charakteristika diese IORs aufweisen. Letztlich erfolgt eine Abgrenzung verschiedener Beziehungsstrukturen, welche die Grundlage für die nachfolgende Gruppierung von Beziehungen liefert.

Definitionen

In diesem Abschnitt werden bereits einige Definitionen erstellt, welche erst später relevant werden. Diese Definitionen werden zur Erstellung des Partnerschaftsmodells in Abschnitt 4.3 verwendet.

4.1.1 Grundlagen der Organisationstheorie

Definition IOR

Das Forschungsgebiet der interorganisationalen Beziehungen ist vielfältig und trotz ähnlichem Schwerpunkt existieren verschiedenste Bezeichnungen für Themen im Bereich der IORs. Dazu gehören etwa *Interorganizational relations/relationships* [170, 171, 166], *Interorganizational Cooperation* [172, 173], *Interorganizational Collaboration* [174, 175, 176], *Interorganizational Coordination* [135] oder *Inter-firm/company Cooperation* [177, 169]. Trotz unterschiedlichen Bezeichnungen sind diese inhaltlich oftmals nicht klar voneinander abzugrenzen und werden im Folgenden gemeinsam unter dem Begriff IOR adressiert, sofern es nicht um eine spezialisierte Form geht. Dabei wir der Definition von Cropper et al. [136, S. 2] gefolgt, die das Feld folgendermaßen definieren: „The study of IOR is concerned with understanding the character and pattern, origins, rationale, and consequences of such relationships. The organizations can be public, business, or non-profit and the relationships can range from dyadic, involving just two organizations, to multiplicitous, involving huge networks of many organizations“. Dieser umfassend definierte Anwendungsbereich beschreibt auch die Tatsache, dass der Fokus der Forschung die Beziehung an sich ist, unabhängig von deren Ausprägung.

Historie

Erste Unternehmensnetzwerke haben sich bereits kurz nach der industriellen Revolution gebildet. Im 19. bis hinein ins 20. Jahrhundert war die vertikale, funktionale Organisationsstruktur vorherrschend, bei der alle Funktionen, die für ein Produkt notwendig sind, vollständig innerhalb der Organisation vorhanden waren. Diese wurde letztlich abgelöst durch die bereichsübergreifende Form, die besser auf einen nun heterogenen Markt zugeschnitten war, der zum Teil verschiedene Anpassungen desselben Produktes benötigte. Erst in den 60er Jahren begann diese aufgrund von Schwierigkeiten bei der funktionsübergreifenden Koordination von der Matrix-Organisation verdrängt zu werden, welche durch flexiblere Verantwortlichkeiten auch laterale Beziehungen ermöglicht hat. Diese Entwicklung mündete schließlich in der sogenannten Netzwerkorganisation. In globalen, dynamischen Märkten wurde es letztlich unverzichtbar für Firmen, auch andere Organisationen als relevante externe Faktoren zu betrachten. Dies war der erste Schritt einer bis heute fortschreitenden Entwicklung, bei der Unternehmen ihr Business in immer kleinere, funktionale Einheiten aufteilen müssen, um weiterhin erfolgreich in einem immer spezialisierteren Markt zu sein. Dies führt letztlich dazu, dass Funktionen die früher in einer einzigen Organisation zusammengefasst waren nun über einzelne, unabhängige Organisationen oder Teile von Organisationen verteilt sind. [171]

Forschungsfeld IOR

Durch die Entstehung von IORs in der Industrie entwickelte sich somit auch die Notwendigkeit für Forschung und Entwicklung in diesem Bereich. In der Literatur beginnt die Erforschung von organisationsübergreifenden Beziehungen bereits Anfang der 1950er Jahre mit vereinzelten Veröffentlichungen zum Thema. Erst Mitte der 1960er Jahre wurden die allgemeine Systemtheorie und die Managementtheorie kombiniert, um auch Organisationen und deren interne und externe Faktoren als Systeme anzusehen, die von Managern koordiniert werden müssen. Im nächsten Jahrzehnt wurden IORs als Forschungsgebiet immer populärer. Die gemeinsame Strategie und Netzwerke von Organisationen wurden als neue Konzepte eingebracht. Viele der heute etablierten Ansichten basieren dabei auf den

frühen Arbeiten von Aldrich [178] zu Organisationstheorie und interorganisationalen Beziehungen, sowie Powell [179], der den Begriff der Netzwerkorganisation geprägt hat. Dabei wurde bereits erkannt, dass diese organisationsübergreifende Zusammenarbeit von äußeren Auswirkungen, wie politischen oder ökonomischen Faktoren, beeinflusst wird. Diese Erkenntnisse lieferten die Grundlagen für die weitere Forschung im Feld der IORs, welches sich seitdem kontinuierlich weiterentwickelt hat. Obwohl der Forschungsbereich der IORs groß und dennoch sehr fragmentiert ist, lässt er sich nach Cropper et al. [136, S. 8] wie folgt zusammenfassen: „it focuses on the properties and overall pattern of relations between and among organizations that are pursuing a mutual interest while also remaining independent and autonomous, thus retaining separate interests“. Sie zeigen außerdem, dass IORs im Kern auf Organisationen und den Beziehungen zwischen diesen basieren. Je nach Forschungsbereich und Fokus werden dabei verschieden Dimensionen definiert, um entweder die Organisationen selbst oder ihre Beziehungen zu beschreiben. Relevant sind insbesondere der Makro- und Mikro-Kontext der Organisationen, deren Beziehung und der enthaltenen Prozesse. [136]

4.1.2 Beziehungen zwischen Organisationen

Die Forschung beschäftigt sich somit mit vielen verschiedenen Aspekten von IORs. Es stellt sich die Frage, was es faktisch bedeutet, wenn zwei Organisationen eine Beziehung eingehen. Die Grundidee einer interorganisationalen Beziehung beschreibt Cousins [170, S. 75] wie folgt: „The central concept of a relationship approach is concerned with the collaboration and sharing of resources, either physical (such as machinery) or intangible (such as intellectual know-how, technological processes) as well as the primary goal of gaining competitive advantage through improvements in product and process redesign, making both firms more efficient in the supply of the end product“. Es geht im Kern also um das Teilen von Ressourcen innerhalb einer partnerschaftlichen Beziehung, um gemeinsam erfolgreicher zu sein. Diese Verknüpfung sollte laut Achrol [171, S. 68] als „minisociety of interdependent, reciprocal exchange relationships characterized by restraint of power, commitment, trust, solidarity, mutuality, flexibility, role integrity, and harmonization of conflict“ verstanden werden. Damit listet er bereits viele der elementaren Eigenschaften, die im Kontext einer IOR relevant sind. Im Folgenden sollen die Charakteristika einer solchen Zusammenarbeit genauer betrachtet werden.

IOR Eigenschaften

Eine Möglichkeit diese organisationsübergreifenden Beziehungen zu definieren ist es, die drei von Bachmann und Witteloostuijn [166] definierten Haupteigenschaften zu betrachten:

1. Es handelt sich dabei um eine formal definierte Beziehung zwischen zwei oder mehr unabhängigen Organisationen.

2. Das Ziel dieser ist es, durch die gemeinsame Nutzung der Assets aller Teilnehmer einen Mehrwert zu generieren. Dabei spielt es keine Rolle, ob es sich dabei um einen materiellen Gewinn oder einen immateriellen Wert handelt.

3. Innerhalb dieser Beziehung werden sowohl Input als auch Output von den beteiligten Organisationen geteilt.

Entwicklung einer IOR

Solche Beziehungen entwickeln sich üblicherweise nicht über Nacht, sondern bauen auf einer kontinuierlichen Zusammenarbeit der Teilnehmer auf. So ist eine IOR langfristig orientiert und basiert auf einer fortlaufenden Interaktion der Beteiligten. Die Art der Beziehung entwickelt sich jedoch mit der Zeit und wird so zunehmend intensiver werden. Allerdings müssen die Teilnehmer Zeit, Geld und andere Ressourcen investieren, damit die Beziehung langfristig funktioniert. Die Bindung zwischen den Partnern basiert dabei auf dem Verhältnis von Macht und Abhängigkeit, dem vorherrschenden Status von Konflikt oder Kooperation, der zunehmenden Verbundenheit oder Entfernung zwischen den Organisationen und letztlich der gemeinsamen Erwartungen an die Beziehung. Dies lässt sich auch auf die drei grundlegenden Werte Vertrauen (Trust), Engagement (Commitment) und Anpassung (Adaptation) zurückführen. [167]

Vertrauen

Das Konzept des Vertrauens wird im folgenden noch sehr oft aufgegriffen werden, da es sich zweifelsfrei als eines der zentralen Aspekte in IORs etabliert hat. Die meisten Veröffentlichungen [170, 136, 167, 169, 180], die sich mit der Zusammenarbeit von Organisationen beschäftigen, berücksichtigen diese Eigenschaft der Beziehung und sehen Vertrauen als wichtigen Teil einer strategischen Partnerschaft. Seit Beginn der Forschung gab es viele verschiedene und teilweise unscharfe Definitionen [181] mit unterschiedlichsten Formen [168] des Vertrauens in der Literatur. Lewicki und Bunker [182] sagen sogar, dass sich die Dynamik von Vertrauen zwischen Organisationen genauso wie zwischenmenschliches Vertrauen im Verlauf einer Beziehung stetig weiterentwickelt und es daher nicht die Eine statische Definition geben kann. Morgan und Hunt [183, S. 23] „conceptualize trust as existing when one party has confidence in an exchange partner's reliability and integrity". Sie definieren Vertrauen damit als Maß für die Verlässlichkeit eines Partners. Eine Alternative bieten Bachmann und Witteloostuijn [166, S. 4], die Vertrauen im Hinblick auf den guten Willen des Partners definieren: „Trust is the expectation that other actors will voluntarily reciprocate one-sidedly offered favors, even if this is not done immediately and directly". Diese Definition scheint die Idee des Vertrauens in IORs besser widerzuspiegeln, da sie stärker das gegenseitige Wohlwollen einer partnerschaftlichen Beziehung berücksichtigen. Achrol [171, S. 65] bezieht dabei zusätzlich noch die Allianz als Ganzes mit ein: „A firm's trust in its network partners is the belief that the partners will, without the exercise of influence or control, strive for outcomes that are beneficial for all member firms". Damit wird zum Ausdruck gebracht, dass ein hohes Vertrauen innerhalb einer IOR bedeutet, dass die Partner zum Wohlergehen der gesamten Partnerschaft handeln und nicht zu ihrem eigenen.

Definition 4.1: Vertrauen

Vertrauen beschreibt ein Maß für die Erwartungshaltung von Organisationen in einer IOR (Def. 3.1), dass alle Partner (Def. 3.2) zu jeder Zeit zum Wohle der Partnerschaft handeln.

Koordinationsstrukturen

Unabhängig vom konkreten Auslöser der Zusammenarbeit ist die übergreifende Koordination ein wichtiger Aspekt in einer IOR. Diese ist per Definition komplizierter, da die Planung die Interaktion mehrerer Organisationen erfordert, um Entscheidungen und Aktionen der Teilnehmer zu arrangieren. Einfache Beziehungen können sich dabei selbst organisieren und benötigen keine Führung, komplexere strategische Netzwerke jedoch schon [167]. Das *informelle Netzwerk* beschreibt die schwächste Form der Koordination und basiert größtenteils auf einem direkten Informationsaustausch zwischen einzelnen Personen im Rahmen von Nachrichten oder Treffen. Damit ist diese Form der Zusammenarbeit auf die niedrigste Koordinationsebene beschränkt und engere Beziehungen sollten ein stärker strukturiertes Vorgehen verwenden, wobei diese durch informelle Kommunikation unterstützt werden können. Der formelle Anteil wird durch gemeinsame Planungs- und Kontrollmechanismen etabliert. Dazu stehen verschiedene Möglichkeiten für formale Koordinationsstrukturen zur Verfügung. Die *organisationsübergreifende Gruppe* ist dabei die einfachste Variante, bei der Vertreter der teilnehmenden Organisationen ein temporäres Gremium bilden, um im Namen ihrer Organisation die gemeinsame Planung und Koordination zu übernehmen. Alternativ können die Partner auch einen *Koordinator* ernennen, eine Einzelperson, die gänzlich für die Planung und Durchführung der gemeinsamen Aktivitäten zuständig ist. Eine Erweiterung wäre die *Koordinationseinheit*, bei der eine unabhängige Organisationseinheit diese Aufgaben vollständig übernimmt, ohne jedoch für die Durchführung verantwortlich zu sein. Im Gegensatz zur organisationsübergreifenden Gruppe ist diese jedoch autonom und die Teilnehmer nicht direkt den Organisationen zugeordnet. Eine weitere unabhängige Struktur sind *nicht-administrierte Programme*, die ausgewählte Aktivitäten durch gezielte Einflussnahme (z.B. Anreize oder Strafen) von außerhalb des Organisationsnetzwerkes steuern. Ebenfalls könnte eine *Führungsorganisation* bestimmt werden, welche die notwendige Macht erhält, um Entscheidungen zu treffen und so die Zusammenarbeit zu lenken (im Unterschied zur ‚machtlosen' Koordinationseinheit). Letztlich bleibt noch die sogenannte *Einzelorganisation*, bei der eine neue Organisation gegründet wird (z.B. durch Fusion von Teilen verschiedener Organisationen), welche für die selbständige Durchführung der Aktivitäten verantwortlich ist. [135]

Normen

Egal welche Koordinationsstruktur gewählt wird, basiert die Zusammenarbeit auf dem Miteinander unabhängiger Organisationen. Daher ist es wichtig, von Anfang an die Erwartungen aller Partner zu berücksichtigen, um eine erfolgreiche Kooperation aufzubauen. Das Etablieren organisatorischer Normen kann helfen, ein gemeinsames Verständnis für die Beziehung zu schaffen und die Interessen aller Teilnehmer zu adressieren. Im Gegensatz zu rechtlich bindenden Verträgen sind solche Vereinbarungen ein leichtgewichtiger Steuerungsmechanismus. Diskrete Normen beziehen sich auf den Austausch zwischen den Organisationen und regeln dazugehörige Aspekte wie Planung, Einverständnis und Überwachung. Beziehungsnormen regeln die Beziehung an sich und sollen definieren, welches Verhalten von den Partnern innerhalb der Beziehung erwünscht oder unerwünscht ist. Ergänzt werden diese durch Normen zur moderierten Autonomie, welche festlegen sollten, welche Verhalten außerhalb der Beziehung erwartet wird, wenn diese nicht an gemeinsamen Projekten arbeiten. Alle drei Aspekte sollten in einer IOR berücksichtigt werden, insbesondere wenn daraus eine langfristige, strategische Partnerschaft entstehen soll. [169]

4.1.3 Gründe für eine Zusammenarbeit

Nachdem nun klar ist, welche Eigenschaften eine IOR besitzt und wie sie grundsätzlich aufgebaut ist, sollen die Gründe für eine Zusammenarbeit genauer betrachtet werden. Es wurde bereits etabliert, dass der Kern einer Beziehung letztlich der Erfolg aller beteiligten Organisationen und das gemeinsame Erreichen von Zielen durch Koordinieren und teilen von Ressourcen ist. Eine IOR sollte als organisationsübergreifender Prozess verstanden werden, der letztlich einen Mehrwert generieren soll (z.B. Kostenreduzierung, Innovation, Effizienz) [170]. Dabei stellt sich jedoch die Frage, welche überlappenden Zielsetzungen zwei unabhängige Organisationen eigentlich haben können.

Kategorien der Zusammenarbeit

Es gibt unterschiedliche Gründe, warum sich Organisationen für eine solche IOR entscheiden. Dabei existieren drei verschiedene Möglichkeiten, wie sich ein unorganisiertes System, d.h. ein Netzwerk von unabhängigen Organisationen, in eine organisierte Kollaborationsstruktur verwandelt. Organisationen die sich auf einen *freiwilligen Austausch* einigen, wollen durch die Interaktion ihre eigenen sowie gemeinsame Ziele erreichen. Die Teilnehmer werden versuchen, die übergreifenden Aktivitäten zu optimieren und solange dabei bleiben, wie die Beziehung ihnen einen Mehrwert liefert. Eine solche Zusammenarbeit entwickelt sich häufig innerhalb einer organisatorischen Domain. Eine Domain beschreibt eine Gruppe von verschiedenen Parteien, welche aufgrund eines gemeinsamen Problems oder Anliegens zusammenarbeiten. Andere sind aufgrund von *Abhängigkeiten* zu einer Zusammenarbeit gezwungen, wobei der Druck dazu meistens von einer besonders mächtigen Organisation ausgeht. Innerhalb einer Domain existieren häufig Assoziationen oder Abhängigkeiten zwischen den Parteien, d.h. Organisationen sind einerseits von einer Disruption der Domain betroffen (z.B. eine Störung des Marktes), können allerdings andererseits auch von den Aktionen Anderer in der Domain betroffen sein (z.B. strategische Entscheidungen von Marktteilnehmern). Das führt dazu, dass innerhalb einer Domain ein gemeinsames Interesse an der Lösung von allgemeinen Problemen besteht. Solche Beziehungen sind oftmals jedoch nicht von Dauer, da eine Organisation diese verlassen wird, sobald das Abhängigkeitsverhältnis nicht mehr vorhanden ist. Eine weitere Kategorie ist das *Mandat*, bei dem sich die Beziehung nur durch einen äußeren Einfluss entwickelt. So können etwa formelle Vereinbarungen oder rechtliche Vorgaben einen verbindlichen Rahmen für die Zusammenarbeit schaffen. [184, 176]

Definition 4.2: Abhängigkeit

Ein Partner (Def. 3.2) ist von einem anderen abhängig, wenn dessen Geschäftsziele nicht ohne den anderen erreicht werden können.

Innovationskraft

Neben der Lösung auftauchender Probleme kann die Zusammenarbeit auch der Durchführung gemeinsamer Projekte und innovativer Aktivitäten dienen. Dabei kann zwischen *gewinnbringender Zusammenarbeit*, bei der es um den Ausbau der eigenen Kompetenzen geht, sowie *forschungsorientierter Zusammenarbeit* mit dem Ziel des Aufbaus neuer Kompetenzen unterschieden werden. Organisationen können ihr Wissen in bestimmten Bereichen miteinander teilen und voneinander lernen, was letztlich die Innovationskraft jedes

Partners stärkt. Zur Umsetzung eines neuen Projektes benötigt eine Organisation häufig Betriebsmittel oder Fachkenntnisse, welche ihr nicht immer selbst zur Verfügung stehen. Innerhalb einer IOR besteht die Möglichkeit, diese Ressourcen auszutauschen oder sie sich zu teilen. Außerdem besteht gerade bei Innovationsprojekten (z.B. Produktentwicklungen) immer die Gefahr, dass diese nicht erfolgreich sind. Organisationen können sich das Risiko eines Fehlschlags durch eine Kollaboration bei solchen Aktivitäten ebenfalls teilen. Diese Vorteile führen dazu, dass IORs bei der Innovation von Produkten, Services, Prozessen und im Marketing grundsätzlich erfolgreicher sind, als es eine einzelne Organisation wäre. [173, 174, 168]

Geteilte Vorteile

Es hat sich inzwischen gezeigt, dass es für Firmen essenziell ist, ihre Lieferkette unter Kontrolle zu haben, um langfristig erfolgreich zu sein. Aus diesem Grund hat sich die übergreifende Strategie von einer breit aufgestellten Auswahl an Lieferanten zu wenigen, komplexen Beziehungen entwickelt. Bereits Deming [185][1] sagte, dass Unternehmen lieber mit weniger Suppliern arbeiten sollten, dafür mit diesen deutlich enger. Dabei sollte der Fokus nicht einzig auf der Gewinnmaximierung liegen, sondern auch auf einer Verbesserung der Produktivität und Effektivität, welche durch eine Zusammenarbeit erreicht werden kann. Eine besondere Herausforderung bei einer einfachen Beziehung zwischen zwei Firmen ist es, opportunistisches Verhalten zu verhindern. Traditionell wird davon ausgegangen, dass ein Lieferant, der nicht direkt unter Kontrolle der Organisation steht, immer seinen eigenen Vorteil maximieren will und nicht das Wohl der Beziehung im Sinn hat. Damit eine komplexe Beziehung also langfristig funktionieren kann, muss beide Parteien von der Partnerschaft gleichermaßen profitieren. [170]

Risiken einer Zusammenarbeit

Dabei bringen IORs für Organisationen nicht nur Vorteile, sondern auch Risiken mit sich, welche häufig zum Scheitern einer Beziehung führen. Durch die enge Bindung der Partner entstehen auch direkte und indirekte Abhängigkeiten voneinander. Dies ist insbesondere eine Gefahr, wenn sich die Größe der beiden Organisationen stark voneinander unterscheidet, da die Größere durch ihre Macht die strategische Ausrichtung maßgeblich beeinflussen kann. Weiterhin besteht das Risiko, dass ein Partner das zuvor genannte opportunistische Verhalten zeigt, d.h. die Beziehung nur zu seinem eigenen Vorteil nutzt und dadurch eventuell sogar den anderen Teilnehmern schadet (z.B. durch Ausnutzen von internem Wissen). Außerdem kann es auch passieren, dass die Organisationen nicht zusammenpassen und sie somit nicht in der Lage sind, sinnvoll Ressourcen zu teilen. Die Teilnehmer können dabei die geteilten Informationen missverstehen oder nicht wirksam in der eigenen Organisation einsetzen. Dadurch entstehen ihnen letztlich mehr Nachteile als Vorteile durch die Beziehung. Eine IOR beeinflusst damit die Autonomie von Organisationen und lässt den Einfluss und die Abhängigkeiten zwischen diesen verschwimmen. Daher ist die organisationsübergreifende Zusammenarbeit oftmals nicht die bevorzugte Strategie von Managern, da deren direkter Einflussbereich an den Grenzen der eigenen Organisation endet. [176, 173, 174]

[1] W. E. Deming ist insbesondere bekannt für die Adaption des ‚Plan-Do-Check-Act Zyklus' in der Managementtheorie, der heute auch die Basis für die ISO/IEC 27001 und andere Managementsysteme ist.

4.1.4 Eigenschaften verschiedener Beziehungen

Faktoren einer Beziehung

Organisationsübergreifende Beziehungen lassen sich grundsätzlich anhand von vier Faktoren unterscheiden. Sozio-organisatorische (Socio-organizational) Faktoren definieren, auf welcher Basis zwei Organisationen miteinander agieren. Es kann zwischen den zwei Mechanismen Macht (Power) und Vertrauen (Trust) unterschieden werden, welche eine unterschiedliche Erwartungshaltung an die beteiligten Organisationen beschreibt. Während die Quelle von Macht üblicherweise organisatorische Vereinbarungen (z.B. Verträge) sind, ist es beim Vertrauen eher das Verhältnis zwischen den Beteiligten (insbesondere zwischen einzelnen Personen). In einer auf Dominanz basierenden Beziehung werden die Teilnehmer das tun, was die Entität mit der meisten Macht fordert, unabhängig von ihren eigenen Wünschen. Basiert die Beziehung jedoch auf Vertrauen, werden die Teilnehmer sich freiwillig gegenseitige Gefallen erweisen. Beide Mechanismen sind sowohl in vertikalen als auch horizontalen Beziehungen zu finden. Sozio-rechtliche (Socio-legal) Faktoren beschreiben rechtlich bindende Aspekte einer Beziehung. Sie werden üblicherweise durch Verträge definiert, welche die Zusammenarbeit verschiedener unabhängiger Organisationen erst ermöglichen. Inhaltlich können sie die Verantwortlichkeiten, Pflichten und Erwartungen jeder Partei definieren. Dabei schaffen Verträge immer nur einen Rahmen der Zusammenarbeit, da sie in komplexen Partnerschaften niemals alle Eventualitäten abdecken können. Sozialpsychologische (Socio-psycholocigal) Faktoren nehmen Bezug auf die menschlichen Aspekte einer Beziehung. Letztlich basiert jede Form der Zusammenarbeit von Organisationen auf Interaktionen zwischen einzelnen Personen, welche essenziell für eine effektive Kooperation sind. Dabei haben sowohl objektive Eigenschaften (z.B. Ausbildung) als auch subjektive Eigenschaften (z.B. Persönlichkeit) der Person Einfluss auf die Beziehung, insbesondere das Vertrauen. Soziotechnische (Socio-technical) Faktoren beschreiben das Teilen von Wissen zwischen den Organisationen (mit Hilfe von Kommunikationstechnologien). Hier sind die Eigenschaften der Artefakte relevant, die geteilt werden sollen, d.h. deren technische Repräsentation. Weiterhin gehören dazu auch die Wege, wie eine Information geteilt wird. Abhängig vom kulturellen, wirtschaftlichen und sozialem Umfeld der Organisationen sind diese mehr oder weniger zur Weitergabe ihrer Daten bereit. [166]

Definition 4.3: Autorität

Autorität beschreibt, ob der Einfluss der Partner innerhalb einer IOR (Def. 3.1) machtbasiert oder vertrauensbasiert (Def. 4.1) erfolgt.

Quellen von Vertrauen

Das Vertrauen ist somit ein zentraler Aspekt in IORs, insbesondere, wenn die Beziehung nicht aufgrund einer Abhängigkeitsbeziehung besteht. Dabei lassen sich wiederum drei verschiedene Arten definieren, welche sich darin unterscheiden, worauf das Vertrauen basiert. Die Basis jeder Geschäftstransaktion ist das *vertragliche Vertrauen* (Contractual Trust). Sobald zwei Parteien eine Leistungserbringung vereinbaren, vertraut jede Seite darauf, dass die Andere ihren Teil der Abmachung einhält. Nur wenn beide Partner darauf Vertrauen können, dass der Andere seine Zusagen auch einhält, dann kann eine erfolgreiche Zusammenarbeit entstehen. Eine weitere Möglichkeit ist das *Vertrauen in die Kompetenz*

(Competence Trust) des Geschäftspartners. Da extern erbrachte Leistungen außerhalb der Kontrolle einer Organisation liegen, wird deren Qualität grundsätzlich hinterfragt. Je höher das Vertrauen in die Kompetenz der Partner ist, desto wahrscheinlicher verlässt sich eine Organisation auf die erzeugten Ergebnisse. Letztlich ist das *Vertrauen in den guten Willen* (Goodwill Trust) ein Maß für die Hingabe einer Organisation zur Beziehung. Im Gegensatz zu vertraglichem Vertrauen wird nicht die Erfüllung bestimmter Forderungen erwartet, sondern die allgemeine Verlässlichkeit in der Beziehung. Können sich die Partner aufeinander verlassen, so wird die Wahrscheinlichkeit für opportunistisches und egoistisches Verhalten geringer. [181]

(Nicht-) Interaktive Beziehungen

Die Beziehung zweier Organisationen kann anhand von zwei Dimensionen definiert werden. Nicht-interaktive Beziehungen, bei denen die Organisationen bestimmte Attribute teilen, z.B. Status, Strategie oder Struktur. Interaktive Beziehungen sind deutlich häufiger, bei denen es um den Austausch von Informationen oder Ressourcen geht. Diese lassen sich in drei Aspekten aufteilen. Der *Inhalt* bezieht sich auf den Informationsfluss und Austausch von Ressourcen zwischen den Organisationen. Die *Struktur* beschreibt die Assoziationen zwischen den verschiedene Organisationen. Der Governance Mechanismus beschreibt wie die Teilnehmer die Beziehung koordinieren und auf welcher Basis (Macht oder Vertrauen) dies geschieht. [136]

Nähe von Organisationen

Ein weiterer wichtiger Aspekt für IORs ist die Nähe (Proximity) zwischen den beteiligten Organisationen. Dieses Konzept beschreibt auf verschiedenen Ebenen, welche Gemeinsamkeiten zwei Organisationen haben, auf denen die Beziehung aufbauen kann. Für IORs sind dabei insbesondere drei Dimensionen relevant, deren Wert für eine erfolgreiche Allianz angemessen hoch sein muss. *Organisatorische Nähe* bezeichnet die Ähnlichkeit von Organisationen in Bezug auf ihre Struktur, Arbeitsweise, Unternehmenskultur oder Zusammenhänge (z.B. deren Netzwerk). Je ähnlicher zwei Organisationen sind, desto höher ist die Wahrscheinlichkeit, dass Informationen für beide relevant sind und ein Wissensaustausch oder eine Kombination von Ressourcen für gemeinsame Innovationsprojekte sinnvoll ist. Bei der *technologischen Nähe* geht es nicht um eingesetzte Technik, sondern um das Verständnis von Technologien und Prozessen. Dabei wird davon ausgegangen, dass zwei Organisationen auf einer ähnlichen Wissensgrundlage aufbauen müssen, um das in der Beziehung gewonnene Wissen überhaupt sinnvoll einsetzen, d.h. voneinander lernen, zu können. *Geografische Nähe* beschreibt die tatsächliche Entfernung der Organisationen bzw. deren Mitarbeiter, da räumliche Nähe einen häufigen und direkten (Wissens-)Austausch zwischen den Akteuren ermöglicht. Abhängig von der Beziehung kann auch eine temporäre geografische Nähe durch regelmäßige Treffen etabliert werden. [175]

Definition 4.4: Nähe

Die Nähe ist ein Maß für die Gemeinsamkeiten von Organisationen.

Interesse

Die bisher genannten Eigenschaften zielten alle darauf ab, Gemeinsamkeiten zwischen den Partnern zu beschreiben, welche die Intensität der Beziehung erhöhen können. Eine Partnerschaft basiert jedoch trotz aller Bestrebungen einer engen Zusammenarbeit immer auf der Prämisse, dass jeder Partner letztlich die eigenen Ziele erreichen will. Diese Voraussetzung bildet die Grundlage dafür, dass eine Organisation überhaupt eine Beziehung eingeht. Somit steht weiterhin die eigene Organisation im Mittelpunkt, denn diese versucht üblicherweise ihre Interessen und eigenen Vorteile durch die Partnerschaft zu maximieren.
Es ist anzunehmen, dass zwei Organisationen nicht zusammenarbeiten, wenn deren Ziele konträr sind bzw. die notwendigen Aktivitäten sich gegenseitig ausschließen. Gleichzeit ist somit denkbar, dass in einer engen Partnerschaft auch die Ziele der Partner miteinander verflochten sind. In dieser Hinsicht nennen Tuusjärvi und Möller [169] drei Arten von Interessen einer Organisation, die bei einer Kooperation zu berücksichtigen sind:

- Das *Eigeninteresse* der Organisation, welche auch der Grund ist, wieso sie die Partnerschaft eingeht.
- Das *strategische Interesse* einer Organisation und ihres Netzwerks.
- Das *gemeinsame Interesse*, welche die Organisation mit den Partnern verbindet.

Darauf aufbauend lassen sich diese unterschiedlichen Interessen auch als Attribute einer IOR betrachten. Bei einer schwachen Beziehung dominieren das Eigeninteresse[2] der eigenen Organisation die Interessen der anderen Partner. Die Beziehung wird stärker, wenn das strategische Interesse auf dem Erfolg der Zusammenarbeit beruht. In einer engen Partnerschaft überwiegt letztlich das gemeinsame Interesse bzw. die Ziele und Interessen der Partner sind identisch.

Definition 4.5: Interesse

Das Interesse gibt an, ob für einen Partner (Def. 3.2) die eigenen, strategischen oder gemeinsamen Ziele im Vordergrund stehen.

[2]Das Eigeninteresse ist eine grundlegende Eigenschaft jeder Organisation, da sie ansonsten keine Ziele hätte. Das würde bereits der Definition einer Organisation als „einheitlich aufgebauter Verband, Zusammenschluss von Menschen zur Durchsetzung bestimmter Interessen, Zielsetzungen o. Ä.“ [186] widersprechen.

4.2 Generische Beziehungstypen

Im vorherigen Abschnitt wurden die grundlegenden Eigenschaften einer IOR beschrieben und besonders relevante Attribute hervorgehoben. Diese verschiedenen Attribute einer Beziehung liefern die Grundlage für die in dieser Arbeit unterschiedenen Arten von IORs. Dabei ist für Zusammenarbeit im CISRM jedoch insbesondere die Art und Intensität der Zusammenarbeit relevant, weniger die Organisationsstruktur. Verschiedene Beziehungstypen sind unterschiedlich gut geeignet, ein bestimmtes Ergebnis zu produzieren und so ist es wichtig, eine für das Ziel angemessene Beziehung zu etablieren [170]. Daher ist es essenziell, die Art der IOR zu berücksichtigen, wenn Organisationen in bestimmten Aktivitäten zusammenarbeiten wollen.

CISRM

Somit spielt der Beziehungstyp auch eine wichtige Rolle, wenn es darum geht, ein gemeinsames CISRM zu etablieren. Dabei handelt es sich letztlich auch nur um eine gemeinsame Aktivität aus dem Bereich ISM, bei der eine Zusammenarbeit nicht in jeder IOR sinnvoll ist. Es geht also darum, einen wirksamen Anwendungsbereich (bezogen auf die Beziehung) für das CISRM zu definieren. Dieser legt fest, in welchen IORs eine Zusammenarbeit im ISRM möglich/wirksam ist und in welchen voraussichtlich nicht. Daher sollen, basierend auf den vorgestellten Merkmalen von Beziehungen, im folgenden generische Beziehungstypen definiert werden.

Beziehungstypen

Bereits im letzten Kapitel wurden verschiedene Ausprägungen von Beziehungen vorgestellt, wie sie in der Praxis anzutreffen sind (Abschnitt 3.1). Dazu gehörten das *Joint Venture* als gemeinsame Unternehmung, der strategische *Verbund* von Organisationen und der *Konzern* bestehend aus mehreren Unternehmen. Obwohl diese Szenarien unterschiedliche Organisationen und Organisationsformen enthalten, deren Strukturen, Hierarchien und Zusammenhänge verschieden aufgebaut sind, wäre die Anwendung des CISRM als interorganisationaler Prozess in allen Fällen denkbar. Die Frage ist, was diese Beziehungen auszeichnet und wie sie anhand ihrer allgemeinen Eigenschaften klassifiziert werden können.

Klassifikation

Im Folgenden werden verschiedene Arten von Beziehungen vorgestellt, die in der Literatur auf Basis ihrer Organisations- oder Koordinationsstruktur unterschieden werden. Diese sind allerdings nicht besonders gut geeignet, um die Intensität einer Beziehung und damit die Eignung für gemeinsame Prozesse zu bewerten. Stattdessen werden drei generische Beziehungstypen für IORs zwischen zwei oder mehr Organisationen bzw. Organisationsteilen definiert, die sich an die existierenden Einteilungen anlehnen. Diese erlauben den Anwendungsbereich für das CISRM besser abgrenzen, als bei der Festlegung auf bestimmte Organisationsformen der Fall wäre. Dabei wird insbesondere diskutiert, welche Art des ISRM in der Beziehung denkbar wäre. Diese Beziehungstypen bilden die Grundlage für das dreistufige Partnerschaftsmodell, welches im nächsten Abschnitt als Hilfsmittel zur Bewertung von IORs vorgestellt wird.

4.2.1 Abgrenzung von Beziehungstypen

Arten von Beziehungen

Vor der Definition eigener Beziehungstypen sollten zuerst existierende Klassifikationen betrachtet werden. Verschiedenste Veröffentlichungen beschreiben bereits organisatorische Beziehungstypen im Einzelnen oder zusammenhängend. Dabei sind diese jedoch meist nicht darauf ausgerichtet, die Art und Intensität der Zusammenarbeit innerhalb einer Partnerschaft zu beschreiben. Diese Eigenschaften sind allerdings wichtig, um die zu bewerten, ob sich eine IOR für die Zusammenarbeit in interorganisationalen Prozessen eignet.

Zur Einordnung der verschiedenen Arten von Koordination wurde von Hamm [187] ein Koordinationswürfel mit den drei Dimensionen „Steuerung“, „Aufgabenzuordnung“ und „Kommunikation“ entwickelt. Der Aspekt *Steuerung* beschreibt die Entscheidungsgewalt innerhalb der Beziehung, bzw. wie die Partner Entscheidungen treffen. Diese Eigenschaft liegt damit sehr nah an dem, was hier als Autorität (Def. 4.3) definiert wurde. Die *Aufgabenzuordnung* definiert, wie die Aktivitäten in der IOR verteilt werden oder ob die Organisationen diese unabhängig voneinander durchführen. Letztlich beschreibt die *Kommunikation* den Informationsfluss innerhalb der Beziehung und welche Partner direkt Daten austauschen. Darauf aufbauend wurden Koordinationsmuster definiert und zwischen hierarchischen und heterarchischen Beziehungen unterschieden, um die Struktur eines Service Provider Netzwerks auf Basis der drei Dimensionen zu beschreiben. Die hierarchische Beziehung definiert eine klar strukturierte Beziehung zwischen einem zentralen Provider und mehreren Sub-Providern. Diese Beziehung kann als klassische Supply Chain angesehen werden, bei der eine Organisation von mehreren Lieferanten beliefert wird. Im Gegensatz dazu definiert die Heterarchie eine kooperative Organisationsstruktur, bei der die Teilnehmer gleichberechtigt an der gemeinsamen Zielerreichung arbeiten. [187, 188]

IOR Typen

Bachmann und Witteloostuijn [166] definieren vier Typen von organisationsübergreifenden Beziehungen, abhängig von den Quellen für Macht und Vertrauen in der Beziehung. Dabei lässt sich zwischen den reinen (Macht und Vertrauen gehen jeweils von derselben Entität aus) und hybriden (Macht und Vertrauen gehen von verschiedenen Entitäten aus) Typen unterschieden. Die vollständig institutionalisierte Form basiert fundamental auf festen Strukturen, bei denen die Aspekte der Beziehung vertraglich detailliert festgelegt sind. Diese Verträge definieren klare Machtverhältnisse zwischen den Organisationen, wobei die Macht üblicherweise bei einer Organisation liegt. Damit ergibt sich ein hierarchisches System mit festen Entscheidungsstrukturen, wie es auch in einem klassischen Unternehmen vorzufinden ist. Aus dieser Zentralisierung der Macht ergibt sich automatisch auch ein Vertrauen zwischen den Beteiligten, da die Interaktionen untereinander erwartbar und mit einem minimalen Risiko verbunden sind. Im Kontrast dazu steht die vollständig personalisierte Form. Dabei gehen Macht und Vertrauen von einzelnen Personen aus, ohne das diese durch organisatorische Rahmenbedingungen wie Verträge gestützt werden. Entscheidungen basieren auf dem Verhältnis dieser Personen, meist Manager, zueinander und der Tatsache, dass sie sich mit Ressourcen gegenseitig unterstützen wollen. Je nachdem ob Macht oder Vertrauen die dominierende Eigenschaft darstellt, kann das die Beziehung beeinflussen, da Personen mit mehr Macht eher versuchen können, verfügbare Ressourcen zu ihren Zwecken zu nutzen. Bei den hybriden Formen besitzt entweder die Organisation oder die Person

jeweils die Macht bzw. das Vertrauen und umgekehrt. So könnte das Vertrauen bei der Organisation und die Macht bei einzelnen Personen liegen. Daraus ergibt sich eine Struktur mit grundsätzlichen Vereinbarungen auf organisatorischer Ebene, aber der Notwendigkeit, Macht auf der persönlichen Ebene aufzubauen. Das Gegenstück basiert auf persönlichem Vertrauen, während die Macht bei der Organisation liegt. Dabei existieren klare hierarchische Strukturen und Regeln in der Beziehung, während Gleichzeitig eine Kultur der kooperativen Problemlösung vorherrscht. Vertrauen zwischen den einzelnen Personen ist insbesondere essenziell, damit die formale Macht nicht durch opportunistisches Verhalten die Kollaboration behindert.

Horizontales und vertikales Vertrauen

Es ist anzunehmen, dass organisatorisches Vertrauen in horizontalen Beziehungen geringer ist als in vertikalen Beziehungen. So ist die Wahrscheinlichkeit für opportunes Verhalten in horizontalen Beziehungen deutlich höher als in vertikalen. Schließlich besteht immer die Gefahr, dass die Partner die Kooperation nur für den eigenen Vorteil missbrauchen. In vertikalen Allianzen stammen die Partner meistens aus verschiedenen Märkten und stehen somit nicht in direkter Konkurrenz zueinander. Weiterhin sind Abhängigkeiten bei horizontalen Allianzen deutlich schwächer ausgeprägt oder gar nicht vorhanden, da diese nicht in einem direkten Abhängigkeitsverhältnis stehen. In einer vertikalen Allianz besteht ein für die Partner essenzieller Austausch von Ressourcen oder Dienstleistungen, ohne die eine Organisation ihre eigenen Ergebnisse nicht produzieren kann. Trotz dieser Gründe für geringeres Vertrauen lässt sich allerdings auch argumentieren, dass dieses für horizontale Beziehungen eine geringere Rolle spielt als für vertikale Beziehungen. Diese etablieren sich üblicherweise zwischen Organisationen, die bereits eine gewisse Nähe zueinander aufweisen. Dadurch ist es wahrscheinlich, dass bereits persönliche und institutionelle Verbindungen bestehen, die eine Kooperation voraussetzen. [177]

IOR Levels

Aus Sicht einer einzelnen Organisation kann die Kooperation mit anderen Organisationen stufenweise betrachtet werden. Dabei basiert jede Beziehung auf einzelnen Interaktionen, die letztlich zu längeren Episoden und infolge dessen einer intensiveren Zusammenarbeit führen können. Die einfachste Beziehung die sich aus mehreren erfolgreichen Episoden ergeben kann ist die *Zweiergruppe*. Beide Akteure unterstützen sich dabei gegenseitig und helfen sich die eigenen Ziele zu erreichen, wobei der Mehrwert auch in der Beziehung selbst liegen kann. Geht eine Organisation mehrerer solcher Beziehungen ein, kann von einem *Portfolio* gesprochen werden. Diese koordinierte Zusammenarbeit kann genutzt werden, um eines oder mehrere Ziele zu erreichen und sie liefern in Summe mehr als es jede einzelne Verbindung könnte. Als Erweiterung davon kombiniert das *Netz* alle Portfolios einer Organisation. Abhängig davon, wie gut die einzelnen Portfolios aufeinander abgestimmt werden können, liefern sie ebenfalls in ihrer Gesamtheit die Möglichkeit, einen erhöhten Mehrwert zu generieren. Das höchste Level stellt das *Netzwerk* dar, welches Verbindungen in einer kompletten Branche bzw. einem Markt betrachtet. [167]

Netzwerkformen

Achrol [171, S. 59] definiert Netzwerkorganisationen wie folgt: „a network organization is distinguished from a simple network of exchange linkages by the density, multiplexity, and reciprocity of ties and a shared value system defining membership roles and responsibilities“. Er beschreibt dazu vier mögliche Formen eines Unternehmensnetzwerks. Eine *Interne Netzwerkorganisation* (Internal Market Networks) beschreibt eine Struktur, bei der eine

Organisation aus mehreren, unabhängigen Teilbereichen besteht, wodurch die hierarchischen Abhängigkeiten größtenteils aufgelöst werden. Obwohl diese weiterhin die Organisationsrichtlinien gebunden sind, arbeiten sie dennoch als gewinnorientierte Profitcenter[3] mit internen und externen Kunden. Im Gegensatz dazu besteht eine *Vertikale Netzwerkorganisation* (Vertical Market Networks) aus unabhängigen Organisationen, die im Zuge einer Lieferantenbeziehung zusammenarbeiten. Die Teilnehmer der Beziehung sind häufig spezialisierte Zulieferer, während nur eine zentrale Organisation eine integrierende Rolle einnimmt. Eine Erweiterung davon stellt die *Marktübergreifende Netzwerkorganisation* (Intermarket Network) dar. Sie verbindet Teilnehmer eines vertikalen Netzwerks aus unzusammenhängenden Branchen, welche insbesondere durch geteilte Ressourcen, strategische Entscheidungen und gemeinsame Aktivitäten eine übergreifende Unternehmensgruppe bilden. Letztlich kann das *Chancen-Netzwerk* (Opportunity Network) als eine Art dynamische Zusammenarbeit angesehen werden. Dabei gehen mehrere Organisationen eine temporäre Beziehung ein, um ein bestimmtes Projekt zu verwirklichen oder ein gemeinsames Problem zu lösen.

Vorteile der Ansätze

Damit bilden die verschiedenen Netzwerkformen sehr gut die vorher beschriebenen Chancen und Risiken ab, die eine IOR mit sich bringt. Die interne Netzwerkorganisation ist dabei ein gutes Beispiel dafür, dass selbst große Unternehmen versuchen ihre monolithischen Strukturen aufzubrechen und damit Kontrolle aufgeben, um stattdessen eher ein flexibleres Unternehmensnetzwerk aufzubauen. Die Teilnehmer einer vertikalen Netzwerkorganisation wollen durch die Zusammenarbeit die eigenen bzw. gemeinsamen Ziele erreichen und sind dafür bereit, ein Abhängigkeitsverhältnis einzugehen. Schließen sich Organisationen freiwillig zu einer Marktübergreifenden Netzwerkorganisation zusammen, geschieht dies, um die Innovationskraft der Teilnehmer zu erhöhen, obwohl es mit Risiken durch opportunistisches Verhalten innerhalb der Gruppe einhergeht. Im Chancen-Netzwerk wird versucht komplexe Aktivitäten zu verwirklichen, die für eine Organisation alleine zu schwierig wären. Dabei wird die Umsetzung durch die befristete Zusammenarbeit erst ermöglicht, aber sie zwingt die Teilnehmer ebenfalls, ihr eigenes Verhalten kurzfristig an die Partner anzupassen.

Nachteile der Ansätze

Leider liefern all diese Definitionen und Klassifizierungen hauptsächlich eine Aussage darüber, wie die Struktur der Zusammenarbeit in einer IOR aussieht. Sie liefern kaum Informationen darüber, wie eng die Zusammenarbeit zwischen verschiedenen Organisationen ist. Dies wäre jedoch die notwendige Klassifikation, um den Anwendungsbereich des CISRM festzulegen. Die Beziehungstypen sollen es ermöglichen zu klassifizieren, wie eng bzw. intensiv eine Gruppe von Organisation zusammenarbeitet. Daher wird im Folgenden versucht, eine neue Klassifikation auf Basis der existierenden Ansätze zu erstellen.

Beziehungstypen

Unter Berücksichtigung der existierenden Strukturen erscheint zumindest eine sehr einfache Form der Zusammenarbeit die unterstützende Beziehung zu sein. Sie ist eine Ausprägung eines vertikalen Netzwerks und bereits in einer Zweiergruppe möglich. Alle anderen Kooperationsformen benötigen ein höheres Vertrauen, um etwa gemeinsam in einem Marktübergreifenden oder Chancen-Netzwerk zusammenzuarbeiten. In diesem Zusammenhang

[3] Autonomer Teilbereich einer Organisation mit direktem Marktzugang, der wie ein selbständiges Unternehmen geführt wird. [189]

versucht auch ITIL verschiedene Partnerschaften zu spezifizieren, die sich darauf anwenden lassen. Dort wird die Intensität der Zusammenarbeit, wie beim Interesse einer Organisation, auf Basis der Ziele definiert. *ITIL 4: Create, Deliver and Support* [190] unterscheidet dabei zwischen der Kooperation als „Working with others to achieve your own goals“ und der Kollaboration als „Working with others to achieve common shared goals“. Die Unterscheidung zwischen den beiden Beziehungstypen basiert anhand dieser Definition also auf der jeweiligen Zielsetzung und nicht auf der Struktur der Organisation.

4.2.2 Unterstützende Beziehung

Eine unterstützende Beziehung setzt grundsätzlich die eigene Organisation ins Zentrum und ist drauf ausgelegt, einen möglichst großen Mehrwert für diese zu generieren. Sie sind die klassische Form der vorgestellten vertikalen Netzwerkorganisation, bei der verschiedene Teilnehmer an der Herstellung eines Produktes oder einer Dienstleistung beteiligt sind. Die unterstützende Beziehung stellt lediglich eine funktionale Beziehung mit dem Fokus auf eine Verbesserung der Produktion dar und unterscheidet sich daher grundlegend von einer strategischen Allianz [171]. Damit ist die Art der Zusammenarbeit nicht besonders intensiv und es handelt sich dabei nur um eine sehr schwach ausgeprägte IOR.

Definition 4.6: Unterstützende Beziehung

Eine direkte, funktionale Beziehung zwischen zwei Organisationen zum Erreichen **unabhängiger Ziele** der Partner (Def. 3.2).

Lieferanten

Lieferanten sind Organisationen oder Teile davon, welche eine Leistung einer anderen Organisation zur Verfügung stellen. Diese Lieferanten können sowohl interne als auch externe Organisationseinheiten sein. Ein interner Lieferant stellt die Leistung einem anderen Teil derselben Organisation (interne Netzwerkorganisation), ein externer einer anderen Organisation bereit (vertikale Netzwerkorganisation). Die Organisationen stehen dabei in einem Abhängigkeitsverhältnis, welches bei externen Lieferanten meist vertraglich begründet ist. Intern besteht die Abhängigkeit aufgrund der Unternehmenshierarchie oder internen Service Level Agreements (SLAs). Beides sind Ausprägungen von starken sozio-rechtlichen Faktoren einer Beziehung. Aus diesem Grund wird diese Beziehungsform auch einfach als Hierarchie bezeichnet [188]. Die unterstützende Beziehung ist damit ein Beispiel für eine IOR, die sozio-organisatorisch fast vollständig auf Macht aufgebaut ist.

Supply Chain Modell

Bei der unterstützenden Beziehung stehen einzelne Organisationen in direkter Beziehung zueinander, oftmals in den Rollen Kunde und Lieferant, etwa bei einer Lieferantenbeziehung. Dabei kann natürlich jede Organisation beliebig viele unterstützende Beziehung eingehen (1:n Beziehung), aber diese sind grundsätzlich unabhängig voneinander. Auch wenn der Kunde die verschiedenen Dienstleistungen zu einem Produkt kombiniert und so für ihn Abhängigkeiten mit mehreren Lieferanten entstehen, spielt dies für die einzelne Beziehung keine Rolle. Abbildung 4.1 zeigt dies beispielhaft an drei Organisationen. Dabei bezieht Org_A in der Rolle Kunde Leistungen von den Lieferanten Org_B und Org_C. Jede

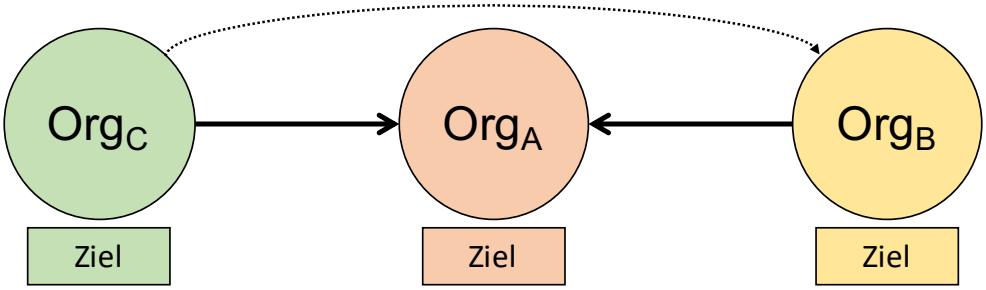


Abbildung 4.1: Struktur einer unterstützenden Beziehung

dieser Organisation hat ihre eigenen Ziele und die Zusammenarbeit hilft ihnen, diese zu erreichen. Dabei ist es für die Partner unwichtig, ob der jeweils andere seine eigenen Ziele erreicht oder nicht. Weitere Beziehung zwischen den Partnern, z.B. Org_B und Org_C, sind zwar möglich, jedoch nicht relevant. Diese bilden dann jedoch eine eigene, unabhängige unterstützende Beziehung.

Lieferanten im RM

Das ERM beschäftigt sich traditionell mit Risiken und dem Umgang mit diesen innerhalb der eigenen Organisation. Damit ist es nicht geeignet, um einen RM Ansatz zu unterstützen, welcher über die Grenzen der Organisationen hinausgeht. Einen Schritt weiter geht das SCRM, welches sich auch im Kontext der IS auf die durch Lieferanten eingebrachten Risiken bezieht. Damit wird das ERM allerdings lediglich um eine Kategorie von Risiken erweitert, welche sich aus der Zusammenarbeit mit Lieferanten ergeben. Diese Supplier Risks (SRs) sind für die Kundenorganisation etwa der Ausfall oder die Kompromittierung des Lieferanten, bzw. letztlich der eingekauften Leistung, welche im ISRM zu einem Verlust der Schutzziele führt. Ein gemeinsames RM kann den Parteien helfen, die Risiken innerhalb der Partnerorganisationen besser zu verstehen. Dies erfordert jedoch eine gewisse Offenheit im Umgang mit IS bezogenen Informationen und die Bereitschaft, mit Lieferanten zu zusammenzuarbeiten und dabei SRs als gemeinsame Risiken anzuerkennen. [30]

Gemeinsames SCRM

Weiterhin identifiziert Li et al. [30] zwei Kernaspekte des gemeinsamen SCRM: (1) den Austausch von risikobezogenen Informationen zwischen den Partnern (*risk information sharing*) und (2) die Etablierung einer gemeinsamen RM Methodik und Zuweisung von Verantwortlichkeiten (*risk sharing mechanism*). Ersteres ist essenziell, um die Risiken der einzelnen Organisationen untereinander sichtbar zu machen und damit ein übergreifendes Bewusstsein für diese zu schaffen. Zweiteres dreht sich um die konkrete Methodik die genutzt wird, um diese Informationen zwischen den Partnern auszutauschen. Beide Aspekte sind notwendig, um sowohl das SCRM zu erweitern als auch das interne ERM in einer unterstützenden Beziehung auf die Partnerorganisationen auszudehnen und ein gemeinsames SCRM zu ermöglichen. Dabei hat sich gezeigt, dass die Länge der bestehenden Partnerschaft, das Vertrauen zwischen den Partnern und ein gemeinsames Verständnis des SCRM wichtige Eigenschaften sind, welche das Teilen von Informationen unterstützen.

SCR Eventuell kann behauptet werden, dass SRs nur in eine Richtung fließen, nämlich vom Lieferanten zum Kunden. Dies setzt voraus, dass die Risiken des Kunden keinen Einfluss auf die IS des Lieferanten haben können. Dies ist sicherlich für unmittelbare Bedrohungen der Fall, so das etwa ein Angriff auf den Lieferanten zu verschiedenen Risiken in Bezug auf die Schutzziele des Kunden führen kann. Im Gegenzug hat ein Angriff auf den Kunden keine direkten Auswirkungen auf den Lieferanten. Indirekt beeinflusst allerdings die Bedrohungslage und das Risikoniveau des Kunden auch die Risikobewertung des Lieferanten. Liefert ein Lieferant eine Leistung an einen Kunden mit einem hohen Risikoprofil, so kann sich damit auch die Eintrittswahrscheinlichkeit oder die Auswirkung von Risiken erhöhen, welche die bereitgestellte Leistung bedrohen. Weiterhin sind auch ERM Risiken des Kunden, etwa die Offenlegung von Informationen, von Bedeutung für den Lieferanten, auch wenn diese nicht von der bereitgestellten Leistung verursacht werden, aber damit in Zusammenhang stehen.

4.2.3 Kooperative Beziehung

Eine kooperative Beziehung zeichnet sich durch eine enge Zusammenarbeit der Organisationen aus, die an einer gegenseitigen Wertschöpfung ausgerichtet ist. Dabei ist diese Form deutlich mehr an einer gemeinsamen, langfristig ausgerichteten Partnerschaft orientiert, als dies bei einer unterstützenden Beziehung der Fall ist. Für eine solche Beziehung ist nicht nur ein höheres Maß an Vertrauen notwendig, sondern auch die Möglichkeit für alle Organisationen zusätzliche Vorteile aus der Partnerschaft zu ziehen. Die Art der Zusammenarbeit entwickelt sich dabei von einer rein vertikalen Beziehung mit klaren organisatorischen Grenzen zu einer integrierten Produktion mit geteilten Verantwortlichkeiten bei bestimmten Aktivitäten. Dies bietet den Organisationen die Möglichkeit, langfristiger zu planen und Produkte koordiniert zu entwickeln. [172]

Definition 4.7: Kooperative Beziehung

Langfristig ausgerichtete Beziehung zwischen zwei oder mehr Organisationen, welche auf das Erreichen der **strategischen Ziele** der einzelnen Partner (Def. 3.2) ausgelegt ist.

Partnerschaft Obwohl eine kooperative Beziehung als Weiterentwicklung der unterstützenden Beziehung gesehen werden kann, könnte sie auch unabhängig davon entstehen. So könnten sich etwa Organisationen in der gleichen Branche zusammenschließen, um gemeinsame Produkte zu entwickeln. Es kommt vor, dass Produktionsfirmen und IT-Unternehmen strategische Partnerschaften eingehen, um damit jeweils das eigene Portfolio zu erweitern. Ein Beispiel für eine solche Kooperation findet sich etwa bei der Zusammenarbeit von Automobilherstellern und Technologieunternehmen. Dabei sind beide Teil einer Partnerschaft, bei der langfristig an integrierten Produkten gearbeitet wird. Die Zusammenarbeit ist intensiver als bei einer klassischen unterstützenden Beziehung und auch die Ziele der Organisationen sind aneinander ausgerichtet. Damit ist die Abhängigkeit zwischen den Organisationen automatisch

höher als in einer unterstützenden Beziehung. Denn eine gegenseitige Abhängigkeit entsteht entweder, wenn Ergebnisse nur durch Zusammenarbeit erreicht werden können oder Aktivitäten selbst nur gemeinsam sinnvoll durchgeführt werden können [135]. Damit ist nachvollziehbar, warum das Vertrauen zwischen den Partnern bei zunehmender Intensität der Beziehung immer wichtiger wird.

Macht Ungleicheit

Gleichzeitig verändern sich auch die Machtverhältnisse, da in einer IOR entweder Macht oder Vertrauen dominiert (egal ob institutionalisiert oder persönlich). So intensiver die Beziehung wird, desto wichtiger wird somit ein Gleichgewicht zwischen den Partnern, welches insbesondere in der gemeinsamen Entscheidungsfindung Ausdruck findet. Dabei ist es wichtig, dass keine Organisation innerhalb der Allianz zu viel Macht und somit Einfluss erhält, da sonst keine partnerschaftliche Beziehung mehr möglich ist. Sako [181] nennt dabei den „power inequality threshold“, einen Grenzwert der bei Überschreitung dazu führt, dass der schwächere Partner sich von der Macht des stärkeren bedroht fühlt. Dadurch wird die Partnerschaft an sich infrage gestellt, das Vertrauen zwischen den Partnern sinkt und die Wahrscheinlichkeit für opportunistisches Verhalten steigt. Letztlich ist anzunehmen, dass dadurch das Eigeninteresse der Organisation in den Vordergrund rückt, wodurch maximal noch eine unterstützende Beziehung möglich ist.

Modell der Kooperation

Die Struktur einer kooperativen Beziehung ist auf den ersten Blick ähnlich zu einer unterstützenden Beziehung, wie Abbildung 4.2 zeigt. Der Hauptunterschied zur unterstützenden Beziehung liegt darin, dass die Zusammenarbeit in beide Richtungen verläuft und die Ziele aneinander ausgerichtet sind. Die Zusammenarbeit ist hier für die Partner essenziell, da sie direkt deren strategischen Interessen unterstützt. Somit sollen durch die Durchführung der gemeinsamen Aktivitäten die Ziele aller Partner erreicht werden. Im Gegensatz zur unterstützenden Beziehung kann die Kooperation auch zwischen mehreren Organisationen stattfinden (n:n Beziehung), falls deren Ziele aufeinander abgestimmt sind. Dabei bleiben die Ziele jedoch unterschiedlich und nicht alle Partner haben die gleichen gemeinsamen Ziele. So teilt sich Org_A Ziele mit Org_B und Org_C, aber die Kooperation von Org_B und Org_C berücksichtigt die Ziele von Org_A nicht direkt.

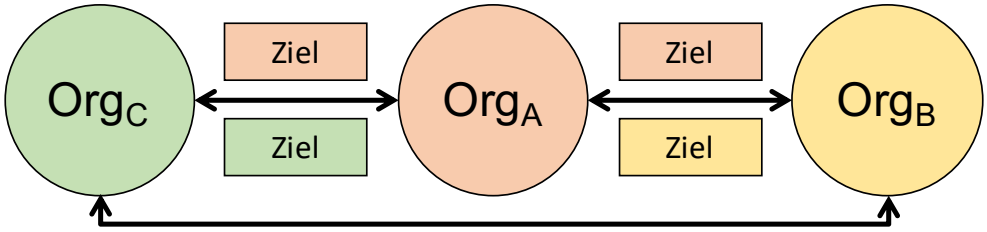


Abbildung 4.2: Struktur einer kooperativen Beziehung

Zielerreichung

Als Erweiterung der unterstützenden Beziehung kann von ähnlichen Rahmenbedingungen in Bezug auf direkte und indirekte Risiken ausgegangen werden. Weiterhin stehen mindestens die gleichen Möglichkeiten zur Zusammenarbeit zur Verfügung. Auch hier können klassische SCRs betrachtet werden, um die Auswirkung einer Beeinträchtigung der Partner auf die eigene Organisation abzuschätzen. Durch die intensivere Zusammenarbeit und die dadurch entstandenen Abhängigkeiten sind die Organisationen jedoch deutlich stärker von Risiken in der Partnerschaft betroffen. Die Definition der kooperativen Beziehung sagt bereits, dass die Partner diese eingehen, um ihre eigenen Ziele zu erreichen. Eine Beeinträchtigung des Partners führt somit dazu, dass die Unternehmensziele nicht erreicht werden und gleichzeitig können gemeinsame Projekt nicht einfach wie ein Lieferant gewechselt werden.

Kooperation im RM

Aufgrund dieser Abhängigkeiten sollten die Partner ein größeres Interesse daran haben, sich gegenseitig bei der Vermeidung von Risiken zu unterstützen. Durch die langfristige ausgerichtete Partnerschaft ist es außerdem leichter möglich, feste Strukturen für den Austausch von Risikoinformationen zu etablieren. Kooperationen sind damit eine gute Basis, um gemeinsame Managementfunktionen im ISM aufzubauen, wenn dabei das Teilen von Informationen im Mittelpunkt steht. Trotzdem arbeiten die Organisationen weitgehend unabhängig voneinander und sind auf ihre eigenen Ziele fokussiert, wodurch es unwahrscheinlich ist, dass diese Kompromisse zum Wohl der Partnerschaft oder der Partner eingehen. Risiken die keine Auswirkung auf die Zielerreichung eines Partners haben sind für diesen irrelevant. Daher ist es fraglich, ob die Organisationen in einer kooperativen Beziehung tatsächlich bereit wären, eine gemeinsame Strategie im RM zu verfolgen.

4.2.4 Kollaborative Beziehung

Eine kollaborative Beziehung bildet die höchste Stufe einer IOR bezogen auf die Intensität der Zusammenarbeit. Gray [176] beschreibt Kollaboration im organisationsübergreifenden Kontext als die Zusammenlegung der Ressourcen von zwei oder mehr Organisationen zur Lösung eines Problems, welches nicht von einer Organisation alleine gelöst werden kann. Obwohl die Problemlösung einer der maßgebenden Gründe für jede IOR ist, kommt bei dieser Erklärung noch einmal das Teilen der Ressourcen in Spiel. Diese Form der Zusammenarbeit ist bereits nahe an dem, wie eine Organisation intern strukturiert ist. Innerhalb einer einzelnen Organisation ist die Kollaboration der Normalfall, bei dem die einzelnen Geschäftseinheiten letztlich gemeinsam an der Erreichung der Geschäftsziele arbeiten.

Definition 4.8: Kollaborative Beziehung

Eine langfristige Partnerschaft zwischen zwei oder mehr Organisationen, um die **gemeinsamen strategischen Ziele** der Partner (Def. 3.2) zu erreichen.

Eigenschaften

Cousins [170] beschreibt in seinem IOR Modell, dass eine strategische Kollaboration nur unter bestimmten Rahmenbedingen entstehen kann. Dazu definiert er die Eigenschaften Abhängigkeit/Unabhängigkeit und Gewissheit/Ungewissheit als Maßstab, wann eine Beziehung reif genug ist. Die Verteilung der Abhängigkeiten in der Beziehung ist der erste

entscheidende Faktor für eine langfristige Zusammenarbeit, d.h. sind die Partner unabhängig, besteht eine einseitige Abhängigkeit oder eine gegenseitige Abhängigkeit. Nur wenn alle Partner gegenseitige Abhängigkeiten besitzen, die dazu führen, dass sie gemeinsam erfolgreicher sind, wird eine Kollaboration entstehen. Damit diese jedoch funktionieren kann, brauchen alle Partner die notwendige Gewissheit, dass die Beziehung eine langfristige Perspektive hat. Alle beteiligten Organisationen müssen aktiv in die Beziehung investieren und ihre gegenseitigen Aktivitäten aneinander ausrichten, um das Vertrauen der Partner in die Kollaboration sicherzustellen.

Freiwilligkeit

Eine weitere Eigenschaft, die besonders betont wird, ist das es sich bei Kollaborationen um einen freiwilligen Austausch handelt [24]. Das scheint nachvollziehbar, da sich langfristiges Vertrauen kaum etablieren lässt, wenn die Partner in die Beziehung gezwungen werden. Eine weitere denkbare Möglichkeit wäre jedoch das Mandat, bei dem davon ausgegangen wird, dass dieses nur der Auslöser ist, aber die Teilnehmer grundsätzlich zusammenarbeiten wollen [191]. Hier könnte davon ausgegangen werden, dass die gegenseitige Abhängigkeit durch das Mandat gegeben ist.

Modell der Kollaboration

Abbildung 4.3 zeigt die Struktur einer kollaborativen Beziehung. Wie auch bei der kooperativen Beziehung können dabei zwei oder mehr Organisationen beteiligt sein (n:n Beziehung). Wie dargestellt ist der Hauptunterschied nun, dass die Organisationen nicht mehr nur ihre eigenen Ziele haben, sondern alle Partner ein gemeinsames Ziel verfolgen. Org_A, Org_B und Org_C arbeiten also auf dasselbe Ziel hin und jeder weitere Partner teilt dieses Ziel der Gemeinschaft. Damit begründet sich auch die gegenseitige Abhängigkeit. Zum einen sind die Partner gegenseitig auf ihre Mitwirkung angewiesen, um das gemeinsame Ziel zu erreichen. Zum anderen bedeutete das, wenn eine Organisation ihr Ziel nicht erreicht, werden es die Partner auch nicht. Somit ist auch klar, wieso Vertrauen und Gewissheit in der kollaborativen Beziehung essenziell sind. Schließlich wird keine Organisationen ihren Erfolg von einer Partnerschaft abhängig machen, wenn die Risiken der Zielerreichung ungewiss sind.

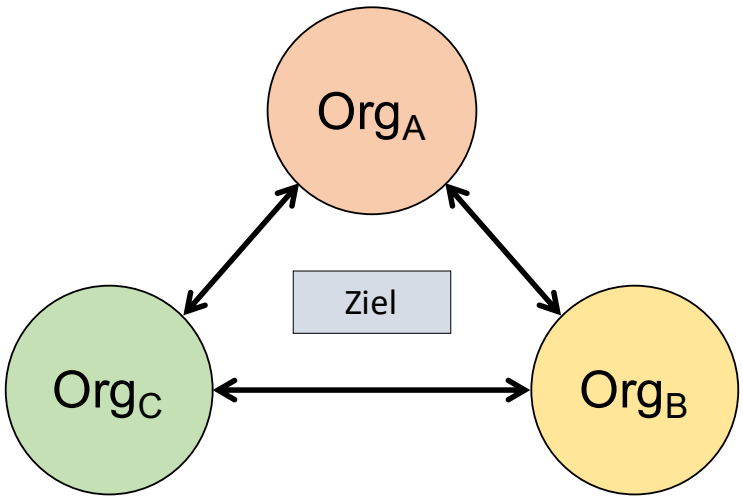


Abbildung 4.3: Struktur einer kollaborativen Beziehung

Kollaboration im RM

Wie auch bei der kooperativen Beziehung besteht eine gegenseitige Abhängigkeit zwischen den Partnern, weshalb das Interesse an gemeinsamen Risiken grundsätzlich vorhanden sein sollte. Jedoch können die Partner nur miteinander langfristig erfolgreich sein, da die Partner zusammen ein gemeinsames Ziel verfolgen. Somit ist die Gemeinschaft stärker von allgemeinen Disruptionen betroffen und Risiken eines Partners sind eine potenzielle Gefahr für alle anderen. Es ist davon auszugehen, dass die Partner bereits sind, eine gemeinsame Strategie zum RM zu etablieren.

Allianz

Ein Zusammenschluss von Organisationen in einer kollaborativen Beziehung kann auch als strategische Allianz bezeichnet werden. Dabei vermittelt der Begriff sehr gut die enge Bindung zwischen den Beteiligten, die so nicht in den anderen Beziehungsformen existiert. Weiterhin beschreibt die Allianz nicht die Beziehung an sich, sondern die organisatorische Gruppe, welche aus dem Zusammenschluss der Partner entsteht. Im restlichen Verlauf dieser Arbeit wird der Begriff der Allianz genutzt, um die Gemeinschaft einer kollaborativen Beziehung zu bezeichnen.

Definition 4.9: Allianz

Bezeichnet die Entität, die aus dem Zusammenschluss der Partner (Def. 3.2) in einer kollaborativen Beziehung (Def. 4.8) entsteht.

4.3 Partnerschaftsmodell des ISM

Im vorherigen Abschnitt konnten drei verschiedene Beziehungstypen (Abschnitt 4.1) definiert werden, welche sich zur Klassifikation von IORs eignen. In diesem Abschnitt sollen diesen die zuvor aus der Literatur identifizierten Kerneigenschaften von IORs (Abschnitt 4.2) zugeordnet werden. Das Ziel ist es, eindeutige Beziehungstypen zu spezifizieren, um anschließend zu analysieren, welcher Typ die besten Voraussetzungen für CISRM liefert. Dadurch kann im Vorfeld evaluiert werden, ob eine gegebene IOR für das CISRM grundsätzlich geeignet ist.

Eigenschften

Das Hauptkriterium zur Definition der drei Beziehungstypen waren deren Unternehmensziele, die sich für jede Beziehung und Partnerschaft unterscheiden können. Diese Ziele entsprechen dem zuvor identifizierten Interesse (Def. 4.5) einer Organisation. So steht bei einer unterstützenden Beziehung das Eigeninteresse im Vordergrund, bei einer kooperativen Beziehung das strategische Interesse und bei einer kollaborativen Beziehung das gemeinsame Interesse. Nachdem diese Dimension damit bereits feststeht, gilt es noch die weiteren Kerneigenschaften zu identifizieren, welche den jeweiligen Beziehungstyp definieren.

Modell

Die durch die Kerneigenschaften beschriebenen Beziehungstypen ergeben damit letztlich ein dreistufiges Partnerschaftsmodell, welches als Werkzeug bei der Klassifizierung von IORs dienen kann. In diesem Modell wird die Art der Zusammenarbeit auf jeder Stufe intensiver, wodurch die Entwicklung einer Beziehung dargestellt werden kann. Es stellt sich die Frage, welchen Reifegrad das CISRM erfordert. Bereits bei der Definition der Beziehungstypen wurden denkbare Anwendungsfälle für das ISRM diskutiert und ob ein gemeinsames Vorgehen mit den Partnern vorstellbar ist. Im Folgenden wird nun Anhand der Eigenschaften des Modells zusätzlich argumentiert, welche Form der Zusammenarbeit notwendig ist. Das Partnerschaftsmodell bildet damit den Anwendungsbereich des CISRM ab und stellt somit einen essenziellen Teil des kollaborativen Frameworks dar.

Anwendbarkeit

Das erstellte Partnerschaftsmodell ist dabei nicht spezifisch für das ISRM, sondern könnte auch für andere Anwendungsfälle genutzt werden. Es bietet sich für alle ISM Prozesse oder auch in einem komplette anderen Kontext zur Einstufung von Beziehungen an, wenn dabei die Art und Intensität der Zusammenarbeit im Vordergrund steht. In diesem Zusammenhang haben Schmidt und Mizani [165] das Partnerschaftsmodell auf alle 17 ISM Prozesse angewendet, die in der ISO/IEC 27022 [192] gelistet sind. Dabei hat sich gezeigt, dass dieses als allgemeines Werkzeug genutzt werden kann, um IORs und deren Eignung für die Implementierung von interorganisationalen Sicherheitsprozessen zu bewerten. In dieser Arbeit liegt der Fokus jedoch auch im Weiteren auf einer detaillierten Analyse für das CISRM. Trotzdem werden diese Ergebnisse am Ende des Abschnitts kurz eingeordnet, insbesondere um die Anwendbarkeit des Partnerschaftsmodells zu evaluieren.

4.3.1 Vergleich der Beziehungen

Nachdem nun die drei Kategorien von Beziehungen vorgestellt wurden, sollen diese klar voneinander abgegrenzt werden. Dies erfolgt auf Basis der im letzten Abschnitt etablierten Eigenschaften von IORs. Auf diese Art sollen klare Kriterien für IORs geschaffen werden, um damit den Anwendungsbereich für CISRM festzulegen.

Charakterisierung der Beziehungstypen

Ausgelassene Eigenschaften

Nicht alle Eigenschaften sind dabei für die Klassifikation der vorgestellten Beziehungstypen relevant. Grundsätzlich sind alle drei sowohl als vertikale als auch als horizontale Beziehung vorstellbar, wobei die Vor- und Nachteile vom konkreten Szenario abhängen. Dabei ist auch die Netzwerkform nicht eindeutig. Unterstützende Beziehungen sind klassisch vertikale Netzwerke, eine kooperative Beziehung könnte eine Weiterentwicklung einer vertikalen Netzwerkorganisation oder auch ein Chancen-Netzwerk sein und eine kollaborative Beziehung könnte ein interne oder marktübergreifende Netzwerkorganisation darstellen. Auch die Anzahl bzw. Struktur als Zweiergruppe, Portfolio oder Netzwerk spielt keine Rolle für die Beziehungstypen.

Ausgewählte Eigenschaften

Relevante Eigenschaften der IOR sind solche, die etwas über das Verhältnis der Partner zueinander aussagen. Dies beinhaltet das **Interesse** der Organisationen (Def. 4.5), die **Abhängigkeiten** voneinander (Def. 4.2), die *Nähe* zwischen den Partnern (Def. 4.4), die **Autorität** der Partner, d.h. die dominierende sozio-organisatorische Eigenschaft (Def. 4.3) in der Beziehung, und die Art des **Vertrauens** zwischen den Partnern (Def. 4.1). Somit werden die Partnerschaften anhand von fünf Kriterien mit jeweils 2-3 Stufen klassifiziert. Tabelle 4.1 listet diese Eigenschaften für alle drei Beziehungstypen, deren Zuordnung nachfolgend erklärt wird.

Tabelle 4.1: Kriterien zur Einteilung von IORs

	Beziehungstyp		
Eigenschaft	**Unterstützend**	**Kooperativ**	**Kollaborativ**
Interesse	Eigen	Strategisch	Gemeinsam
Abhängigkeit	Einseitig	Gegenseitig	Gegenseitig
Vertrauen	Vertraglich	Kompetenz	Guter Wille
Autorität	Machtbasiert	Vertrauensbasiert	Vertrauensbasiert
Nähe	Keine	Gering	Hoch

Interesse Das Interesse beschreibt die Zielsetzung der einzelnen Organisationen und ist damit eine der wichtigsten Eigenschaften um zu beurteilen, wie intensiv die Partnerschaft tatsächlich ist. Bei einer unterstützenden Beziehung steht für jeden Teilnehmer das Eigeninteresse im Mittelpunkt und jede Organisation will die eigenen Ziele erreichen. Dahingegen steht das strategische Interesse bei einer kooperativen Beziehung im Vordergrund, welches sich bereits mit dem der Partner überschneiden sollte, da beide ein Interesse an den gemeinsamen Aktivitäten haben. Bei der kollaborativen Beziehung steht letztlich das gemeinsame Interesse an erster Stelle. Dabei agieren die Partner so, dass sie teilweise ihr Eigeninteresse zurückstellen, um die gemeinsamen Ziele zu erreichen oder die Partner zu unterstützen.

Abhängigkeit Die Abhängigkeiten zwischen den Organisationen sind eine weitere wichtige Eigenschaft einer Beziehung. In der unterstützenden Beziehung herrscht eine einseitige Abhängigkeit, wodurch auch keine enge Bindung zwischen Kunde und Lieferant besteht. Sowohl bei einer kollaborativen als auch kooperativen Beziehung ist eine gegenseitige Abhängigkeit vorhanden, da der Erfolg aller Partner von den gemeinsamen Aktivitäten abhängen.

Nähe Nähe wurde als Maß für die Gemeinsamkeiten von zwei Organisationen etabliert. Für eine einfache unterstützende Beziehung ist keine besondere Nähe notwendig, da nur Leistungen ausgetauscht werden. Eine kooperative Beziehung benötigt zumindest eine geringe Nähe zwischen den Partnern, damit die Zusammenarbeit erfolgreich ist. Dabei ist insbesondere die technologische Nähe relevant, da eine ähnliche Wissensgrundlage die Voraussetzung für eine gemeinsame Unternehmung ist. Für eine kollaborative Beziehung ist die Nähe noch einmal deutlich wichtiger. Hier wird vor allem die organisatorische Nähe ein entscheidender Faktor, da Arbeitsweise und Unternehmenskultur grundsätzlich kompatibel sein müssen, um eine langfristige Partnerschaft zu ermöglichen. Geografische Nähe ist sowohl in einer kooperativen als auch kollaborativen Beziehung hilfreich, kann allerdings leicht durch (virtuelle) Treffen etabliert werden.

Autorität Jede IOR lässt sich grundsätzlich basierend auf dem Verhältnis von Macht und Vertrauen klassifizieren, wobei die vorherrschende Eigenschaft die Art und Weise definiert, wie die Partner zusammenarbeiten. Als machtbasierte Beziehung ist die Macht in der unterstützenden Beziehung einseitig verteilt, wobei sowohl Kunde als auch Lieferant die mächtige Partei sein kann. Die Machtposition basiert dabei üblicherweise auf der Größe der Organisationen oder der Stellung im Markt. Wird die Zusammenarbeit zwischen zwei Organisationen jedoch intensiver, so ändert sich dieses Verhältnis und Vertrauen wird zur dominierenden Eigenschaft. Kooperative und kollaborative Beziehungen werden nicht dadurch zusammengehalten, dass eine Partei besonders viel Macht hat, sondern durch gegenseitiges Vertrauen aufgrund einer etablierten Zusammenarbeit und gemeinsamen Zielen.

Vertrauen Grundsätzlich ist das Vertrauen immer eine Kerneigenschaft in IORs, selbst wenn Macht die dominierende Eigenschaft ist. Dabei liegt der Unterschied maßgeblich darin, welche Art von Vertrauen zentral für die jeweilige Beziehung ist. Für eine unterstützende Beziehung ist das vertragliche Vertrauen grundsätzlich am wichtigsten. Nur wenn beide Partner davon ausgehen können, dass der andere seine Verpflichtungen auch einhält, kommt eine Beauftragung zustande. Nachdem es in der kooperativen Beziehung bereits um die Durchführung gemeinsamer Aktivitäten geht, steht hier das Vertrauen in die Kompetenz im Fokus. Alle Partner gehen davon aus, dass die Teilnehmer die notwendigen Kompetenzen zur Zusammenarbeit mitbringen, die effizienter sein soll als eine Einzelunternehmung. Auch bei der kollaborativen Beziehung ist vertragliches und Vertrauen in die Kompetenz relevant, jedoch ist das Vertrauen in den guten Willen der Partner das Entscheidende. Das Verhalten der einzelnen Organisationen über einen langen Zeitraum spiegelt deren Hingabe zur gemeinsamen Unternehmung wider und beeinflusst die langfristige Leistungsfähigkeit der Zusammenarbeit.

4.3.2 Darstellung des Partnerschaftsmodells

Die identifizierten Kerneigenschaften einer Beziehung und deren Zuordnung zu den Beziehungstypen ist ein Beispiel für eine Klassifikation von Beziehungen auf Basis der Intensität ihrer Zusammenarbeit. Diese soll nun als allgemeines Werkzeug bereitgestellt werden, um eine gegebene IOR einem Typen zuordnen zu können. Dieses Werkzeug stellt das grafische Partnerschaftsmodell dar.

Daten

Die Datensätze aus Tabelle 4.1 wurden den einzelnen Beziehungstypen zugeordnet, um eine grafische Darstellung des Partnerschaftsmodells zu visualisieren, welche die unterstützende Beziehung, die kooperative Beziehung und die kooperative Beziehung hervorhebt. Abbildung 4.4 zeigt nun ein Spinnendiagramm mit den drei Beziehungstypen, anhand dessen die Organisationen ihre aktuelle IOR bewerten können. Dadurch kann diese überprüfen, ob sie sich in der richtigen Position befindet, um mit ihren Partnern ein CISRM zu implementieren.

Visualisierung

Das Partnerschaftsmodell liefert eine grafische Repräsentation der Kerneigenschaften einer Beziehung. Dabei wurden die vorgestellten Beziehungstypen, die unterstützende Beziehung, die kooperative Beziehung und die kollaborative Beziehung, bereits darauf abgebildet. Die farbig dargestellten Beziehungstypen werden durch die fünf ausgewählten Eigenschaften eindeutig charakterisiert. Dabei wurde die Darstellungsform so gewählt, dass die Intensität der Beziehung nach außen gehend zunimmt. Auf diese Weise kann auch die Entwicklung einer Beziehung nachvollzogen werden. Somit zeigt das Diagramm, wie die Partnerschaft von einer unterstützenden Beziehung zu einer kooperativen Beziehung heranreift. Dabei ist jedoch zu berücksichtigen, dass sich die Eigenschaften zum Teil gegenseitig beeinflussen.

Eignung für das CISRM

Diese fünf Eigenschaften definieren die Kriterien für drei generische Beziehungen. Dabei sind nicht alle gleichermaßen gut geeignet, um gemeinsame Prozesse zu etablieren, insbesondere mit Blick auf das ISM. Dabei gilt für jede Managementfunktion zu bewerten, welche Eigenschaften für einen organisationsübergreifenden Prozess tatsächlich notwendig sind. Speziell für das ISRM zeigt sich jedoch ganz klar, dass nur die kollaborative Beziehung

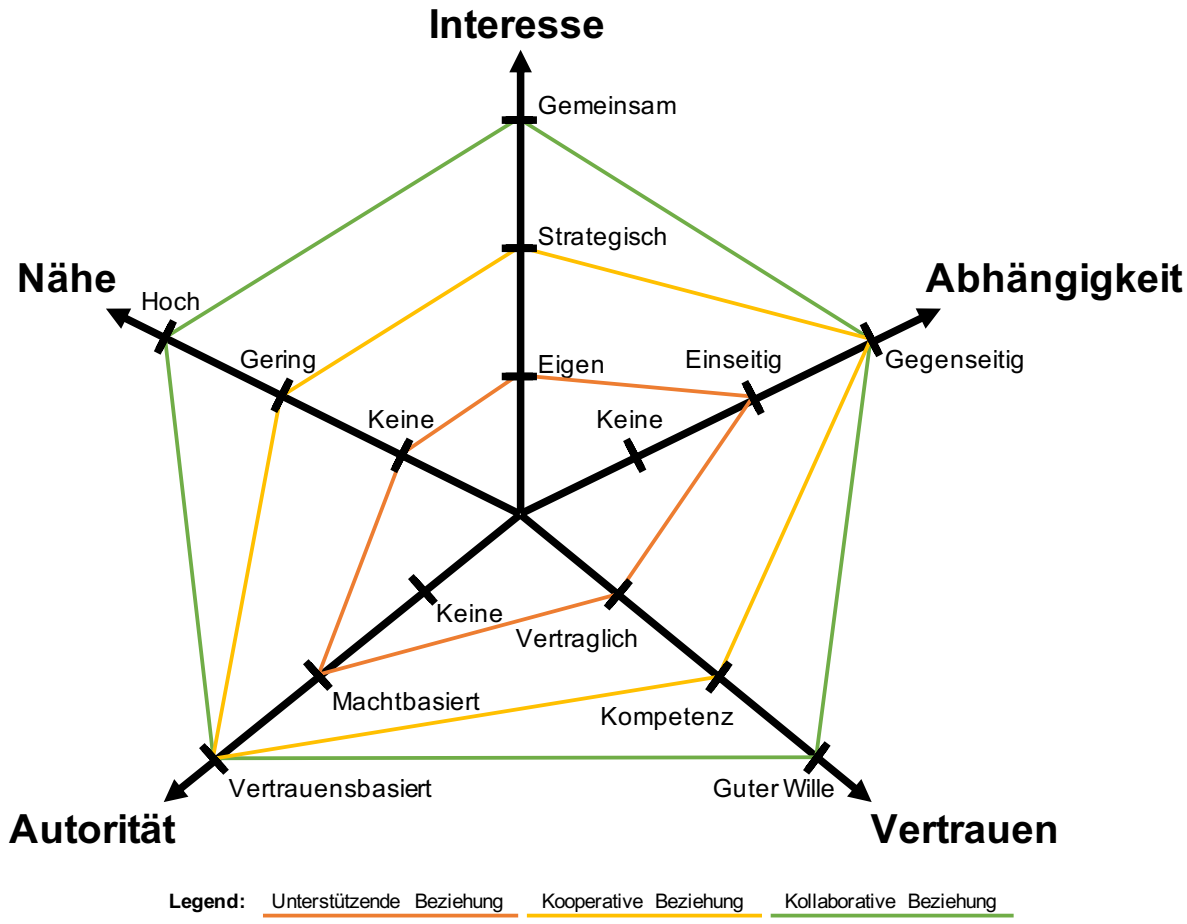


Abbildung 4.4: Grafisches Partnerschaftsmodell basierend auf den Kerneigenschaften verschiedener Beziehungstypen

wirklich geeignet ist, ein CISRM zu implementieren. Die Grundvoraussetzung stellt definitiv ein sehr hohes Vertrauen dar, das die Partner immer das Wohlergehen der Allianz im Sinn haben. Das trifft allerdings auch auf die kooperative Beziehung zu, wie die gegenseitige Abhängigkeit, welche erforderlich ist, damit die Partner überhaupt von den Risiken in der Allianz betroffen sind. Gleiches gilt für eine angemessene Nähe zwischen den Partnern, wobei eine geringe Nähe eventuell ausreichend sein kann. Zusätzlich muss allerdings auch das gemeinsame Interesse im Vordergrund stehen, damit die Partner ein echtes Anliegen an der Sicherheit der anderen Teilnehmer und der gemeinsamen Risikobehandlung haben. Letztlich ist das Vertrauen in den guten Willen der Partner die notwendige Basis, damit die Abstimmung bei der Risikofreigabe funktionieren kann. Nur wenn die Partner bereits sind, in langfristig die Allianz zu investieren, ohne einen direkten Vorteil zu erhalten, werden sich die Partner auf ein Vorgehen einigen können.

Kollaborative Beziehung

Aufgrund dieser Kriterien zeigt sich, dass für gemeinsame ISRM eine sehr enge Partnerschaft notwendig ist. Dieses Ergebnis überrascht nicht, da eine höhere Integration auf organisatorischer und strategischer Ebene generell die Zusammenführung von Unternehmensprozessen erleichtert. Bereits im SCRM wurde argumentiert, dass die Dauer der Partnerschaft, das Vertrauen zwischen den Partnern und das Verständnis der Partnerorganisation essenzielle Eigenschaften sind, um organisationsübergreifendes RM zu etablieren. Somit bildet nun die kollaborative Beziehung den Anwendungsbereich für das CISRM.

Werkzeug für IORs

Das erstellte Partnerschaftsmodell (Abbildung 4.4) kann Organisationen, die eine Zusammenarbeit im ISM erwägen, als Werkzeug zur Festlegung des Anwendungsbereichs dienen. Verschiedene Managementfunktionen haben unterschiedliche Anforderungen an eine Beziehung, wenn sie gemeinsam ausgeführt werden sollen. Vor dem Etablieren eines organisationsübergreifenden Prozesses, sollten die Partner prüfen, ob ihre IOR die nötigen Anforderungen erfüllt. Wie oben gezeigt wurde, sollten für eine Zusammenarbeit im ISRM die Eigenschaften einer kollaborativen Beziehung erfüllt sein, damit dieses wirksam sein kann. Daher macht das CISRM nur Sinn, wenn eine IOR bereits den höchsten Reifegrad erreicht hat.

4.3.3 Bewertung des Modells

Das vorgestellte Partnerschaftsmodell (Abbildung 4.4) wurde initial zur Festlegung des Anwendungsbereichs des CISRM konzipiert. Es hat sich jedoch gezeigt, dass das Modell auch im Kontext anderer ISM Prozesse hilfreich sein kann. Wie auch beim ISRM kann es dazu genutzt werden, die angemessene Beziehung für einen bestimmten Prozess zu finden.

ISM

Schmidt und Mizani [165] wenden das Partnerschaftsmodell daher auf weitere ISM Prozesse an. Dabei werden die 17 ISM Prozesse der ISO/IEC 27022 [192] mit Hilfe des Modells ausgewertet. Zusätzlich erfolgt eine Analyse, welche Art der Zusammenarbeit für welchen Prozess sinnvoll erscheint. Dazu werden drei generische Forms of Cooperation (FoC) unterschieden: „Daten austauschen“, „Ressourcen bündeln“ und „Gemeinsam ausführen“. Durch die Zuordnung von Prozessen zu diesen FoC und die Festlegung von minimalen Beziehungstypen für jeden davon, konnte feststellen werden, ob es sinnvoll ist, einen bestimmten Prozess in einer IOR zu implementieren.

Prozesse

Tabelle 4.2 zeigt eine Liste von ISM Prozessen zugeordnet zu den FoC. Dabei sind nur die Prozesse gelistet, bei denen tatsächlich ein Mehrwert durch die interorganisationale Ausführung festgestellt werden konnte. Die verbleibenden Prozesse wurden den drei Beziehungstypen zugeordnet und jeweils bewertet, ob diese gut „+“ oder sehr gut „++“ für die gemeinsamen FoC geeignet sind. Einige der Prozesse sind abhängig voneinander oder von anderen Faktoren, weshalb es schwierig ist deren interorganisationalen Mehrwert isoliert zu bewerten. Zum Beispiel ist das gemeinsame Ausführen der Ressourcenplanung im *Resource management process* nur dann sinnvoll, wenn die Organisationen auch planen diese Ressourcen gemeinsam zu nutzen. Wenn die Partner allerdings in anderen Prozessen ihre Ressourcen teilen bzw. bündeln, dann kann die gemeinsame Ausführung sinnvoll sein. Die Bewertung der betroffenen Prozesse ist daher in Klammern „(++)“ dargestellt.

Tabelle 4.2: Evaluation von ISM-Prozessen mit Hinblick auf verschiedene Arten der Zusammenarbeit in IORs [In Anlehnung an 165]

Ausführbare Prozesse pro Kooperationsform	UN	KP	KL
Daten austauschen			
IS risk assessment process		+	+
Security implementation management process		+	+
Ressourcen bündeln			
IS risk assessment process		+	+
Security implementation management process		+	+
Process to control outsourced services		+	+
Process to assure necessary awareness and competence		++	++
IS incident management process		++	++
IS change management process		+	+
Internal audit process		+	+
IS improvement process		+	+
IS customer relationship management process		(++)	(++)
Gemeinsam ausführen			
IS risk assessment process			++
Security implementation management process			++
Process to control outsourced services			++
Process to assure necessary awareness and competence			+
IS incident management process			++
Internal audit process			+
Performance evaluation process			++
Resource management process			(+)
Communication process			(++)
IS customer relationship management process			(++)

Beziehungen: Unterstützend (UN), Kooperativ (KP), Kollaborativ (KL)
Prozessbewertung: gut geeignet +, sehr gut geeignet ++, abhängig (+/++)

Untersützende Beziehung
Es hat sich gezeigt, dass die unterstützende Beziehung generell nicht geeignet ist, um ISM Prozesse bei einer der drei Aktivitäten zu unterstützen. Der Beziehung fehlen die relevanten Eigenschaften, damit die Partner tatsächlich an einer gemeinsamen Ausführung der Prozesse interessiert zu sind. Das reine Austauschen von Daten ist maximal in einer Sharing Community denkbar, welche sich allerdings nicht als echte Partnerschaft qualifiziert.

Kooperative Beziehung
Die kooperative Beziehung liefert zumindest die Grundlage für einen Datenaustausch oder gemeinsame Ressourcen für einige der Prozesse. Insbesondere das Bündeln von Ressourcen kann in dieser Beziehungsform einen positiven Einfluss auf die Prozesse haben. Die Partner profitieren von ähnlichen Zielen, der Nähe zueinander und dem Vertrauen in die Kompetenz der anderen Organisationen.

Kollaborative Beziehung
Letztlich ist jedoch nur die kollaborative Beziehung geeignet, alle Formen der Zusammenarbeit und die meisten der Prozesse zu unterstützen. Sie unterstützt alle Prozesse in den FoC Daten austauschen und Ressourcen bündeln, welche auch in einer kooperativen Beziehung sinnvoll erscheinen. Insbesondere die gemeinsame Ausführung von Prozessen liefert jedoch nur in dieser Beziehungsform einen Mehrwert, da Vertrauen in den guten Willen der Partner und die gemeinsamen Ziele hier essenziell sind.

Ergebnis
Es zeigt sich, dass das ISM grundsätzlich von einer gemeinsamen Ausführung innerhalb einer Allianz profitieren kann. Die Prozesse im Bereich Risiko Management, Incident Management und Awareness Management eignen sich dabei am besten für ein interorganisationales Vorgehen. Im Gegensatz dazu liefert die Zusammenarbeit bei Governance-Prozesse kaum einen Mehrwert, wenn diese gemeinsam ausgeführt werden. Obwohl die betrachtete ISO/IEC 27022 zwar eine andere Aufteilung der Prozesse vornimmt und insbesondere das ISRM in mehrere Teilprozesse aufspaltet, bestätigt sich damit noch einmal, dass die vorgeschlagene Zusammenarbeit im Kontext eines CISRM sinnvoll erscheint.

Evaluation
Die Anwendung auf verschiedene ISM Prozesse kann als eine Evaluation des Partnerschaftsmodells gesehen werden. Offensichtlich ist es ein geeignetes Werkzeug, um Beziehungen und Prozesse im IS-Bereich einzustufen. Es kann dazu genutzt werden, um den Reifegrad einer Beziehung einzuschätzen. Es erlaubt es interessierten Organisationen zu bewerten, ob ihre IOR für ein gemeinsames Vorgehen geeignet ist. In Kontext dieser Arbeit wird das Partnerschaftsmodell dem CISRM Framework als erste Komponente hinzugefügt, aber es steht auch für andere Prozesse zur Verfügung.

4.4 CISRM in kollaborativen Beziehungen

In diesem Kapitel wurden die theoretischen Grundlagen für Beziehungen zwischen Organisationen genauer untersucht. Das Ziel war es, basierend auf den in Kapitel 2 vorgestellten Grundlagen des RM/ISRM dessen Anwendbarkeit in Allianzen zu untersuchen. Die Idee dabei ist es, dass diese strategischen Partnerschaften von Organisationen geeignet sein können, um ein organisationsübergreifendes ISRM zu etablieren. Dieses CISRM soll ein gemeinsames und abgestimmtes Vorgehen ermöglichen, welches nicht nur die Sicherheit der Allianz als Ganzes verbessert, sondern den Partnern auch eine effektivere Risikobehandlung ermöglichen, als es jede einzelne Organisation könnte. Dabei wurden im Detail die folgenden Fragestellungen untersucht und diskutiert:

- Warum gehen unabhängige Organisationen eine Beziehung ein und wie sind diese IORs strukturiert (Abschnitt 4.1)?
- Wie können verschiedene Beziehungstypen anhand ihrer Eigenschaften zur Zusammenarbeit klassifiziert werden? (Abschnitt 4.2)?
- Welche Eigenschaften muss eine IORs aufweisen, damit sie sich für das CISRM eignet (Abschnitt 4.3)?

IORs

Zu Beginn des Kapitels wurde als Erstes der aktuelle Stand der Wissenschaft im Bereich der interorganisationalen Beziehungen vorgestellt. Dabei wurde nicht nur diskutiert, was eine IOR eigentlich ist, sondern auch, welche Gründe es für Organisationen gibt zu kooperieren. Sofern es sich um eine freiwillige Zusammenarbeit und kein Mandat handelt, sind diese meist auf eine höhere Innovationskraft bei Projekten und die geteilten Vorteile einer Steigerung der Effektivität zurückzuführen. Weiterhin wurden relevante Eigenschaften einer Beziehung wie Nähe, Ausrichtung, Abhängigkeit, Vertrauen und Macht erklärt. Abhängig vom Verhältnis dieser Eigenschaften in der Beziehung ergeben sich andere Netzwerke und Koordinationsstrukturen. Die entstehenden IORs sind dabei für verschiedenen Aufgaben unterschiedlich gut geeignet, weshalb der passende Beziehungstyp für das CISRM gesucht wurde.

Beziehungstypen

Basierend auf diesen Erkenntnissen wurden generische Beziehungstypen definiert, welche die Intensität der Zusammenarbeit beschreiben. In der Folge wurden drei Klassen von IORs eingeführt: die *unterstützende Beziehung* (Def. 4.6), die *kooperative Beziehung* (Def. 4.7) und die *kollaborative Beziehung* (Def. 4.8). Diese beschreiben jeweils eine bestimmte Form einer IOR, bei der sich insbesondere Nähe und Abhängigkeit von den anderen unterscheidet. Dabei intensiviert sich die Art der Zusammenarbeit und Wertschöpfung, so enger die Beziehung zwischen den Organisationen wird.

Partnerschafts-modell

Anschließend wurde ein Partnerschaftsmodell (Abbildung 4.4) erstellt, welches die drei Beziehungstypen abbilden kann. Die unterstützende Beziehung ist dabei die einfachste Form, bei der keine besondere Bindung zwischen den Partnern besteht, welche über die Lieferung eines Produktes hinausgeht. Neben dem Vertrauensverhältnis und einer strategisch ausgerichteten Partnerschaft der kooperativen Beziehung, definiert sich eine kollaborative Beziehung an den gemeinsamen Zielen und dem Bedarf, gemeinschaftlich Probleme zu lösen. Diese Form der Beziehung bietet damit die beste Umgebung, um auch gemeinsame Managementprozesse zu etablieren. Dabei wurde ebenfalls gezeigt, dass verschiedene ISM Prozesse unterschiedliche Anforderungen an die Beziehung stellen. Letztlich scheint die *kollaborative Beziehung* als einzige geeignet, um ein interorganisationales CISRM zu etablieren.

Aufbau des CISRM

Nachdem auf diese Weise der Anwendungsbereich für das CISRM definiert wurde, gilt es nun herauszufinden, wie dieses implementiert werden kann. Ziel dieser Arbeit ist es, das Design eines kollaborativen Prozesses zu skizzieren und die für den Aufbau in IORs notwendigen Hilfsmittel bereitzustellen. Basierend auf den verschiedenen Szenarien und vorhandenen Erkenntnissen in der Literatur sollen daher die Voraussetzungen für eine organisationsübergreifende Zusammenarbeit identifiziert werden. Am Ende muss ein solches Vorgehen nicht nur funktionsfähig sein, sondern auch einen entsprechenden Mehrwert im Gegensatz zum klassischen ISRM/ERM liefern.

Kapitel 5

Ableitung einer einheitlichen ISRM Terminologie

Inhaltsangabe

Aufbau

Allianzen müssen die richtigen Rahmenbedingungen aufweisen, damit ein CISRM erfolgreich sein kann. Zuvor wurde gezeigt, dass nicht jede IORs dafür geeignet ist, da bereits eine intensive Zusammenarbeit mit Eigenschaften wie einem hohen Maß an Vertrauen und gemeinsamen Zielen etabliert sein muss. In diesem Kapitel soll die zweite Komponente, eine Terminologie des ISRM, des kollaborativen Frameworks entwickelt werden (Abbildung 3.1 - Modul 2: Terminologie des ISRM). Dazu werden die in Abschnitt 2.3 vorgestellten ISRM Frameworks genauer untersucht. Basierend auf diesen wird eine allgemeingültige Terminologie definiert, welche Kernbegriffe und Schlüsselkonzepte des ISRM beschreiben.

Relevanz

Obwohl ein Terminologie-Mapping selbst schon hilfreich für Organisationen sein kann, die versuchen unterschiedliche ISRM-Prozesse zu vergleichen, liefert sie besonderen Wert für verteilte Organisationsstrukturen. Da es sich bei den Teilnehmern einer Allianz um unabhängige Organisationen handelt, kann nicht davon ausgegangen werden, dass diese die gleichen Frameworks oder Methoden verwenden, um ISRM zu implementieren. Da die Partner grundsätzlich gleichberechtigt sind, kann die Nutzung einer bestimmten Methode nicht erzwungen werden. Somit sprechen die Partner im ISRM eine unterschiedliche Sprache, was intern für die Organisationen kein Problem ist, aber die Kommunikation innerhalb der Allianz erschwert. Eine einheitliche Sprache ist somit die Grundlage zur fachbezogenen Verständigung und damit die Kollaboration im ISRM innerhalb der Allianz. Somit erscheint die Definition einer allgemeingültigen Terminologie notwendig (CSF 2). Sie bildet die Basis für das weitere Vorgehen und die Ableitung der anderen beiden Komponenten des kollaborativen Frameworks.

Vorgehen

Im Folgenden werden Begriffe und Konzepte untersucht, die häufig im ISRM verwendet werden, um dessen aktuelle Terminologie zu umreißen. Um den Unterschied zwischen einer Terminologie, einem Begriff und einem Konzept zu verdeutlichen, werden diese kurz erörtert (Abschnitt 5.1) und bestehende Publikationen zu diesem Thema untersucht (Abschnitt 5.2). Kurz gesagt, Kernbegriffe sind Begriffe, die in mehreren Rahmenwerken verwendet werden, was ein Indikator dafür ist, dass sie stabil und weithin akzeptiert sind. Schlüsselkonzepte sind Konzepte, die in allen Rahmenwerken verwendet werden und auf die mit oder ohne Verwendung desselben Begriffs Bezug genommen werden kann. Beide sind für eine allgemeine ISRM-Terminologie wichtig, daher werden die Begriffe aufgelistet, bewertet und die Schlüsselkonzepte hervorgehoben (5.3). Die Identifikation dieser Schlüsselkonzepte erfolgt durch eine semantische Analyse der Begriffsdefinitionen und anschließende Zuordnung der Begriffe. Anschließend werden die Beziehungen zwischen den so extrahierten Konzepten analysiert (Abschnitt 5.4). Die erkannten Begriffsbeziehungen werden abschließend modelliert und in einem Konzeptdiagramm dargestellt. Das erstellte Konzeptdiagramm bietet einen schnellen und einfachen Überblick über die gängige ISRM-Terminologie, um Kernbegriffe, Schlüsselkonzepte und Konzeptbeziehungen zu verstehen.

Veröffentlichung

Die hier vorgestellte Methodik zur Ableitung der Kernbegriffe und Schlüsselkonzepte zur Definition einer einheitlichen Terminologie wurde ursprünglich im Kontext dieser Arbeit erstellt, um das kollaborative Framework zu entwickeln. Die Inhalte und Ergebnisse aus diesem Kapitel wurden bereits im Forschungsartikel „Information security risk management terminology and key concepts“ [193] beschrieben und veröffentlicht.

5.1 Einführung in Terminologien, Begriffe, Konzepte

Heterogenes Vokabular

Wie in vielen Managementdisziplinen stammen die im ISRM verwendeten Begriffe meist direkt aus der praktischen Anwendung und nicht aus der Wissenschaft. Durch die Übernahme in internationale Rahmenwerke haben sich viele Begriffe durchgesetzt und sind de facto standardisiert. Shameli-Sendi et al. [73] zeigen in ihrer umfassenden Metastudie zur Risikoeinschätzung, dass diese Rahmenwerke für Organisationen weltweit unverzichtbar sind und berücksichtigen daher akademische Literatur und industrielle Rahmenwerke gleichermaßen. Wie bereits dargestellt gibt es jedoch eine Vielzahl verschiedener ISRM-Rahmenwerke, welche zum Teil einen unterschiedlichen Schwerpunkt haben, sodass die verwendeten Begriffe nicht immer übereinstimmen. Einige Rahmenwerke definieren ihre Terminologie sehr detailliert und verwenden eine große Anzahl von Begriffen zur Darstellung des ISRM-Prozesses, andere wiederum nur einige Wenige. Es gibt also keine allgemeingültige Terminologie, die verwendeten Begriffe sind nicht immer eindeutig und selbst die Konzepte können variieren. Sowohl in der Praxis als auch in akademischen Veröffentlichungen kann das verwendete Vokabular von vielen Faktoren wie der Branche, dem technischen Wissen oder dem Hintergrund des Autors abhängen. All dies erschwert die organisationsübergreifende Kommunikation und die Framework-unabhängige Diskussion über ISRM und behindert letztlich die Zusammenarbeit und Weiterentwicklung des Bereichs.

Inkonsistente Begriffe

Darüber hinaus werden die Beziehungen zwischen den Konzepten in der Literatur selten oder nur unvollständig dargestellt. Beispielsweise wird im ISRM oft angenommen, dass ein Risiko aus einer Schwachstelle in Kombination mit einer Bedrohung resultiert, aber diese Beziehung ist oft nicht explizit definiert und wird von Experten lediglich abgeleitet. Die korrekte Verwendung von ISRM-Begriffen ist sowohl im wissenschaftlichen Bereich wünschenswert als auch in der Praxis notwendig, um Risikokonzepte verständlich ausdrücken zu können. Eine einheitliche Terminologie bildet die Grundlage für die Kommunikation und Zusammenarbeit über Organisationsgrenzen hinweg, bis hin zur rechtlichen Relevanz, wenn Aspekte des IS oder RM rechtsverbindlich werden. Daher ist es besonders wichtig, dass nicht nur einheitliche Begriffe verwendet, sondern dass deren Konzepte auch gleich verstanden werden. [21, 69, 194]

Abgrenzung

In diesem Kapitel wird eine Terminologieüberprüfung auf Basis relevanter Literatur durchgeführt. Dabei soll der Fokus auf der Analyse des Zustands der tatsächlich definierten Begriffe liegen, wie sie in den Quellen vorgefunden werden. Im Gegensatz dazu wäre es ein möglicher Ansatz, auf Basis von Erfahrungen aus der Praxis oder dedizierten Expertenwissen eine Terminologie zu erstellen.

Grundlagen

Dazu ist es notwendig, zuerst einige Grundlagen zu schaffen, bevor die ISRM-Rahmenwerke im Detail diskutiert werden. Um die ISRM-Terminologie untersuchen zu können, muss zunächst einmal geklärt werden, was eine Terminologie, Begriffe und Konzepte eigentlich sind. Dieser Abschnitt soll lediglich einen kurzen Überblick über die Unterschiede und Zusammenhänge zwischen den Begriffen geben, die für das Verständnis dieses Kapitels notwendig sind. Dabei werden die Definitionen festgelegt, welche im Rahmen dieser Arbeit verwendet werden.

5.1.1 Theoretische Grundlagen

Die verwendeten Definitionen stammen aus anderen akademischen Bereichen, insbesondere den Sprach- und Terminologiewissenschaften, welche sich im Detail mit den für Terminologien relevanten Bestandteilen beschäftigen. Tatsächlich wäre es notwendig, verwandte Begriffe wie lexikalische Einheiten, Zeichen, Wörter, Sprache, Wissen und Benennung sowie die linguistischen und etymologischen Unterschiede zwischen ihnen zu verstehen, um Terminologie vollständig korrekt zu definieren. Das ist jedoch für das weitere Verständnis dieser Arbeit nicht erforderlich, daher werden im Folgenden nur die verkürzten Grundlagen vorgestellt. Von dieser theoretischen und praktischen Basis werden die Definitionen abgeleitet, welche den Rest des Kapitels verwendet werden.

Systeme von Begriffen

Eine mögliche Definition lautet wie folgt: „Terminologists are interested in signs, i.e. words and units larger than the word, only to the extent to which they function as names, denoting objects, and as indicators of concepts.“ [195, S. 29]. Vereinfacht gesagt, definiert eine Terminologie eine Gruppe von unterscheidbaren Wörtern, die als Begriffe bezeichnet werden. Im Gegensatz zu Systemen von Namen zur Kennzeichnung von Objekten die wir aus täglichen Leben kennen, sogenannten Nomenklaturen, sind Terminologien Systeme von Begriffen. Was einen Begriff einzigartig und damit unterscheidbar macht ist seine Definition, welche dessen inhaltliche Bedeutung erklärt. Nach einigen traditionellen Auslegungen lässt sich ein Konzept im Wesentlichen als das notwendige Wissen über die Verwendung eines bestimmten Wortes ableiten. Dabei ist insbesondere zu berücksichtigen, dass ein Konzept auch ohne einen zugeordneten Begriff existieren kann. [195, 196]

Definition 5.1: Terminologien

Terminologien sind Systeme von definierten Begriffen, welche die Struktur und Verwendung von Wissen in einem bestimmten Feld vorgeben.

Denken und Sprache

Wie bereits erwähnt, ist all das nur eine starke Vereinfachung der genannten Theorie der Sprach- und Terminologiewissenschaften. Über das Verhältnis von Konzepten und Begriffen sagt Rey [195, S. 24]: „[...] the fundamental opposition between concepts and terms too often appears as a dichotomy between thought and language. In this field, the best-known theories from a rather idealistic and undialectic intellectual construct which immediately postulates a conceptual structure which must be matched item by item a suitable terminological structure“. Es geht also im Grundsatz der Unterscheidung sehr stark um den Zusammenhang von Denken und Sprache. Dabei ist unklar, wie genau diese Elemente zusammengeführt oder auch unabhängig voneinander verwendet werden können. Es ist vorstellbar, dass ein Konzept als Gedankenkonstrukt existiert, aber nicht benannt ist. Dahingegen ist ein Begriff ohne Konzept nicht denkbar, da er dann keine Bedeutung hätte. Eine solch detaillierte Betrachtung der theoretischen Interpretation ist jedoch für das weitere Verständnis dieser Arbeit nicht erforderlich, da sich im Folgenden auf die praktische Anwendung fokussiert wird.

5.1.2 Praktische Anwendung

Definitionen

Um die theoretischen Grundlagen der Terminologiewissenschaft leichter nutzbar zu machen, haben sich nationale und internationale Organisationen um die Schaffung eines vereinfachten Vokabulars bemüht. Die internationale Norm zur Terminologiearbeit und Terminologiewissenschaft [197] definiert die wichtigsten Begriffe und ihre Zusammenhänge, die in dieser Publikation verwendet werden.

Terminologie

Laut der Norm ist eine *Terminologie* ein „set of designations (3.4.1 [Begriffsbezeichner]) and concepts (3.2.7) belonging to one domain (3.1.4) or subject (3.1.5)“. Die beiden letztgenannten definieren den Geltungsbereich, wobei eine *Domäne* ein „field of special knowledge“ und ein *Thema* eine „area of interest or expertise“ ist, welches im Kontext dieser Arbeit das ISRM ist.

Definition 5.2: Domäne

Eine **Domäne** beschreibt ein klar abgegrenztes Fachgebiet bzw. einen definierten Teil davon.

Konzept

Ein *Konzept* ist eine „unit of knowledge created by a unique combination of characteristics (3.2.1)“. Diese *Charakteristiken* sind eine „abstraction of a property (3.1.3)“, welche ein „feature of an object (3.1.1)“ sind, d.h. „anything perceivable or conceivable“. Somit sind Konzepte klar umrissene Wissenssammlungen, welche aus einer Menge von Eigenschaften bestehen.

Definition 5.3: Konzept

Ein **Konzept** beschreibt eine Sammlung von Wissen und zusammengehörenden Eigenschaften, welches Verständnis innerhalb eines bestimmten Bereichs liefert.

Konzept-beziehung

Eine wichtige Eigenschaft eines *Konzeptes* ist, dass es mit anderen eine *Konzeptbeziehung* bildet, d.h. es gibt eine „relation between concepts (3.2.7)“. Konzepte sind somit keine unabhängigen Entitäten, sondern formen ein Netz von zusammengehörigem Wissen. Das ist nachvollziehbar, da ein Konzept Verständnis über die Anwendbarkeit dieses Wissens innerhalb einer Domain liefern soll. Ohne Beziehungen zu weiteren Konzepten wäre ein Konzept isoliert und würde keinen praktischen Mehrwert liefern.

Definition 5.4: Konzeptbeziehung

Ein oder mehrere *Konzepte* (Def. 5.3) können in Zusammenhang zueinander stehen bzw. miteinander verbunden sein, was als **Konzeptbeziehung** bezeichnet wird.

Begriff

Im Gegensatz dazu ist eine *Bezeichnung* lediglich eine „representation of a concept (3.2.7) by a sign which denotes it in a domain (3.1.4) or subject (3.1.5)“. Das bedeutet, dass die *Bezeichnung* als Etikett eines *Konzeptes* innerhalb einer bestimmten *Domäne* angesehen werden kann. Bei der Verwendung einer „designation (3.4.1) that represents a general concept (3.2.9) by linguistic means“, wird es als *Begriff* bezeichnet.

Definition 5.5: Begriff

Ein **Begriff** ist die sprachliche Repräsentation eines Konzeptes, d.h. er benennt und verweist immer auf genau ein *Konzept* (Def. 5.3).

Allgemeines Konzept

Der Vollständigkeit halber und um den Zirkelschluss der zitierten Definitionen zu schließen, ist ein *allgemeines Konzept* ein „concept (3.2.7) that corresponds to a potentially unlimited number of objects (3.1.1) which form a group by reason of shared properties (3.1.3)“.

Definition 5.6: Terminologie

Eine **Terminologie** besteht aus abgegrenzten *Konzepten* (Def. 5.3) und diesen zugewiesenen *Begriffen* (Def. 5.5), welche über definierte *Konzeptbeziehungen* (Def. 5.4) miteinander verbunden sind.

ISRM Terminologie

Zusammengefasst besteht eine *Terminologie* (Def. 5.6) in der *Domäne* (Def. 5.2) ISRM also aus wissensbildenden, miteinander *verbundenen Konzepten* (Def. 5.4) und *Begriffen* (Def. 5.5), die ein *Konzept* (Def. 5.3) sprachlich repräsentieren.

Harmonisierung

In den folgenden Abschnitten wird durch die Untersuchung von relevanten Rahmenwerken versucht, die Begriffe und Konzepte des ISRM aufzuarbeiten. Ein Rahmenwerk ist ein Dokument oder eine Reihe von Dokumenten, die ein System von Ideen, Regeln und Methoden beschreiben, um Aktivitäten in einem bestimmten Bereich, in diesem Fall ISRM, zu ermöglichen. In diesem Zusammenhang definiert ein Rahmenwerk seine eigene Terminologie, die Überschneidungen mit anderen Rahmenwerken haben kann oder auch nicht. Gemäß der Norm zur Harmonisierung von Konzepten und Begriffen [198] ist dies unvermeidlich, da sich „[c]oncepts and terms develop differently in individual languages and language communities, depending on professional, technical, scientific, social, economic, linguistic, cultural or other factors.“.

Äquivalenz

Da es keine allgemeingültige RM oder ISRM Terminologie gibt, muss untersucht werden, inwieweit sich diese Terminologien voneinander unterscheiden. Wenn sich zwei oder mehr Terminologien überschneiden, stellt sich die Frage, ob sie nur dieselben Begriffe verwenden oder dieselben Konzepte definieren bzw. ob es verschiedene Begriffe für dasselbe Konzept gibt. Diese „relation between designations in different languages representing the same concept“ [198] wird als *Äquivalenz* bezeichnet. Es kann davon ausgegangen werden, dass äquivalente Konzepte, die in mehreren gängigen Rahmenwerken vorkommen, für die ISRM Domäne wichtig sind und daher als Schlüsselkonzepte hervorgehoben werden sollten.

Definition 5.7: Schlüsselkonzept

Schlüsselkonzepte sind äquivalente *Konzepte* (Def. 5.3), die innerhalb einer Domain in verschiedenen *Terminologien* (Def. 5.1) enthalten sind. Auf sie kann in verschiedenen Quellen mit oder ohne Verwendung desselben *Begriffs* (Def. 5.5) Bezug genommen werden.

Standardisierung

Da Konzepte grundsätzlich unabhängig vom zugewiesenen Bezeichner sind, könnten die Rahmenwerke unterschiedliche Begriffe für äquivalente Konzepte definieren. Im Kontext der prozessübergreifenden und damit Framework-unabhängigen Zusammenarbeit stellt das ein Problem dar, da so keine einheitliche Kommunikation etabliert werden kann. An dieser Stelle ist somit eine gewisse Standardisierung der verwendeten Begriffe notwendig. Es stellt sich die Frage, ob für jedes Schlüsselkonzept auch ein Kernbegriff identifiziert werden kann, der mehrheitliche Akzeptanz gefunden hat.

Definition 5.8: Kernbegriff

Kernbegriffe sind solche Begriffe, die sich innerhalb einer Domain als Bezeichner für ein *Schlüsselkonzept* (Def. 5.7) durchgesetzt haben.

5.2 Terminologie in der Literatur

Nachdem nun die notwendigen Grundlagen für das Verständnis im Bereich der Terminologielehre etabliert wurden, wird als Nächstes die relevante Literatur im Themenbereich untersucht. Einige Autoren haben bereits über Terminologie im RM geschrieben und dabei verschiedene Vorgehensweisen präsentiert, um Begriffe und Konzepte zu identifizieren, bewerten oder zu vergleichen. Weiterhin liefern die bereits vorgestellten ISRM Frameworks (Kapitel 2.3) oftmals eigene Begriffe und Konzepte, welche im Terminologievergleich genauer analysiert werden sollen.

5.2.1 Wissenschaftliche Veröffentlichungen

Obwohl Terminologien ein verbreitetes Forschungsthema sind, gibt es vergleichsweise wenige Veröffentlichungen, die sich speziell mit ISRM befassen. Häufig finden sich einschlägige Artikel auch in den übergeordneten Bereichen IS oder RM. Im Folgenden werden die Publikationen von drei Autoren vorgestellt, die sich besonders mit der Terminologie in den Bereichen IS/RM/ISRM beschäftigt haben, und ihre Forschungen in den Kontext dieser Arbeit gestellt.

Expertenanalyse von Schlüsselkonzepten

Brooks [21] beschreibt einen umfassenden Ansatz zur Ermittlung von ISRM Schlüsselkonzepten durch Extraktion von Kategorien aus vermitteltem Sicherheitswissen. Nach einem quantitativen Ansatz zur Ermittlung von RM Kategorien, der auf den in Hochschulkursen für Sicherheit gelehrten Schlüsselthemen basierte, konnte eine endgültige Liste von 14 Kategorien erstellt werden. Diese Liste wurde dann von einer Gruppe von Experten verwendet, um Verbindungen zwischen den Kategorien zu identifizieren, was im Ergebnis zur einem psychometrischen Konzeptdiagramm führte. Diese Arbeit zeigt, wie wichtig ein gemeinsames Verständnis auf der Grundlage der Terminologie ist und dass die Begriffe selbst wichtige Konzepte enthalten. Die ursprüngliche Studie wurde bereits 2009 veröffentlicht [199], und die Kategorien sind an die Terminologie der australischen RM-Norm von 2004 [200] angeglichen, die inzwischen durch die ISO 31000 ersetzt wurde. Obwohl diese Studien nach wie vor wertvoll sind, erscheint eine Aktualisierung nach mehr als 10 Jahren in einem schnelllebigen Bereich wie dem der IS für sinnvoll. Darüber hinaus zieht die Studie ihre Schlussfolgerung über die Verknüpfung der Kategorien aus dem Expertenwissen und stellt damit dar, wie Fachleute bestimmte Konzepte tatsächlich verstehen. Während dies ein solider Ansatz ist, kann eine auf Fachliteratur basierende Untersuchung zu einem anderen Konzeptmodell führen, welches eine andere Perspektive auf dasselbe Thema bietet. Die Stärke des im Folgenden vorgestellten Ansatzes der Dokumentenprüfung ist die Tatsache, dass es eine objektive Analyse der Konzepte ermöglicht, ohne implizite Annahmen von Experten einzubeziehen. Aus dem Vergleich der beiden Modelle ließe sich ableiten, wie viel des damaligen Expertenwissens inzwischen in die Rahmenwerke und damit in die gängigen ISRM-Standards eingeflossen ist.

Untersuchung und Diskussion der Standardbegriffe

Aven [69] analysiert die allgemeine RM-Terminologie der ISO-Normen auf der Grundlage des ISO Guide 73 [67], welcher zum damaligen Zeitpunkt erst neu erschienen war. Die Begriffe und ihre Definitionen werden inhaltlich intensiv untersucht und auf ihre Konsistenz geprüft. Dies wirft verschiedene Fragen über die inhärente Bedeutung der darin definierten Begriffe und Begriffsbeziehungen auf, insbesondere in Bezug auf Risiken und Unsicherheit. Es zeigt sich, dass die ISO ISRM-Terminologie nicht geeignet ist, einen konsistenten, konzeptionellen Rahmen für den Bereich zu schaffen. Zum einen werden nicht alle verwendeten Begriffe eindeutig definiert und manche impliziten Konzepte nur angedeutet. Insbesondere die verwendete Definition eines Risikos als Unsicherheit der Zielerreichung ist dabei inhaltlich sehr unscharf. Dabei wird deutlich, wie wichtig Begriffe für die Kommunikation und das Verständnis von Schlüsselkonzepten im ISRM/RM sind. Während die Publikation sehr detailliert auf die Definitionen und Konzepte des Guide 73 eingeht, werden andere RM-Normen nicht berücksichtigt. Andere Veröffentlichungen des Autors befassen sich ebenfalls mit der Terminologie und ihrer Standardisierung, allerdings mit dem Fokus auf RM im Allgemeinen und nicht speziell für den Teilbereich IS. Es bietet sich daher an, neben dem allgemeinen RM ebenfalls die spezifische ISRM-Terminologie zu untersuchen.

Review existierender Standards

Luko [201] führt eine Terminologieüberprüfung auf der Grundlage von *ANSI/ASSE Z690.1* [202] durch, bei der es sich um eine nationale Entsprechung des ISO Guide 73 [67] handelt. Die Norm und ihre Definitionen werden sehr detailliert untersucht. Nachfolgende Veröffentlichungen befassen sich dann mit Grundsätzen und Leitlinien [203] und Bewertungstechniken [204]. In diesen Veröffentlichungen wird der Schwerpunkt auf eine spezielle Überprüfung der Norm und der darin enthaltenen RM-Begriffe und -Techniken gelegt. Die Autoren hatten zuvor die Bedeutung der Terminologie hervorgehoben und sie im Kontext der ISO-Normen untersucht [205, 194]. Obwohl diese Veröffentlichung die Terminologie des ISO Guide 73 für allgemeines RM untersucht, geht sie nicht speziell auf die IS ein. In diesem Zusammenhang wird weder ein Vergleich mit anderen Rahmenwerken vorgenommen noch werden die grundlegenden Konzepte analysiert. Nichtsdestotrotz ist die Überprüfung in ihrem Umfang tiefgreifend und es lohnt sich, sie mit einem Fokus auf ISRM zu erweitern.

5.2.2 Terminologie in Frameworks

Neben den wissenschaftlichen Untersuchungen zum Thema definieren auch die vorgestellten ISRM-Rahmenwerke (Abschnitt 2.3) ebenfalls eigene Terminologien. Neben diesen gibt es viele weitere Publikationen, die aber meist eine bereits etablierte Terminologie verwenden. Die überwiegende Mehrheit der Literatur scheint sich auf dieselbe Reihe von Rahmenwerken zu beziehen. Erfahrungen aus der Praxis zeigen ebenfalls, dass der Abdeckungsgrad des ISRM durch die genannten Rahmenwerke in Organisationen sehr hoch ist. Trotz vieler Versuche in den vergangenen Jahren ist es nicht gelungen, eine universelle und übergreifen-

de RM-Terminologie zu schaffen [84]. Ein Versuch ist das von der Society for Risk Analysis veröffentlichte Glossar [206]. Ähnlich wie der hier vorgestellte Ansatz zielt er darauf ab, verschiedene RM-Kernbegriffe zu sammeln und zu gruppieren, hat aber keinen spezifischen Fokus auf ISRM. Der Versuch, die Terminologie zu vereinheitlichen, scheint im ISRM Bereich jedoch vielversprechender zu sein. Da es lediglich einen Teilbereich umfasst, ist zu erwarten, dass die Begriffe weniger allgemein und die Konzepte domänenspezifisch sind.

ISO

Die ISO 31000 [35] selbst definiert nur eine kleine Anzahl von Begriffen, verweist aber auf den allgemeinen Guide 73 [67]. Dieser Leitfaden wiederum hat mit *ANSI/ASSE Z690.1* [202] ein nationales ANSI Äquivalent, welches Vokabular für RM bereitstellt. Ein Vergleich der beiden äquivalenten Normen wurde bereits von Luko [201] durchgeführt. Darüber hinaus bieten sowohl ISO[1] als auch IEC[2] eine kostenlose Online-Datenbank mit allgemeinen und spezifischen Begriffen aus allen Normen an. Die spezifische ISO/IEC 27000 [49] selbst bietet Terminologie für IS im Allgemeinen, die ISO/IEC 27005 [98] speziell für ISRM. Insgesamt sind die von der ISO bereitgestellten Informationen sehr gut strukturiert. Die Zusammenhänge zwischen den Begriffen werden größtenteils durch Inline-Referenzen dargestellt. Aufgrund der Standardisierung und der Verweise auf andere Normen werden in den ISO und IEC Normen meist durchgängig die gleichen Begriffe verwendet, weshalb sie in verschiedenen Dokumenten immer gleich definiert sind. Dadurch wird eine Einheitlichkeit in der gesamten ISO-Umgebung hergestellt.

NIST

Die NIST-Dokumente enthalten im Anhang jeweils ein umfassendes Glossar. Die Terminologie ist weitgehend harmonisiert und in allen Dokumenten anwendbar. Der Umfang der definierten Begriffe ist jedoch sehr unterschiedlich. Es gibt allgemeine (z.B. Konfigurationselement), umgebungsspezifische (z.B. Bundesbehörde) sowie IT-spezifische (z.B. Firmware) Begriffe. Im Allgemeinen sind die einzelnen Begriffe gut definiert, aber die Beziehung zwischen verschiedenen Begriffen ist nicht eindeutig geklärt. Einige Begriffe sind aus verwandten Publikationen wie FIPS 200 [92] oder CNSSI 4009 [207] übernommen.

RiskIT

Die zweite Auflage des *Risk IT Framework* [119] enthält im Abschnitt Definitionen und Terminologie nur sehr wenige Begriffe. Es wird auch darauf hingewiesen, dass allgemein anerkannte Konzepte aus anderen Rahmenwerken verwendet werden, die verwendeten Begriffe können jedoch von diesen abweichen. Das Rahmenwerk ist jedoch so verfasst, dass die meisten Unterkapitel ein bestimmtes Konzept definieren und beschreiben, wie z. B. *Risikotoleranz* oder *Risikoreaktion*.

[1] `https://www.iso.org/obp`
[2] `https://std.iec.ch/glossary`

FAIR

Open FAIR unterstreicht die Bedeutung einer gemeinsamen Sprache und allgemeiner Konzepte auf dem Gebiet des ISRM, um beispielsweise die Kluft zwischen IT- und Business-Managern zu überwinden. Mit der Open FAIR *Risk Taxonomy (O-RT)* [122] wurde daher ein Dokument für die Definition der eigenen Terminologie veröffentlicht. Die Open Group war bestrebt, ihre Konzepte so universell anwendbar und kompatibel wie möglich zu gestalten.
Es ist erwähnenswert, dass die Prinzipien, die der Risikobewertung zugrunde liegen, komplexer zu sein scheinen als die der anderen Rahmenwerke. Dies könnte darauf zurückzuführen sein, dass der FAIR-Ansatz stärker auf eine realistische Risikoberechnung ausgerichtet ist und versucht, die Genauigkeit durch Hinzufügen zusätzlicher Variablen zu verbessern. Die Kernkomponenten des Risikos sind die *Loss Event Frequency* und die *Loss Magnitude*. Sie lassen sich in einen verzweigten Baum verschiedener Konzepte aufteilen und erben ihre Werte von diesen zugrunde liegenden Aspekten. Es lässt sich sagen, dass dieser Ansatz einen starken Fokus auf die mathematische Seite der Risikobewertung hat. Trotzdem stellt das Modell auch einen wertvollen Untersuchungsgegenstand dar, wenn nur Konzepte auf höchster Ebene wie *Loss Event Frequency* und *Loss Magnitude* verwendet werden.

MoR

Auch MoR verfügt über ein Glossar der wichtigsten Begriffe und definiert weitere einzelne Begriffe wo sie verwendet werden. Allerdings sind die Konzepte im Vergleich zu den anderen Rahmenwerken wesentlich einfacher gehalten. Dennoch wird die Terminologie auf vergleichbare Weise definiert. Aufgrund seiner Fokussierung auf praktische Aspekte fügt MoR dem Review eine weitere wichtige ISRM-Perspektive hinzu. Ein einfacher Vergleich der Begriffe von MoR und der 2009er Version der ISO 31000 wurde von der British Standards Institution im Jahr 2013 durchgeführt [208], jedoch mit einem anwendungsorientierten Fokus und ohne Berücksichtigung von Konzepten. Wie bereits erwähnt wird MoR von derselben Organisation wie ITIL herausgegeben. Es gibt jedoch keinen Zusammenhang zwischen diesen beiden Rahmenwerken und sie verwenden kein gemeinsames Glossar oder Wörterbuch. Es wäre sicherlich interessant, zu untersuchen, ob die RM-Terminologie der Rahmenwerke ähnlich ist. Zumal die neueste Version ITIL 4 auch RM (als eine sogenannte Praxis) enthält. Dies würde jedoch zu weit führen und liegt außerhalb des Scopes dieser Arbeit.

Andere

Die Rahmenwerke COBIT und ENISA RM wurden nicht weiter betrachtet, da sie keine eigene Terminologie definieren. ENISA liefert ein Glossar [209], aber dieses stützt sich wiederum auf ISO-Definitionen. Auch das ISACA Glossar [210] enthält Begriffe, jedoch wird weder in RiskIT noch in COBIT direkt darauf verwiesen. Weiterhin handelt es sich beim IT-Grundschutz lediglich um ein nationales Rahmenwerk, dessen Begriffe international keine Relevanz haben sollten.

5.3 Vergleich der Terminologie

Frameworks

Im vorangegangenen Abschnitt wurden ISO/IEC, NIST SP 800, RiskIT, OpenFAIR und MoR im Hinblick auf ihre Terminologie untersucht. Im Folgenden sollen nun Begriffe und Konzepte dieser Rahmenwerke untersucht und miteinander verglichen werden. Bei der Analyse der Dokumente hat sich gezeigt, dass Umfang und Reichweite der von den einzelnen Rahmenwerken definierten Terminologie sehr unterschiedlich ist. Dabei unterscheidet sich nicht nur die absolute Anzahl der Begriffe, sondern auch, wie umfassend sie definiert (Charakteristiken) und miteinander verknüpft sind (Konzeptbeziehungen). Oft werden Begriffe nicht explizit definiert, sondern nur implizit in ihrem Verwendungskontext. Daraus ergibt sich die potenzielle Gefahr unscharfer Definitionen und einer inhomogenen Verwendung von Begriffen. Daher wird im Folgenden eine Methode verwendet, welche nur eindeutig definierte Begriffe und klar erkennbare Konzepte berücksichtigt. Durch einen anschließenden Vergleich und der Beschränkung auf gemeinsame Begriffe beim Ableiten von Schlüsselkonzepten, werden unklare Definitionen zusätzlich aussortiert.

5.3.1 Methodik des Reviews

Vorgehen

Bei einer Terminologie geht es nicht nur um Benennung und Etikettierung von Entitäten, sondern grundsätzlich um Begriffe und deren Bedeutung: „Terminology is fundamentally concerned with names and the process of naming. Any discussion of names and naming must also include a discussion of language and meaning“ [195, S. 11]. Es ist also nicht sinnvoll, die Begriffe der Rahmenwerke als inhaltslose Bezeichner zu vergleichen. Stattdessen sind ihre Definitionen zu betrachten, welche letztlich ein Konzept beschreiben können. Das Ziel ist es, bei der Untersuchung Überschneidungen zwischen den Terminologien zu identifizieren. Dabei gibt es beim Vergleich zweier Rahmenwerke genau vier Möglichkeiten: (1) sie haben keine Überschneidungen in ihrer Terminologie; (2) sie verwenden denselben Begriff für unterschiedliche Konzepte; (3) sie definieren dasselbe Konzept, ohne denselben Begriff zu verwenden; (4) sie definieren dasselbe Konzept unter Verwendung desselben Begriffs. Dieser Vorgang wird als Harmonisierung bezeichnet, eine „activity leading to the establishment of a correspondence between two or more closely related or overlapping concepts having professional, technical, scientific, social, economic, linguistic, cultural or other differences, in order to eliminate or reduce minor differences between them“ [198]. Es ist anzunehmen, dass sich diese Überschneidungen tatsächlich auf dieselben ISRM-Konzepte beziehen (Äquivalenz), die zur Definition einer Reihe von ISRM-Schlüsselkonzepten zusammengefasst werden können.

Explizite Definitionen

Bei diesem Terminologievergleich wurden nur explizit definierte Begriffe verwendet, ohne implizit definierte Konzepte zu berücksichtigen, indem nur Glossare, Terminologiedokumente und andere Dokumententeile berücksichtigt wurden, in denen Begriffe eindeutig definiert sind. Schmidt et al. [211] stellen eine Methode zur Durchführung einer tiefgehenden Inhaltsanalyse im Bereich des Servicemanagements (Domain) vor, bei der unter anderem Artefakte und Aktivitäten aus Prozessframeworks extrahiert werden. Sie weisen im Speziellen darauf hin, dass für den Einsatz eines Frameworks in der Praxis häufig externes

Wissen erforderlich ist, um logische Lücken zu schließen. Jedoch würde das Einbeziehen von Begriffen, die lediglich implizit innerhalb der Rahmenwerke definiert sind, zu unerwünschten Risiken führen. So könnten Annahmen über die untersuchten Konzepte auf der einen Seite zu Begriffen führen, die zwar beschrieben, aber nicht definiert sind oder auf der anderen Seite zu Konzepten ohne zugehörigen Begriff. Beides sind ungewollte Ergebnisse, die eine inkonsistente Terminologie erzeugen würden. Insgesamt sollte es bei einem Terminologiereview vermieden werden, externes Wissen durch die Interpretation von Begriffen einzuführen, die nicht explizit durch das Framework selbst etabliert wurden. Im Gegensatz dazu könnte ein Ansatz wie von Brooks [21] beschrieben verwendet werden, wenn speziell die Terminologie auf der Grundlage von Expertenwissen untersucht werden soll. Der Zweck dieser Analyse besteht jedoch darin, Begriffe zu extrahieren, die explizit in diesen Rahmenwerken definiert sind, um Kernbegriffe zu ermitteln, sowie benannte Konzepte zu vergleichen, um Schlüsselkonzepte zu identifizieren.

Dokumente

Da einige Rahmenwerke aus mehreren Dokumenten bestehen, werden sie in Bezug auf ihre Terminologie als Einheit betrachtet. Daher wurden die oben genannten Dokumente wie folgt gruppiert:

- **FAIR:** OpenFAIR Risk Taxonomy
- **ISO:** ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27005, ISO 31000, ISO Guide 73
- **MoR:** Management of Risk: Guidance for Practitioners
- **NIST:** NIST SP 800-30, NIST SP 800-37, NIST SP 800-39
- **RiskIT:** Risk IT Framework v1, Risk IT Framework v2

Scope

Sofern nicht ein bestimmtes Dokument genannt wird, beziehen sich alle weiteren Erwähnungen eines Rahmenwerks auf die Gruppe in dieser Liste. Der gesamte Terminologievergleich wurde auf Basis der englischen Primärliteratur durchgeführt. Eine Übersetzung der Begriffe würde den Vergleich verfälschen. Daher werden im Folgenden die englischen Begriffe verwendet und erst das Endergebnis wird übersetzt. Einige Rahmenwerke enthalten allgemeine Begriffe, die für ISRM nicht notwendig sind. Um einen aussagekräftigen und vergleichbaren Überblick zu schaffen, wurde die Sammlung von Begriffen bereinigt, indem alle Begriffe entfernt wurden, die nicht direkt mit dem ISRM in Verbindung stehen. Diese Begriffe können bereichsspezifisch sein oder aus verwandten Bereichen stammen, z.B. *Assurance* oder *System* im NIST-Rahmenwerk.

5.3.2 Semantische Analyse

Begriffe

Die Terminologien der Rahmenwerke wurden entsprechend der Gruppierung untersucht, d.h. jede dieser Gruppen definiert eine Reihe von Begriffen. Nach der Auflistung der Begriffe aus den einzelnen Dokumenten wurden diese in einem nächsten Schritt analysiert, um gleiche Konzepte in allen Rahmenwerken zu ermitteln. Zu diesem Zweck wurden alle Begriffsdefinitionen semantisch geprüft und die Merkmale der beschriebenen Konzepte miteinander verglichen. So wird beispielsweise der Begriff *impact* in MoR [127] als „result of a particular threat or opportunity actually occurring“ definiert. Darin referenziert wird ein *threat*, ein „uncertain event that could have a negative impact on objectives or benefits“. Beide Definitionen zusammen zeigen, dass der *impact* ein Konzept über den Einfluss eines Ereignisses auf die Zielerreichung beschreibt. Dies ist inhaltlich gleich zu dem „outcome of an event affecting objectives“, was die ISO-Definition [49] von *consequence* ist. Daraus lässt sich schließen, dass sich beide Rahmenwerke auf dasselbe Konzept beziehen, somit ist eine Begriffsäquivalenz gegeben. Dieses Verfahren wurde für alle Begriffe durchgeführt, um einen umfassenden Abgleich der Terminologien der Rahmenwerke zu erstellen.

Konzept-vergleich

Daraus ergibt sich ein Mapping aller ähnlichen Begriffe der fünf Frameworks. Dieses listet alle Begriffe der Frameworks, zu denen es eine Übereinstimmung gab, d.h. mindestens zwei Frameworks verweisen auf ein ähnliches Konzept. Die alte und neue Version von RiskIT wurden dabei einzeln aufgelistet, da sie einen unterschiedlichen Glossar definieren und der direkte Vergleich interessante Ergebnisse liefert. So ist es überraschend zu sehen, das beide sowohl verschiedene Begriffe verwenden, als auch unterschiedliche Konzepte definieren. In der Auswertung wurden die zwei Versionen jedoch gemeinsam berücksichtigt, um das Ergebnis nicht zu verfälschen. Das die Frameworks unterschiedliche Begriffe für dasselbe oder ein ähnliches Konzept verwenden, war dabei ein erwartetes Ergebnis. Zusätzlich hat sich allerdings auch herausgestellt, dass manche Frameworks ein Konzept verwenden, ohne dazu einen Begriff zu definieren. Ein Indiz für die Existenz des Konzeptes liefern dabei andere Begriffsdefinitionen, die dieses beschreiben oder Konzepte, die dazu in Beziehung stehen. Somit wird also ein Konzept definiert bzw. eine Konzeptbeziehung aufgestellt, ohne einen eigenen Begriff damit zu verknüpfen. Es ist anzunehmen, dass dies Begriffsleere in der Praxis nicht auffällt, da Anwender bereits bekannte Begriffe verwenden.

Auswertung

Ziel dieser Analyse ist es, ISRM-Schlüsselkonzepte zu identifizieren, d.h. Konzepte, die in allen Rahmenwerken vorkommen. Dazu ist es erforderlich, die während des Konzeptabgleichs erstellte Zusammenstellung zu reduzieren, um Konzepte zu entfernen, die nur in wenigen Rahmenwerken vorkommen. Als Indikator für die Bedeutung eines Konzepts wurde daher der Definition Count (DC) festgelegt. Er beschreibt die Anzahl der Rahmenwerke, die ein bestimmtes Konzept definieren, unabhängig davon, ob sie denselben oder einen anderen Begriff verwenden. Ein Schlüsselkonzept muss in der Mehrzahl der Rahmenwerke verwendet werden, da es ansonsten offensichtlich nicht signifikant ist. Daher wird als Schwellwert festgelegt, dass mindestens drei der fünf Rahmenwerke ein Konzept definieren ($DC \geq 3$). Folglich werden alle Konzepte, die nur in wenigen Rahmenwerken verwendet werden ($DC < 3$), nicht als Schlüsselkonzepte betrachtet und aus der Zusammenstellung entfernt. Die verbleibenden Konzepte können in verschiedene Gruppen aufgeteilt werden,

welche ihr Relevanz beschreiben. Sie wurden in die drei Kategorien vollständig abgedeckte (DC5), überwiegend abgedeckte (DC4) und teilweise abgedeckte (DC3) Konzepte unterteilt. Das Ergebnis dieses Verfahrens ist in Tabelle 5.1 dargestellt. Jede Zeile steht für ein identifiziertes Konzept, jede Spalte für den im jeweiligen Rahmen verwendeten Begriff, sofern vorhanden. Fett gedruckte Begriffe kennzeichnen Kernbegriffe, d.h. überwiegend verwendete Begriffe, welche im Folgenden verwendet werden. In der ersten Spalte wurden alle Begriffe nach ihrem DC geordnet. Die Tabelle ist alphabetisch nach der ISO-Spalte sortiert, das hat jedoch keine weitere Bedeutung. Als Ergebnis dieser Konsolidierung konnte die gesamte Terminologiesammlung auf 42 eindeutige Begriffe reduziert werden, die 21 Konzepten zugeordnet sind. Im Folgenden werden die bei dieser Analyse entdeckten Erkenntnisse und Anomalien näher erläutert.

5.3.3 Diskussion der Ergebnisse

ISO Begriffe

Es stellte sich heraus, dass die meisten Begriffe in den ISO-Normen tatsächlich in den verschiedenen Dokumenten des Rahmenwerks einheitlich definiert sind. Es werden lediglich neue Begriffe zu den Dokumenten in der Rahmenhierarchie hinzugefügt, aber vererbte Definitionen werden normalerweise nicht geändert. Allerdings gibt es einige Inkonsistenzen zwischen den Dokumenten. Die in Tabelle 5.1 aufgeführte *vulnerability* wird beispielsweise in ISO 27000 als „weakness of an asset or control [...] that can be exploited by one or more threats“ [49] definiert, während sie im Guide 73 als „intrinsic properties of something resulting in susceptibility to a risk source [...] that can lead to an event with a consequence“ [67] definiert wird. Dennoch bleibt die ISO ein größtenteils konsistentes Framework und letztlich auch das am besten strukturierte in dieser Analyse, insbesondere aufgrund der klar definierten Beziehungen zwischen den Definitionen.

Acceptance vs Retention

Der Umgang mit Risiken nach deren Bewertung und Priorisierung ist eine Schlüsselaktivität im ISRM, bei der die informierte Akzeptanz von Risiken eine zentrale Rolle spielt. RiskIT verwendet in diesem Zusammenhang den Begriff *risk acceptance*, während MoR den Begriff *retention* verwendet. ISO [67] hingegen definiert beides, mit *risk acceptance* als „informed decision to take a particular risk“ und *risk retention* als „acceptance of the potential benefit of gain, or burden of loss, from a particular risk“. Anhand der Definitionen war es jedoch nicht möglich zu erkennen, ob und wie sich die beiden Konzepte unterscheiden. Eine Interpretation wäre, dass es bei der *risk acceptance* um die Entscheidung zur Akzeptanz, d.h. die Aktivität, geht, während die *retention* den Umstand bezeichnet, dass ein Risiko akzeptiert wird, d.h. seinen Zustand. Dies ist jedoch nur eine Annahme auf Basis der ISO-Definitionen, die weder von einem der anderen Rahmenwerke gestützt noch innerhalb der Aktivitäten der Prozess einheitlich eingesetzt wird. In ihren eigenen Dokumenten verwendet die ISO jedoch hauptsächlich den Begriff *risk acceptance*. NIST nutzt den Begriff *risk acceptance* in seinen Dokumenten, definiert ihn allerdings niemals explizit. Es scheint, dass *risk acceptance* und *risk retention* sich eigentlich auf dasselbe Konzept beziehen, nur die ISO-Definition beider Begriffe ist irritierend. Eine Expertenevaluierung könnte helfen festzustellen, ob Praktiker tatsächlich zwischen den Begriffen und Konzepten unterscheiden oder diese in der Praxis analog verwenden.

Tabelle 5.1: ISRM Schlüsselkonzepte abgeleitet aus dem ISRM Terminologievergleich

	FAIR	ISO	MoR	NIST	RiskIT
DC5 – Vollständig Abgedeckt	loss magnitude	consequence	**impact**	**impact**	**impact**
	threat event	**event**	risk event	threat event	**event**
	risk	level of risk	**risk**	**risk**	**risk**/business risk
	loss event frequency	**likelihood**/probability/ frequency	probability	likelihood of occurrence	**likelihood**/ frequency
	threat agent	**risk source**	risk cause	threat source	threat
	threat	**threat**	**threat**	**threat**	threat event
DC4 - Überwiegend Abgedeckt	- - -	**residual risk**	**residual risk**	**residual risk**	**residual risk**
	asset	**asset**	- - -	**asset**	**asset**
	risk assessment approach	**risk management process**	risk management process guide	risk assessment methodology	- - -
	- - -	**risk mitigation**/reduction	reduction	**risk mitigation**	**risk mitigation**
	- - -	risk treatment	**risk response**	**risk response**	risk disposition
	vulnerability	**vulnerability**	- - -	**vulnerability**/weakness	**vulnerability**
DC3 - Teilweise Abgedeckt	action	**attack**	- - -	(cyber) **attack**	- - -
	control	**control**	- - -	**control**/countermeasure	- - -
	- - -	**risk acceptance**/retention	retention	- - -	**risk acceptance**
	- - -	**risk appetite**	**risk appetite**	- - -	**risk appetite**
	- - -	**risk avoidance**	removal	- - -	**risk avoidance**
	- - -	risk financing	transfer	- - -	**risk transfer**
	- - -	**risk register**	**risk register**	- - -	risk portfolio view
	- - -	**risk tolerance**	**risk tolerance**	- - -	**risk tolerance**
	- - -	- - -	severity of risk	impact level/value	**magnitude**
DC2 – Uneinheitlich definiert		availability		availability	
		confidentiality		confidentiality	
		risk criteria		criticality	
		risk description			risk statement
		risk evaluation			evaluating […] risk
		risk management plan	risk management plan		
		risk management policy	risk management policy		
		risk matrix	risk map		
		risk register			risk portfolio view
				risk factor	risk factor
	loss event				loss event
	control strength			control effectiveness	
			inherent risk		inherent risk
			risk profile		risk profile

Konsistenz

Wie bereits erwähnt, wurden verschiedene Dokumentfamilien wie ISO 31000/27000 und NIST 800 als Gruppe geprüft und die in einem oder mehreren Dokumenten definierten Begriffe konsolidiert, um die Zuordnung in Tabelle 5.1 zu erstellen. Dabei zeigte sich jedoch, dass es unklar ist, wann ein Begriff, der bereits in einem übergeordneten Dokument definiert wurde, in einem untergeordneten Dokument erneut erwähnt wird. Zum Beispiel soll ISO 27005 die Terminologie von ISO 27000 sowie von Guide 73 übernehmen: Ein *event* wird in allen drei Dokumenten definiert, die *vulnerability* nur in 27000 und *hazard* nur im ISO Guide 73. Dennoch scheinen alle Begriffe für RM, IS und ISRM relevant zu sein. Da die ISO 27000er Dokumente neuer sind als Guide 73, würde dies zumindest die Einführung neuer Begriffe erklären, nicht aber die anderen Ungereimtheiten. Ähnliche Beispiele lassen sich auch für NIST finden. Dies deutet darauf hin, dass die Dokumentenfamilien nicht vollständig integriert oder synchronisiert sind. Dies bestätigt den Eindruck von Aven [69], der bereits feststellte, dass die von den ISO-Dokumenten festgelegte Terminologie allein nicht geeignet ist, um einen konsistenten konzeptionellen Rahmen für RM zu schaffen. Ob diese Inkonsistenzen bei der Umsetzung von ISRM tatsächlich relevant sind oder ob dies dazu führen könnte, dass sich unterschiedliche Begriffe in der Praxis in unterschiedlichem Maße durchsetzen, kann an dieser Stelle nicht beurteilt werden.

Assets

Das Konzept des Assets war schwierig zu bewerten, was eine Überraschung war, da es oft als ein grundlegendes Konzept des ISRM erscheint. Obwohl vier der Rahmenwerke dieses Konzept verwenden, wird es nur in RiskIT und FAIR ausdrücklich definiert. Sowohl NIST als auch ISO verwenden den Begriff *asset* recht häufig und stellen Begriffsbeziehungen als Teil anderer Begriffsdefinitionen her, definieren ihn aber nicht. Es gibt jedoch Dokumente der ISO 27000-Familie, die sich nicht auf RM beziehen, die ein *asset* als „anything that has value to an individual, an organization or a government“ [212] definieren, aber überraschenderweise keines der risikobezogenen Dokumente, d.h. 27005, 31000 oder Guide 73. Seltsamerweise enthielt die ISO 27005er Version von 2005 eine Definition des Begriffs *asset*, die jedoch in der aktuellen Version entfernt wurde. MoR verwendet weder den Begriff *asset* noch scheint es ein entsprechendes Konzept anzubieten. Stattdessen identifiziert es Bedrohungen (*threats*) und Chancen (*opportunities*) in Abhängigkeit davon, ob die Organisation ihre Ziele erreichen kann. Wir gehen davon aus, dass es sich dabei nicht um konkurrierende Konzepte handelt, sondern dass Assets lediglich ein Mittel sind, um die ansonsten schwer messbare Unsicherheit bei der Zielerreichung abzuleiten. In diesem Fall wären Vermögenswerte für das ISRM nicht wesentlich, wenn die Auswirkungen auf die Unternehmensziele auf andere Weise bewertet werden können.

CIA

Eine überraschende Beobachtung ist, dass die bekannten IT-Ziele (CIA) nicht immer definierte Begriffe sind. Der sogenannte CIA-Dreiklang oder das goldene Dreieck spielt eine zentrale Rolle in der Anwendung und Lehre von IS sowie dem wertebasierten, d.h. auf Assets basierendem ISRM [213]. Insbesondere das Integritätsziel wird nur von NIST definiert. Ein Blick auf die inhaltlichen Abschnitte des Frameworks zeigt, dass die Integrität (von Informationen) zwar häufig angesprochen wird, aber nicht als wesentliches Konzept für RM wahrgenommen zu werden scheint. Die Ziele Verfügbarkeit und Vertraulichkeit werden nur von ISO und NIST definiert. Die Tatsache, dass CIA nur in ISO und NIST definiert ist, könnte daran liegen, dass diese Rahmenwerke auch allgemeine IS abdecken,

während FAIR, MoR und RiskIT ISRM-spezifisch sind.

Entwicklungen

Eine Erkenntnis von Brooks [21] war, dass der Begriff Bedrohung von den Experten zwar als Schlüsselbegriff anerkannt wurde, aber in keiner der damals geltenden Normen definiert war. Es stellte sich heraus, dass sich dies inzwischen geändert hat. Heute haben alle fünf Rahmenwerke ein Bedrohungskonzept und verwenden sogar einen ähnlichen Begriff. Dies zeigt einerseits, dass sich die Rahmenwerke auf der Grundlage von Entwicklungen und Erfahrungen im Bereich des ISRM weiterentwickeln, andererseits aber auch, dass die ISRM-Konzepte bisher nicht stabil waren. Es kann also davon ausgegangen werden, dass sich die Rahmenkonzepte tatsächlich auf der Grundlage von Entwicklungen und Erfahrungen aus der Praxis weiterentwickeln und nicht notwendigerweise andersherum. Wenn dies der Fall ist, kann auch argumentiert werden, dass die definierten Konzepte immer auf Fortschritten in der Praxis beruhen und dass die Realität den Rahmenwerken daher zeitlich voraus ist.

Besonderheiten

RiskIT bietet die am schlechtesten definierte Terminologie. Insbesondere werden verschiedene Risikobegriffe verwendet, ohne sie ausreichend zu definieren. Aufgrund fehlender Details ist die Bedeutung von Begriffen wie *business risk, IT risk, IT risk issue* und *cyber risk* nicht klar darstellbar und eine Abgrenzung schwer möglich. Eine vertiefte Überprüfung von COBIT könnte zeigen, ob diese Unterscheidung im weiteren Kontext der IT/IS-Governance geklärt ist. Weitere Unterschiede ergeben sich insbesondere im Hinblick auf den zentralen Risikobegriff, auf den im Folgenden noch näher eingegangen wird.

5.4 Etablieren der Konzeptbeziehungen

Durch die Untersuchung der betrachteten Frameworks wurden nun 21 Schlüsselkonzepte und die zugehörigen Begriffe identifiziert. In den meisten Fällen sind dabei auch eindeutige Kernbegriffe zu erkennen, in Einzelfällen verwenden die Frameworks eine komplett unterschiedliche Sprache (z.B. risk source). Nun gilt es, die Zusammenhänge zwischen den einzelnen Konzepten zu untersuchen, d.h. die Konzeptbeziehungen zu beschreiben. Diese werden ebenfalls aus den Begriffsdefinitionen der Frameworks extrahiert und anschließend zusammengefasst.

Definition des Risikos

Im ersten Schritt soll dabei das grundsätzliche Risikokonzept genauer untersucht werden. Als zentrales Element des ISRM ist es besonders wichtig, da es sowohl den Zusammenhang der anderen Elemente maßgeblich beeinflusst, als auch für das allgemeine Verständnis essenziell ist. Im Kontext der Kollaboration innerhalb einer Allianz ist es zwingend erforderlich, dass alle Partner sich auf ein gemeinsames Risikokonzept einigen. Zwar ist das Ziel, dass die Organisationen ihre Prozesse größtenteils unabhängig voneinander ausführen und auch die Risikohöhe individuell festlegen können, aber trotzdem muss eine einheitliche Risikodefinition vorliegen. Schließlich ist ein Austausch von Risikoinformationen nicht sinnvoll, wenn nicht klar ist, welche Rahmenbedingungen (z.B. Wahrscheinlichkeit, Unsicherheit, Zielerreichung) der Risikoeinschätzung zugrunde liegen.

Beziehungen darstellen

Anschließend werden alle anderen Konzepte genauer untersucht und deren Konzeptbeziehungen extrahiert. Diese sind der letzte Teil, neben den Schlüsselkonzepten und Kernbegriffen, der einheitlichen ISRM Terminologie. Es gilt insbesondere festzustellen, ob die identifizierten Schlüsselkonzepte in einen sinnvollen Zusammenhang gebracht werden können oder ob dabei logische Lücken entstehen. Als Ergebnis wird ein Konzeptdiagramm erstellt, welches die Beziehungen zwischen den Schlüsselkonzepten darstellt.

5.4.1 Analyse des Risikokonzeptes

Das Vorgehen zur Definition des der Risiko-Methodik erfolgt analog zum Terminologievergleich. Der Begriff Risiko wird häufig in Verbindung mit den Begriffen Eintrittswahrscheinlichkeit und Auswirkung verwendet oder erklärt. Zur Analyse des Risikobegriffs sind die Definitionen der Begriffe Risiko (*risk*), Eintrittswahrscheinlichkeit (*likelihood*), Auswirkung (*impact*) und Ausmaß (*magnitude*) aus Tabelle 5.1 in Tabelle 5.2 aufgeführt. Abgesehen von der Verwendung unterschiedlicher Begriffe für gleiche Konzepte ist festzustellen, dass die grundlegende Definition eines Risikos in den meisten Rahmenwerken ähnlich oder sogar gleich ist. Bei näherer Betrachtung erweisen sich die Begriffsbeziehungen jedoch insbesondere bei den Rahmenwerken RiskIT und ISO als unterschiedlich.

Risikomodell

In allen Rahmenwerken wird ein Risiko als das Ergebnis einer Kombination aus Eintrittswahrscheinlichkeit und Auswirkung beschrieben. Abbildung 5.1 veranschaulicht die verschiedenen Risikokonzepte auf der Grundlage der Risikodefinition in Tabelle 5.2. Sie werden unter Verwendung derselben Struktur dargestellt, um den grafischen Vergleich der Konzeptbeziehungen zu erleichtern. Die Konzepte *[r]isk*, *[l]ikelihood* und *[i]mpact* sind dabei farblich hervorgehoben.

Konzeptbeziehungen

Wenn man die Definitionen auf diese Weise nebeneinander stellt, wird deutlich, dass die Struktur und der Zusammenhang dieser Konzepte grundsätzlich gleich sind. Erst bei der Betrachtung der ISO-Definitionen fällt auf, dass es ein weiteres ISO-spezifisches Risikokonzept gibt, das sich von den anderen unterscheidet, wie später beschrieben wird. Es ist anzumerken, dass RiskIT zwar ein ähnliches Risikokonzept definiert und verwendet, aber den Begriff *likelihood* selbst nicht ausdrücklich definiert. Dies ist jedoch nur in der neuesten Version der Fall, da das Framework mit dem letzten Upgrade einige Begriffe geändert hat (siehe Bezeichnung *old* in Tabelle 5.2). Zuvor wurde anstelle von Risiko der Begriff Geschäftsrisiko (*business risk*) und anstelle von Eintrittswahrscheinlichkeit die zeitbezogene Häufigkeit (*frequency*) verwendet.

ISO-Definition

Von besonderem Interesse ist die ISO-Definition, die sich von den anderen unterscheidet. Die ISO unterscheidet zwischen den Begriffen *risk* und *LoR*. Damit wird ein neues Metakonzept eingeführt, das in den anderen Rahmenwerken nicht enthalten ist. Während in den anderen Definitionen *risk* als eine Kombination aus *impact* und *likelihood* verstanden wird, entspricht dies in der ISO dem *LoR*. *Risk* wird als „effect of uncertainty on objectives“ [67] definiert, die einen *LoR* hat. Dieser *LoR* ist also nicht das Risiko selbst, sondern ein Merkmal von diesem, d.h. ein verwandtes Konzept. Diese Unterscheidung beeinflusst nicht nur das Risikokonzept, sondern vor allem die Verwendung seiner Begriffe. Eine andere Ansicht besagt, dass der *LoR* kein Konzept an sich ist, sondern nur eine Eigenschaft des Risikos, eine ähnliche Frage wie die, ob *impact* und *likelihood* wirklich Konzepte oder nur Eigenschaften sind. Die Annahme, dass es sich tatsächlich um Konzepte handelt, ist jedoch überzeugender, da sie Wissen über die Verwendung einer Idee transportieren und ihrerseits Eigenschaften haben, wie z.B. *uncertainty* und *time*.

Unsicherheit

Jedenfalls ist die ISO das einzige Framework, das über ein Risikokonzept verfügt, welches über die Berechnung eines durch *impact* und *likelihood* definierten Wertes hinausgeht. Aven [69] analysiert detailliert die Bedeutung und die Folgen dieser Konzepte mit besonderem Augenmerk auf die *uncertainty*. Er kommt zu dem Schluss, dass die Bedeutung der ISO-Definition des Risikos nicht klar definiert ist, was ein Hauptproblem darstellt, da es unterschiedliche Auslegungen des Konzepts ermöglicht. Diese Schlussfolgerung deckt sich mit den in dieser Arbeit präsentierten Ergebnissen, da der Vergleich mit anderen Rahmenwerken ebenfalls zeigt, dass das ISO-Konzept nicht eindeutig in andere ISRM-Konzepte eingeordnet oder mit ihnen verglichen werden kann.

Tabelle 5.2: Risikodefinition - Vergleich des Risikokonzeptes der fünf Frameworks

Quelle	Risk	Likelihood
FAIR	Risk	Loss Event Frequency
	The probable frequency and probable magnitude of future loss.	The probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.
ISO	Level of Risk	Likelihood
	magnitude of a risk, expressed in terms of the combination of consequences and their likelihood	chance of something happening
MoR	Risk	Probability
	An uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives. A risk is measured by a combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives.	This is the evaluated likelihood of a particular threat or opportunity actually happening, including a consideration of the frequency with which this may arise.
NIST	Risk	Likelihood of Occurrence
	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.
RiskIT	Risk / Business Risk *(old)*	Likelihood / Frequency *(old)*
	The combination of the likelihood of an event and its impact - - - - - A probable situation with uncertain frequency and magnitude of loss (or gain)	*none* - - - - - A measure of the rate by which events occur over a certain period of time

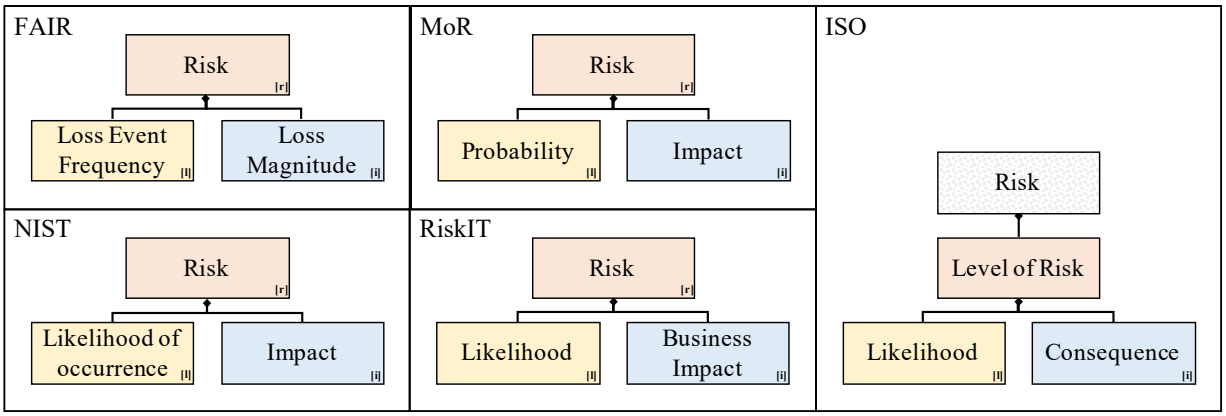
Tabelle 5.2: Risikodefinition (fortgesetzt)

Quelle	Impact	Magnitude	Uncertainty Risk
FAIR	Loss Magnitude	- - -	- - -
	The probable magnitude of loss resulting from a loss event.		
ISO	Consequence	- - -	Risk
	outcome of an event affecting objectives		effect of uncertainty on objectives
MoR	Impact	Risk effect	- - -
	Impact is the result of a particular threat or opportunity actually occurring.	A description of the impact that the risk would have on the organizational activity should the risk materialise.	
NIST	Impact/Potential Impact	Impact Level	- - -
	With respect to security, the effect [...] of a loss of confidentiality, integrity, or availability of information or a system.	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.	
RiskIT	Business Impact	Magnitude	- - -
	The net effect, positive or negative, on the achievement of business objectives	A measure of the potential severity of loss or the potential gain from a realised IT-related event/scenario	

Risikokonzept

Wie bereits erwähnt, setzt sich die Definition des Risikos im Wesentlichen aus den Begriffen *Auswirkung* und *Eintrittswahrscheinlichkeit* zusammen. Ein genauerer Blick auf ihre Definition zeigt jedoch, dass diese Begriffe zwar mit einem *Risiko* in Verbindung stehen, es allerdings nicht wirklich beschreiben. Stattdessen beschreibt die *Eintrittswahrscheinlichkeit* die Möglichkeit des Eintretens eines Ereignisses (*event*) und die *Auswirkung* dessen Ergebnis. Dies zeigt, dass das Risikokonzept nicht einfach ohne die Verwendung zusätzlicher Begriffe erklärt werden kann. Daher muss jede ISRM-Terminologie zumindest die Begriffe *Risiko, Auswirkung, Eintrittswahrscheinlichkeit* und *Ereignis* enthalten, um ein halbwegs brauchbares Risikomodell definieren zu können.

Abbildung 5.1: Darstellung der Risikodefinition anhand eines Konzeptdiagramms der 5 ISRM Frameworks



Unterschiede

Ausmaß des Risikos

Einige Rahmenwerke enthalten auch das sogenannte *Ausmaß (magnitude)* oder einen ähnlichen Begriff (siehe Tabelle 5.2). Dieses Konzept wird entweder einzeln oder in Kombination mit der *Auswirkung* festgelegt. Die Begriffe werden jedoch unterschiedlich verwendet und sind auch in den Rahmenwerken selbst nicht einheitlich. So verwendet FAIR beispielsweise den Begriff *Schadensausmaß (loss magnitude)* anstelle von *Auswirkung*. Das MoR spricht in seiner Risikodefinition vom *Ausmaß der Auswirkung auf Ziele (magnitude of its impact on objectives)*. Dabei handelt es sich nicht nur um die Verwendung unterschiedlicher Begriffe, sondern um unterschiedliche Konzepte. RiskIT beschreibt das *Ausmaß* als Schweregrad des Szenarios, was der NIST-Definition der *Auswirkungskategorie (impact level)* sehr ähnlich ist. Wie man sieht, gibt es in der Literatur kein gemeinsames Verständnis des Konzeptes *Ausmaß*, aber es gibt eine allgemeine Vorstellung in den Rahmenwerken darüber, was dieses Konzept sein soll. Vielleicht wird es sich in Zukunft weiterentwickeln, aber das Konzept/die Konzeptbeziehungen ist noch nicht ausreichend definiert, und die zugehörigen Begriffe sind in diesem Stadium noch nicht einheitlich.

Einheitliche Definitionen

Trotz der oben erwähnten spezifischen Unterschiede zeigt der Vergleich, dass die Definition des Risikos im Allgemeinen recht ähnlich und in den verschiedenen Rahmenwerken gut etabliert ist. Dies deutet darauf hin, dass das zugrunde liegende Konzept des Risikos im Bereich des ISRM bekannt und stabil ist. Der ISO-Ansatz der Konzentration auf den Ungewissheitsaspekt von Ereignissen (*uncertainty*) kann die künftige Entwicklung in diesem Bereich vorantreiben, auch wenn es sich dabei keineswegs um eine neue Idee im RM, sondern um einen ungewöhnlichen Ansatz im Bereich der Informationsgesellschaft handelt. In anderen Bereichen werden Risiko und Ungewissheit schon seit den Anfängen des RM diskutiert, wie z.B. bei Knight [214], der ihre Verbindungen und Unterschiede bereits 1921 diskutierte.

Entwicklung ISRM

Wie die illustrierten Risikodefinitionen gezeigt haben, hat sich das ISRM jedoch in Richtung einer Beschreibung der *Auswirkungen/Eintrittswahrscheinlichkeit* eines *Ereignisses* entwickelt, was ein viel greifbareres Konzept ist als die Ungewissheit, Ziele zu erreichen. Es bleibt abzuwarten, ob die ISO ihre Definition in den IS-bezogenen Normen anpassen wird, um der gängigen Industriepraxis zu folgen, oder ob das Konzept der *Unsicherheit* im ISRM in Zukunft an Bedeutung gewinnen wird.

5.4.2 Kernbegriffe und Schlüsselkonzepte

Nachdem die Terminologien der Rahmenwerke harmonisiert, die Schlüsselkonzepte identifiziert (Tabelle 5.1) und das Risikokonzept verstanden wurden (Tabelle 5.2), besteht der letzte Schritt darin, die Beziehungen der übrigen Konzepte zu untersuchen. Obwohl die Rahmenwerke Begriffe definieren, Konzepte beschreiben und verwenden, werden die Beziehungen zwischen den Konzepten oft nicht ausreichend dargestellt.

Interpretation von Konzepten

Brooks [21] zeigt, dass Experten oft den Kontext interpretieren oder Konzepte mit ihren eigenen Erfahrungen vermischen, um zu einer Schlussfolgerung über die Beziehungen zwischen Konzepten zu gelangen. Daher ist nicht immer klar, welche Aussagen über Konzepte tatsächlich auf Definitionen (von Rahmenwerken) beruhen und welche eine (erfahrungsbasierte) Annahme des Experten sind. Zumindest die ISO hat ein klares System von Querverweisen eingeführt, um auf Begriffe mit eindeutigen Bezeichnern zu referenzieren. Andere Rahmenwerke heben nicht einmal die Begriffe hervor, die in der Definition anderer Begriffe verwendet werden. Das macht es schwierig, die Zusammenhänge zwischen den Begriffen zu verstehen und daraus die Begriffsbeziehungen abzuleiten. In diesem Abschnitt werden die Beziehungen der zuvor identifizierten Schlüsselbegriffe untersucht, um die Struktur der ISRM-Schlüsselbegriffsterminologie aufzuzeigen, die sie bilden.

Konzeptbeziehungen

Konzept-diagramme

In der Regel müssen die Beziehungen zwischen den Konzepten durch Interpretation der Begriffsdefinitionen ermittelt werden, ähnlich wie in den vorherigen Abschnitten. So wurde beispielsweise in Abschnitt 5.4.1 das Risikokonzept untersucht und ähnliche Konzeptbeziehungen festgestellt. Ein Vergleich der fünf Konzeptdiagramme (Abbildung 5.1) zeigte deutlich, dass ein *Risiko* hauptsächlich mit den beiden Konzepten *Eintrittswahrschein-*

lichkeit und *Auswirkung* zusammenhängt. Auch Luko [201] nutzt Konzeptdiagramme zur einfachen Visualisierung von Begriffsbeziehungen, welche einen Gesamtüberblick über die Struktur einer Terminologie geben. Dieser Ansatz scheint daher angemessen, um ein Konzeptdiagramm für alle identifizieren Schlüsselkonzepte zu erstellen.

Visualisierung mit UML

Zur Erstellung des Schlüsselkonzeptdiagramms wurden alle Begriffe aus Tabelle 5.1 verwendet. Wie beim Risikokonzeptdiagramm wurden die durch Begriffsdefinitionen dargestellten Konzepte analysiert und die Konzeptbeziehungen entsprechend abgeleitet. Zur Visualisierung des Konzeptdiagramms wurde eine Notation auf Basis der Unified Modeling Language (UML)[3] gewählt. Brownsword und Setchi [215] verwenden ebenfalls die UML, um ihre RM-Ontologie darzustellen. Ebenso werden im *Shared Information Data* Information Framework [216] auch UML-Klassendiagramme genutzt, um die Beziehungen zwischen Geschäftseinheiten zu visualisieren. Somit scheint es eine geeignete Wahl für die Modellierung von Konzeptbeziehungen zu sein.

Auswahl der Begriffe

Da in den Rahmenwerken unterschiedliche Begriffe für dasselbe Konzept verwendet werden, war es notwendig, einen Begriff für das Diagramm auszuwählen. Daher wurde der am häufigsten verwendete Begriff als repräsentativ für das Konzept verwendet. Wenn es keine Mehrheit gibt, weil alle Rahmenwerke einen anderen Begriff verwenden, wurde der Begriff aus der ISO verwendet. Die im Diagramm verwendeten Begriffe sind in Tabelle 5.1 fett hervorgehoben.

Fehlende Struktur

Es ist anzumerken, dass OpenFAIR das einzige Dokument [122] enthält, welches zumindest die High-Level-Struktur der Konzepte grafisch darstellt. Das tabellarische Format macht es einfach, die erstellten Konzeptdiagramme in eine Framework-spezifische Version umzuwandeln. Eine nützliche Ontologie für RM auf der Grundlage von ISO Guide 73 und AS/NZS 4360 wurde ebenfalls von Brownsword und Setchi [215] erstellt, allerdings mit einem anderen Umfang als in dieser Abbildung.

Konzeptdiagramm

Abbildung 5.2 zeigt das erstellte Konzeptdiagramm. Ähnlich wie beim Vergleich der Terminologie wurden die Konzepte so dargestellt und miteinander verbunden, wie sie in den Rahmenwerken definiert wurden. Das Ergebnis ist ein kohärentes und zusammenhängendes Modell, das die Schlüsselkonzepte des ISRM gemäß den Rahmenwerken in dieser Analyse grafisch darstellt.

Berücksichtigung DC

Um die drei Level zu visualisieren, wurde der DC wie in Tabelle 5.1 farblich kodiert. Es ist zu erkennen, dass beginnend mit der obersten Kategorie *vollständig abgedeckt* (DC5) jedes DC ein in sich geschlossenes konzeptionelles Modell bildet. Diese Eigenschaft wird beibehalten, wenn es auf die Kategorie *teilweise abgedeckt* (DC4) erweitert wird, die lediglich zusätzliche Konzepte hinzufügt und abgeschlossene Konzeptbeziehungen herstellt. Dies unterstützt die Annahme, dass diese Konzepte tatsächlich wesentliche Elemente im ISRM-Bereich sind. Andernfalls wäre zu erwarten, dass es einige verwaiste Konzepte gibt, die nicht eng gekoppelt sind. Es kann davon ausgegangen werden, dass weitere Konzepte,

[3] Spezifikation zur grafischen Darstellung von Objektbeziehungen, `https://www.omg.org/spec/UML`

wie in DC3 gesehen, das ISRM-Modell nur verfeinern, aber nicht verändern. Folglich muss die DC5-Terminologie grundlegend sein und stellt ein minimal praktikables Modell des ISRM dar.

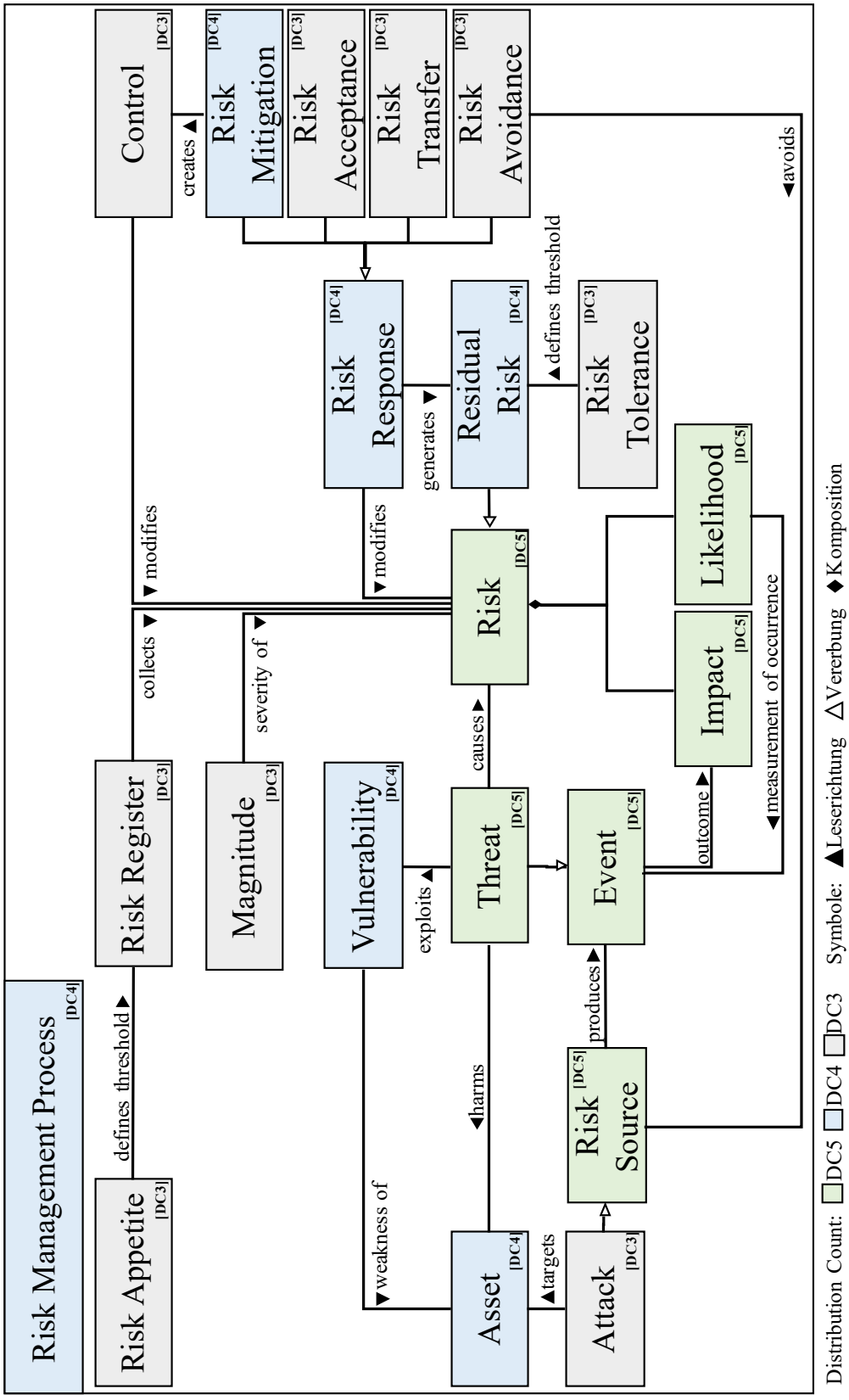
Unzureichende Konzeptbeziehungen

Aufgrund der oft unzureichenden oder nur oberflächlich angedeuteten Begriffsbeziehungen hat sich die Erstellung dieses Konzeptdiagramms als schwierig erwiesen. Insbesondere die ISO-Normen definieren die Begriffsbeziehungen nur unzureichend, obwohl das Rahmenwerk im Übrigen gut strukturiert ist. So gibt die ISO beispielsweise ein *Event* als „occurrence or change of a particular set of circumstances“ [49] an, d.h. sie definiert keine Assoziation. Auf der einen Seite definiert die ISO 27005 die Wahrscheinlichkeit als „chance of something happening“ [98]. Auf der anderen Seite fügt Guide 73 die *Häufigkeit* als „number of events or outcomes per defined unit of time“ [67] hinzu. Beide Begriffe scheinen das gleiche Konzept zu definieren, um die *Eintrittswahrscheinlichkeit* anhand eines numerischen Wertes zu beschreiben, und wurden daher in Tabelle 5.1 zusammengefasst, aber nur eine Definition fügt einen klaren Bezug zu einem *Event* hinzu. Die Überlegung, dass „etwas“ in diesem Zusammenhang auch ein *Event* bedeuten könnte, ist eine fundierte Vermutung, aber für sich genommen schwer zu beweisen. Ähnliche Effekte können auch für die anderen Rahmenwerke beobachtet werden. Es scheint, dass die Begriffsbeziehungen schwach definiert bleiben und sich eher aus dem Verwendungskontext als aus der Semantik der Begriffe ergeben.

Diskrepanz zur Praxis

Dies ist überraschend, da das Verständnis der Beziehungen zwischen Begriffen und Konzepten in der Praxis oft einheitlich dargestellt wird. In der Branche ist es allgemein bekannt, dass Risiken aus Bedrohungen bestehen, die auf eine Schwachstelle eines Assets einwirken. Tatsächlich lässt sich diese Beziehung aus den Aktivitäten ableiten, die im Inhalt der ISRM-Rahmenwerke beschrieben werden, aber sie ist nicht ausdrücklich als Teil der Terminologie definiert. Auch hier stellt sich die Frage, ob diese Unterschiede von den Praktikern tatsächlich wahrgenommen, interpretiert und angewendet werden. Im Hinblick auf akademische Zwecke würde ein gut definiertes Informationsmodell es ermöglichen, die semantischen Assoziationen des ISRM klar zu definieren.

Abbildung 5.2: Allgemeines ISRM Konzeptdiagramm



5.5 Ergebnisse des Terminologievergleichs

Ergebnis

In diesem Kapitel wurde eine einheitliche Terminologie basierend auf den Begriffen und Konzepten der meistgenutzten ISRM-Rahmenwerke abgeleitet. Dabei wurden keine neuen Begriffe oder Konzepte definiert, sondern lediglich die existierenden aufeinander abgebildet und harmonisiert. Das Ergebnis stellt die Grundlage für jegliche Art der organisationsübergreifenden Zusammenarbeit im Bereich ISRM dar. Die Analyse hat gezeigt, dass die Frameworks zum Teil unterschiedliche Begriffe definieren oder die gleichen Begriffe unterschiedlich verwenden. Eine Zusammenarbeit kann nur gelingen, wenn alle Teilnehmer dieselbe Sprache sprechen. Die Ergebnisse dieses Kapitel helfen Organisationen dabei, genau das zu tun.

Teilfragen

Diese Erkenntnisse bietet Forschern und Praktikern im Bereich ISRM einen aktuellen Überblick über allgemein anerkannte Begriffe sowie bekannte Konzepte und deren Verwendung in verschiedenen Frameworks. Sie ermöglichen damit eine gezielte Nutzung der Begriffe und der ihnen innewohnenden Konzepte durch Experten. Mit Hilfe von Tabelle 5.1 können Begriffe aus verschiedenen Frameworks problemlos übersetzt werden. Darüber hinaus erleichtert es die Übersetzung bestimmter spezifischer Begriffe und deren Anwendung in anderen Bereichen. So können Leitlinien, Bücher, wissenschaftliche Artikel und andere Unterlagen, die sich auf eine bestimmte Norm beziehen, leicht an ein anderes Umfeld angepasst werden. Dabei wurden im Kontext des Kapitels die folgenden Fragen beantwortet:

- Was ist eine Terminologie, ein Begriff und ein Konzept (Abschnitt 5.1)?
- Welche anderen Veröffentlichungen beschäftigen sich mit RM/ISRM-Terminologie (Abschnitt 5.2)?
- Welche Rahmenwerke definieren eine ISRM-Terminologie und wie (Abschnitt 5.2)?
- Wie lauten diese Begriffe und welcher Rahmen verwendet welchen Begriff (Abschnitt 5.3)?
- Wie wird der Begriff des Risikos eigentlich definiert (Abschnitt 5.4)?
- Wie interagieren diese Begriffe im Kontext des ISRM (Abschnitt 5.4)?

Nutzung

Abbildung 5.2 zeigt, dass es möglich ist, ein vernünftiges, generisches Konzeptdiagramm zu erstellen, indem man nur ISRM-Schlüsselkonzepte und definierte Konzeptbeziehungen berücksichtigt. Da das Diagramm im Wesentlichen Framework-unabhängig ist und die Begriffe mit Hilfe von Tabelle 5.1 auf andere Rahmenwerke übertragbar sind, kann es als allgemeines Werkzeug in verschiedenen Organisationen und Sektoren verwendet werden. Das Konzeptdiagramm zeigt, dass die ISRM-Schlüsselterminologie in der Tat sehr klein ist. Nur sechs Begriffe bilden die grundlegende Terminologie (DC5), die von allen betrachteten Rahmenwerken geteilt wird. Auch hier wäre es interessant, eine Expertenevaluierung durchzuführen, um zu prüfen, ob Experten aus der Praxis diese Auffassung von der RM-Schlüsselterminologie teilen. Forscher können sich in ihrer akademischen Arbeit auf das Konzeptdiagramm beziehen, wenn sie beabsichtigen, allgemeine Begriffe zu verwenden oder

auf bestimmte Konzepte Bezug nehmen müssen. Schließlich hilft das Konzeptdiagramm in Kombination mit der Begriffstabelle sowohl Wissenschaftlern als auch Praxisexperten die Terminologie des ISRM besser zu verstehen und anzuwenden.

Limitierungen

Obwohl im Ergebnis ein übergreifendes Diagramm angestrebt wurde, stellt das erstellte Konzeptdiagramm letztlich nur eine Vereinfachung der Konzeptstruktur dar. Es handelt sich im Grunde um eine Aggregation von Konzepten und damit auch der Darstellung der aggregierten Konzeptbeziehungen. Damit stellt es die bestmögliche Annäherung an ein generisches Konzeptdiagramm dar, aber unterscheidet sich im Ergebnis von einer frameworkspezifischen Version. Wenn ein Konzeptdiagramm für einen bestimmtes Framework erforderlich ist, muss es nur auf der Grundlage seiner eigenen Terminologie erstellt werden. Die identifizierten Konzepte unterscheiden sich nicht nur durch den verwendeten Begriff, wie im Abschnitt 5.3 erläutert, sondern vor allem durch die Art und Weise, wie ihre Beziehungen definiert sind. Jedes Framework stellt etwas andere Verbindungen her, was zu einer anderen Verkettung von Begriffen führen kann.

Offene Fragen

Das abgeleitete Konzeptdiagramm hilft zwar bereits als einfaches Instrument beim Verständnis von ISRM Begriffen und Zusammenhängen, es kann jedoch keine Aussage darüber getroffen werden, inwieweit diese Unterschiede in der Praxis überhaupt relevant sind. Anhand der vorgestellten Kernterminologie kann in zukünftigen Arbeiten überprüft werden, ob die in den Normen definierten Begriffe mit den wahrgenommenen Konzepten der Experten übereinstimmen. In diesem Fall kann das vorgestellte Konzeptdiagramm die Grundlage für eine Evaluierung bilden, beispielsweise nach der von Brooks [21] benutzen Methodik. Dazu müssten die Experten ihre eigene ISRM-Terminologie und Schlüsselkonzepte beschreiben, die dann mit dem vorgestellten Konzeptmodell verglichen werden. Der Vergleich mit dem erstellten Konzeptdiagramm konnte bestimmte Annahmen nicht verifizieren, aber einen Hinweis auf den Reifegrad der ISRM-Konzepte geben. Ein hoher Reifegrad würde bedeuten, dass die Konzepte relativ stabil sind und gut verstanden werden, während ein niedriger Reifegrad ein Indikator für ein lebendiges Feld ist, in dem sich selbst grundlegende Konzepte ständig ändern. Der Vergleich könnte einen Einblick in die Überschneidung zwischen Terminologietheorie und -praxis geben, was ein Indikator für die Reife von ISRM-Konzepten ist. Letzteres würde bedeuten, dass die meisten Experten einen anderen Blick auf die Zusammenhänge haben und die Kategorien unterschiedlich interpretieren, d.h. der Wandel führt zu einer kontinuierlichen Weiterentwicklung der Disziplin. Diese durchaus interessanten Folgefragestellungen liegen jedoch außerhalb des Fokus dieser Arbeit.

Ausblick

Im Folgenden wird vielmehr auf der erstellen Terminologie aufgebaut, welche selbst die zweite Komponente des kollaborativen Frameworks darstellt. Sie liefert Begriffe, die problemlos aufeinander abgebildet werden können, Schlüsselkonzepte, die von allen Framework unterstützt werden und ein einheitliches Risikoverständnis. Das ermöglicht die grundlegende Kommunikation zwischen den Partnern im Kontext des ISRM (CSF 4). Die einheitliche Terminologie bildet auch die Grundlage für die Konzeption eines adaptiven Prozesses. Dieser muss nicht nur die generischen ISRM Aktivitäten unterstützen, sondern insbesondere die Schlüsselkonzepte einbinden. Durch die Extraktion aus den untersuchten Frameworks ist sichergestellt, dass diese in den darauf basierenden Prozessen etabliert wurden.

Kapitel 6

Konzeption eines kollaborativen Prozesses

Inhaltsangabe

Ziel

Im letzten Kapitel wurden die Konzepte des ISRM untersucht und Begriffe aus verschiedenen Quellen verglichen. Es konnte eine Liste von Kernbegriffen, eine Übersicht über die Schlüsselkonzepte und eine Darstellung der Konzeptbeziehungen erstellt werden. Gemeinsam bilden diese Ergebnisse die erste von drei Komponenten des kollaborativen Frameworks. Nachdem damit eine einheitliche ISRM Terminologie definiert wurde, welche die Grundlage für die Kommunikation zwischen den Partnerorganisationen bildet, soll nun ein kollaborativer Prozess entworfen werden. Dieser Prozess bildet die zweite Komponente des kollaborativen Frameworks.

Vorgehen

Dabei erfolgt die Ableitung der Aktivitäten des ISRM gemäß dem in Abbildung 3.1 bereits vorgestellten Konzept. Im ersten Schritt wird dazu ein allgemeines Prozessmodell modelliert, um eine einheitliche Basis für die Kollaboration zu schaffen. Wie auch die Terminologie muss der Prozess möglichst generisch sein, um in der Praxis kompatibel mit verschiedenen Ausprägungen des ISRM zu sein. Wie zuvor kann nicht davon ausgegangen werden, dass die Partner den gleichen Prozess bzw. ein vergleichbares Vorgehen implementiert haben. Um auch hier ein praxisorientiertes Modell zu erstellen, werden die vorgestellten Frameworks (Kapitel 2.3) erneut untersucht, jedoch diesmal mit Blick auf ihre Aktivitäten. Wie auch bei der Terminologie sollen gemeinsame Aktivitäten identifiziert werden, welche dann die Grundlage für einen generischen Prozess liefern können.

Prozessmodell

Im ersten Schritt werden dazu alle Aktivitäten der Frameworks untersucht und zusammengefasst (Abschnitt 6.1). Durch einen Strukturvergleich der Prozesse sollen ähnliche Aktivitäten identifiziert und von diesen ein übergreifendes Prozessmodell abgeleitete werden. Anschließend wird dieses Modell mit den identifizierten Konzepten aus der im vorherigen Abschnitt (5.4.2) erstellten vereinheitlichten Terminologie kombiniert. Daraus ergibt sich ein vollständiges Modell für einen generischen Prozess, welcher kompatibel zu organisationsspezifischen Prozessen ist, unabhängig vom etablierten Framework.

Kollaborative Aktivitäten

In einem zweiten Schritt werden die Aktivitäten des generischen Prozesses im Hinblick auf ihre enthaltenen Aufgaben betrachtet (Abschnitt 6.2). Dabei wird untersucht, welche Aktivitäten bzw. Teilaktivitäten sich für einen kollaborativen Ansatz eignen und welche Erweiterungen/Schnittstellen dazu notwendig wären. Es geht letztlich um die Frage, welche Aspekte des ISRM innerhalb der Allianz sinnvoll gemeinsam durchgeführt werden können. Dabei lässt sich unterscheiden, ob eine Aktivität bzw. Aufgaben individuell, gemeinsam oder hybrid ausgeführt werden können. Letztlich sollen so die kollaborativen Aufgaben identifiziert werden, welche in der Allianz gemeinsam zu bewältigen sind.

Verantwortlichkeiten

Im letzten Schritt geht es darum festzulegen, wie die Partner potenzielle Aufgaben gemeinsam durchführen können (Abschnitt 6.3). Für alle Aktivitäten gilt es zu definieren, welche Kommunikationswege zur Kollaboration genutzt werden sollen und wer dafür verantwortlich ist. Dazu sind Rollen und Funktionen in der Allianz zu etablieren bzw. es müssen existierenden Funktionen zusätzlichen Aufgaben zugewiesen werden. Dabei sollen den Organisationen möglichst keine zusätzlichen Befugnisse übertragen werden, da die Zusammenarbeit in der Allianz auf Basis einer vertrauensvollen Kollaboration erfolgen soll. Trotzdem gilt es den Austausch von Risikoinformationen und das Treffen von gemeinsamen Entscheidungen zu koordinieren. Das finale Ergebnis ist das um Rollen und Verantwortlichkeiten erweiterte, generische Prozessmodell.

6.1 Ableitung eines generischen Prozessmodells

Neben der einheitlichen Terminologie ist ein wichtiger Aspekt für die Zusammenarbeit im ISRM ein gemeinsames Verständnis über die Vorgehensweise. Insbesondere da davon ausgegangen wird, dass die verschiedenen Organisationen innerhalb einer Allianz bereits einen ISRM-Prozess etabliert haben (siehe Kapitel 3.3), ist ein kompatibles Vorgehen notwendig. Nur wenn die Abläufe in den Organisationen miteinander vergleichbar sind, können diese innerhalb der Allianz koordiniert und aufeinander abgestimmt durchgeführt werden. Alle Partner müssen letztlich in der Lage sein, das eigene Vorgehen miteinander zu synchronisieren, um gemeinsame Aktivitäten zu organisieren. Um das zu ermöglichen wird also ein minimaler Kernprozess benötigt, der die grundlegenden Aktivitäten des ISRM enthält und auf die organisationsspezifischen Prozesse abgebildet werden kann. Dadurch wird eine Allianz in die Lage versetzt zentral zu definieren, an welchen Stellen im Prozess eine Kollaboration angestrebt wird. Die Partner können dann selbständig die erforderlichen Vorkehrungen in ihren eigenen Prozessen treffen und notwendige Schnittstellen aktivieren. Es stellt sich die Frage, wie ein solcher Kernprozess aufgebaut sein sollte. In Kapitel 2.2.3 wurde bereits ein generischer ISRM Prozess basierend auf Shameli-Sendi et al. [73] vorgestellt. Dieser umfasst die vier Aktivitäten *Risikokontext festlegen, Risiken einschätzen, Risiken behandeln und Risiken überwachen*, welche in Abbildung 2.6 dargestellt wurden. Es ist davon auszugehen, dass diese Aktivitäten tatsächlich essenziell für das ISRM sind. Allerdings ist nicht klar, ob diese nur eine Teilmenge darstellen und wie der Bezug zur aktuellen Praxis aussieht. Diese Verknüpfung ist jedoch wesentlich für die Abbildung der organisationsspezifischen Prozesse. Aus diesem Grund sollen die Aktivitäten direkt aus den Industrie-Frameworks abgeleitet und anschließend mit dem generischen Prozess verglichen werden. Es ist zu erwarten, dass der Prozess erweitert, aber nicht reduziert werden kann.

Synchronisierte Abläufe

Generischer Prozess

6.1.1 Analyse der Framework-Prozesse

Wie auch beim Terminologievergleich wird für den Prozessvergleich erneut eine Auswahl der bekannten ISRM Frameworks aus Kapitel 2.3 herangezogen. Dabei wurden jedoch einzelne Frameworks ausgetauscht. Während FAIR zwar eine Terminologie definiert hat, enthält das Framework lediglich ein Vorgehen für die Risikoeinschätzung, jedoch nicht für das komplette ISRM. Daher wird es in dieser Analyse nicht betrachtet. Stattdessen definieren COBIT und IT-Grundschutz, welche nicht für die Terminologie herangezogen wurden, einen Prozess, der ebenfalls untersucht wird.

Nachfolgend sind alle Aktivitäten für die betrachteten Frameworks aufgelistet und erklärt. Dabei wurde versucht, die Prozesse auf einem ähnlichen Level zu betrachten und Implementierungsdetails zu abstrahieren. Die Herausforderung ist, dass die Frameworks einen unterschiedlichen Umfang besitzen und auch die Definition der Prozessschritte im Detailgrad stark variiert. Beispielsweise kann die Beschreibung einer Aktivität im NIST RMF etwa über 10 Seiten lang sein, während die gleiche Aktivität in ISACA RiskIT nur auf einer Seite zusammengefasst wurde. Es hat sich jedoch herausgestellt, dass die Aktivitäten strukturell sehr ähnlich und gut vergleichbar sind, wenn konkrete Anleitungen und Hin-

Prozessaktivitäten

weise zur Umsetzung, welche für das Vorgehensmodell keine Rolle spielen, vernachlässigt werden. Auf diesem Niveau lässt sich damit eine sinnvolle Analyse und darauf aufbauend ein Strukturvergleich durchführen.

Prozessanalyse I: MoR

Der Prozess im *Management of Risk: Guidance for Practitioners* [127] nennt insgesamt sieben verschiedene Aktivitäten. Eine vorbereitende Aktivität, vier sequentielle Aktivitäten im Kontext der Risikoeinschätzung und zwei parallele unterstützende Aktivitäten.

Grundlagen Zu Beginn des Prozesses werden die Grundlagen etabliert, die für die korrekte Durchführung notwendig sind. Diese Aktivität ergibt sich zum einen aus dem Aspekt *Management of Risk Principles*, welches den gesamten Prozess umschließt. Bereits beim Etablieren der Prinzipien werden relevante Vorbereitungen getroffen, um die Prozessiteration sinnvoll durchführen zu können, z.B. das Definieren von Zielen oder die Identifikation von Stakeholdern. Zum anderen geht die Aktivität allerdings fließend in den nächsten Schritt *Identifizieren* über, welche auch Aspekte des Kontexts definiert.

Identifizieren Die Aktivität ist zweigeteilt in das Identifizieren des Kontexts und der Risiken, wodurch sie sowohl Teil der Vorbereitung als auch der Risikoeinschätzung ist. Im ersten Schritt werden relevante Rahmenbedingungen für die folgenden Prozessschritte festgelegt. Dazu gehören etwa Anwendungsbereich und Ziele der Iteration, Eingaben von Stakeholdern und das geplante Vorgehen. Das Ergebnis sind Informationen über das Vorgehen, ein RM-Plan, eine Übersicht aktueller Stakeholder sowie neue Erkenntnisse. Diese werden im nächsten Schritt zum Identifizieren neuer Risiken genutzt. Dazu sind für die Organisation relevante Bedrohungen zu untersuchen und betreffende Risiken im Risiko Register zu dokumentieren.

Einschätzen Auch das Einschätzen ist in die zwei Schritte Bewerten und Beurteilen geteilt. Im ersten Schritt werden die im vorbereiteten Risiko Register dokumentierten Risiken genauer untersucht und bewertet. Dazu wird Eintrittswahrscheinlichkeit, Auswirkung und Nähe (wie zeitnah tritt das Risiko ein) der Risiken eingeschätzt. Ergebnis dieses Teils ist ein aktualisiertes und um Metadaten erweitertes Risiko Register, welches eine Priorisierung der Risiken erlaubt. Anschließend wird der tatsächliche Effekt der Risiken beurteilt, indem die bewerteten Risiken auf ein vorbereitetes Risikomodell abgebildet werden. Dabei spielt wiederum das Risikoprofil der Organisation eine Rolle, d.h. Risikoappetit und -toleranz.

Planen Basierend auf dem priorisierten Risiko Register kann ein Aktionsplan erstellt werden, um Risiken zu reduzieren oder zu entfernen. Dabei ist zu dokumentieren, ob und wie auf ein Risiko reagiert werden soll und wer dafür verantwortlich wäre. Ergebnis dieser Aktivität ist ein aktualisiertes Risiko Register und ein vollständiger Behandlungsplan, der dem Management vorgelegt werden kann.

Umsetzen Nach Freigabe folgt die Implementierung der im Behandlungsplan definierten Aktionen. Es ist sicherzustellen, dass die Aktionen von den verantwortlichen Personen wie geplant durchgeführt werden und sich das Ergebnis als Wirksam erweist. Ein Teil dieser Aktivität ist das Erstellen eines kontinuierlichen Berichts über den Zustand der Risikobehandlung in der Organisation. Dazu gehört die Prüfung der Effektivität umgesetzter Maßnahmen, sowie deren kontinuierliche Überwachung. Insbesondere nicht effektive Aktionen sind zu identifizieren, kommunizieren und erneut zu betrachten.

Kommunizieren Während dem gesamten Prozessablauf ist eine kontinuierliche Kommunikation mit relevanten Stakeholdern zu gewährleisten. Bereits bei der Identifikation von Risiken sind aktuelle und verlässliche Informationen notwendig, um akute Bedrohungen zu erkennen (in anderen Bereichen oftmals als Threat Intelligence bezeichnet). Bei der Umsetzung des Prozesses ist die Teilnahme aller Personen in der Organisation essenziell und somit auch die Kommunikation mit diesen. Dazu gehören insbesondere die Mitarbeiter (allgemeines Verständnis), das Management (Informationen über den aktuellen Stand) und der Einkauf (Verbindlichkeiten und Verträge). Das Ergebnis dieser Aktivität ist eine Organisation, die in ihrer Gesamtheit über jeden Schritt des RM informiert ist.

Einbinden und überprüfen Eine weitere übergreifende Aktivität behandelt die Integration des Prozesses in die Organisation. Ähnlich zur Kommunikation steht auch hier die Information und Awareness aller Teilnehmer im Mittelpunkt. Jede Aktivität muss in alle Teilbereiche der Organisation integriert werden, um einen angemessenen Prozess zu etablieren. Ziel dieser Aktivität ist ein gemeinsames Risikobewusstsein auf allen Ebenen.

Prozessanalyse II: NIST

Das NIST RMF [103] definiert ebenfalls sieben Aktivitäten, welche alle sequenziell durchgeführt werden. Wie bereits erwähnt betrachtet NIST das ISRM auf Systemebene, daher wird der Prozess für jedes System individuell gestartet. Alle Aktivitäten sind wiederum in einzelne Aufgaben aufgeteilt, die erledigt werden müssen.

Vorbereiten Im ersten Schritt werden die notwendigen Parameter und Vorbedingungen zur weiteren Durchführung des Prozesses definiert. Mit insgesamt 18 Aufgaben ist diese Aktivität sehr umfangreich ausgestaltet, wobei zwischen Geschäfts- und Systemebene unterschieden wird. Dabei werden essenzielle Rahmenbedingungen wie Rollen, Strategie, Ziele und Assessments etabliert, welche in nachfolgenden Prozessschritten genutzt werden. Eine Besonderheit im Vergleich zu anderen Frameworks ist, dass die Identifikation von Assets und Bedrohungen sowie die gesamte Risikoanalyse und Bewertung bereits Teil dieser Aktivität sind. Damit positioniert sich die Vorbereitungsphase zwischen dem Etablieren von Grundlagen und der Risikoeinschätzung. Auch Ergebnisse aus der vorherigen Iteration des Prozesses werden aggregiert und als Eingabewert an die Folgeaktivitäten weitergereicht.

Kategorisieren Basierend auf den bereits in der Vorbereitung durchgeführten Bewertungen wird nun das System kategorisiert. Im ersten Schritt erfolgt eine Analyse seiner Eigenschaften, wobei existierende Sicherheitsmaßnahmen, das Service Design und Supply Chain Abhängigkeiten zu berücksichtigen sind. Auf Basis dieser Information kann das System anschließend in eine von der Organisation definierten Sicherheitskategorien eingestuft werden. Dazu wird eine BIA durchgeführt, um die Auswirkung von CIA Risiken auf die Organisation zu bewerten. Letztlich muss die gewählte Kategorie freigegeben werden, um eine konsistente Einstufung innerhalb der Organisation sicherzustellen.

Auswählen Die gewählte Sicherheitskategorie liefert die Grundlage für die Auswahl angemessener Maßnahmen. Für jede mögliche Kategorie muss bereits in der Vorbereitungsphase eine Liste an Maßnahmen erstellt werden (Baseline). Anschließend können die Maßnahmen auf Basis der Ergebnisse der Risikoeinschätzung angepasst werden, um angemessen für die spezifischen Bedrohungen zu sein. Die gewählten Maßnahmen und Anpassungen sind anschließend zu dokumentieren und die geeignete Umsetzung zu planen. Dabei ist bereits zu berücksichtigen, wie die Maßnahmen später überwacht werden können. Die Aktivität endet mit der formalen Freigabe der Planung.

Implementieren Nach Freigabe des Maßnahmenplans müssen diese in der Organisation umgesetzt werden. Bereits während der Umsetzung ist der Zustand und die Wirksamkeit der Maßnahmen kontinuierlich zu bewerten und zu überwachen. Abweichungen von der ursprünglichen Planung müssen dokumentiert und in den entsprechenden Dokumenten angepasst werden.

Bewerten Nach Fertigstellung der Implementierung folgt eine Wirksamkeitsprüfung der Maßnahmen. Dabei ist unabhängig zu bewerten, ob die Maßnahmen wie geplant implementiert wurden und ob diese den erwarteten Nutzen erbringen. Die Ergebnisse sind in einem Bericht zu dokumentieren, welcher notwendige Änderungen enthalten kann. Änderungen, die aufgrund der Wirksamkeitsprüfung durchgeführt werden, müssen in den Plänen dokumentiert werden.

Autorisieren Die gesamten Ergebnisse der Risikobehandlung müssen anschließend an das Management kommuniziert werden. Der Bericht der Umsetzung wird zusammen mit den Behandlungsplänen an die für die Freigabe verantwortliche Person übergeben. Diese ist für die Prüfung der Ergebnisse zuständig. Dazu gehört nicht nur die Wirksamkeit der Implementierung, sondern auch Konformität mit der Risikostrategie der Organisation. Die Entscheidung über Freigabe oder Ablehnung der Behandlung sowie wichtige Informationen werden an relevante Stakeholder kommuniziert.

Überwachen Ziel der Überwachung ist die kontinuierliche Überprüfung des Systems und der Systemumgebung. Neue Bedrohungen sind zu identifizieren und die Wirksamkeit der existierenden Maßnahmen regelmäßig zu evaluieren. Die Ergebnisse der Überwachung sind zu dokumentieren, Veränderungen zu planen und notwendige Anpassungen anzustoßen.

Prozessanalyse III: BSI

Die Risikoanalyse auf Basis von IT-Grundschutz [101] kommt mit lediglich vier Aktivitäten aus. Dabei ist zu berücksichtigen, dass das ISRM in den größeren Rahmen des IT-Grundschutzes eingebunden ist, wodurch viele Grundlagen bereits implizit etabliert wurden. Daher werden die unter dem Abschnitt *Vorarbeiten* zusammengefassten Aufgaben als zusätzliche Aktivität gelistet. Gleichermaßen geht die Aktivität *Konsolidierung* fließend in den Sicherheitsprozess über, was im Prozessschritt berücksichtigt werden muss.

Vorarbeiten Die Vorbereitungsphase setzt die Rahmenbedingungen für die Durchführung des Prozesses. Diese sollten bereits durch Etablieren des Sicherheitsprozesses vorhanden sein. Dazu gehört die Identifikation und Einstufung von Assets, eine Schutzbedarfsfeststellung (BIA) und die Definition der Methode. Risikoakzeptanzkriterien werden auf Basis der im IT-Grundschutz gewählten *Absicherung* festgelegt, welche letztlich auf Risikoappetit und Risikotoleranz der Organisation zurückzuführen sind.

Gefährdungsübersicht erstellen Es folgt ein erster Schritt zur Risikoeinschätzung, die Erstellung einer Gefährdungsübersicht. Gefährdungen bezeichnen dabei grundsätzlich Szenarien, die für die *Zielobjekte* relevant sind. Zielobjekte sind dabei die Assets, die in der Schutzbedarfsfeststellung als wichtig eingestuft wurden. Bei der Analyse wird zwischen elementaren und zusätzlichen Gefährdungen unterschieden. Erstere sind generisch und können aus einer Liste ausgewählt, letztere müssen organisationsspezifisch identifiziert werden.

Risikoeinstufung Anschließend erfolgt der zweite Teil der Risikoeinschätzung, die Einstufung der ausgewählten Gefährdungen. Dazu folgt eine Berechnung des Risikos auf Basis von Eintrittshäufigkeit und Schaden des Szenarios, welche sowohl quantitativ als auch qualitativ durchgeführt werden kann. Bei der anschließenden Risikobewertung wird das Risiko einer zuvor definierten Risikokategorie zugeordnet, welche letztlich die Risikohöhe widerspiegelt.

Behandeln von Risiken Mit den Ergebnissen der Risikobewertung kann eine angemessene Risikobehandlung ausgewählt werden. Es kommen die üblichen Behandlungsoptionen (vermeiden, reduzieren, transferieren und akzeptieren) zum Einsatz. Die Behandlung muss Anforderungen des Sicherheitskonzeptes berücksichtigen und dort auch entsprechend dokumentiert werden. Die oberste Leitung muss anschließend die vorgeschlagene Behandlungsoption freigeben und das verbleibende Restrisiko akzeptieren. Ein weiter Teil der

Risikobehandlung ist die kontinuierliche Überwachung der Risiken, um auf zukünftige Änderungen reagieren zu können. Ergebnisse der Beobachtung müssen dokumentiert und bei der nächsten Iteration in der Risikoeinstufung berücksichtigt werden.

Konsolidierung (inkl. Rückführung) Die letzte Aktivität besteht je nach Aufteilung aus ein bis zwei Prozessschritten, wenn die Integration in den Sicherheitsprozess berücksichtigt wird. Bei der Konsolidierung werden die Ergebnisse der Risikoanalyse in das im Sicherheitsprozess erstellte Sicherheitskonzept aufgenommen. Dabei ist zu bewerten, ob alle Maßnahmen sinnvoll zusammenwirken und die neu geplanten Maßnahmen das Sicherheitskonzept sinnvoll ergänzen. Ist das Sicherheitskonzept angemessen, kann dieses bereinigt und formal fertiggestellt werden. Es folgt die Rückführung, welche die Fortsetzung des Sicherheitsprozesses beschreibt. Als Teil dessen werden die geplanten Maßnahmen als Teil dies Prozesses umgesetzt und die Informationssicherheit überprüft. Weiterhin ist das regelmäßige Berichten an die Leitung und relevante Stakeholder durch geeignete Kommunikationskanäle ein Teil dieser Aktivität.

Prozessanalyse IV: ISO

Der Standard ISO/IEC 27005 [98] definiert einen Prozess bestehend aus sechs klar abgegrenzten Aktivitäten. Diese sind aufgeteilt in eine Aktivität zur Vorbereitung, fünf Aktivitäten im Kontext der Risikoeinschätzung und zwei parallele Aktivitäten, die den Prozess unterstützen.

Kontext etablieren In der ersten Aktivität wird der Kontext des Prozesses etabliert, beginnend mit dem Festlegen der Ziele des ISRM. Basierend auf den Zielen wird eine passende Methode definiert die geeignete Einstufungs- und Akzeptanzkriterien enthält. Weiterhin wird der Anwendungsbereich und die Grenzen des ISRM festgelegt, um die betrachteten Assets zu identifizieren. Letztlich müssen die Verantwortlichkeiten für alle Schritte im Prozess definiert werden.

Risikoeinschätzung Die Risikoeinschätzung enthält die drei Aufgaben Identifikation, Analyse und Evaluation. Im ersten Schritt werden die Assets der Organisation, potenzielle Bedrohungen, Schwachstellen und bereits existierende Maßnahmen identifiziert und dokumentiert. All diese Entitäten werden anschließend in der (qualitativen oder quantitativen) Analyse genutzt, um Eintrittswahrscheinlichkeit, Auswirkung und Risikohöhe zu berechnen. Auf Basis der vorher festgelegten Kriterien kann das Risiko nun bewertet und priorisiert werden, um das weitere Vorgehen zu planen.

Risikobehandlung Für die eingeschätzten Risiken kann nun eine Behandlungsoption (modifizieren, erhalten, vermeiden, teilen) ausgewählt werden. Es können beliebig viele Optionen ausgewählt werden, mit dem Ziel, das Restrisiko an die Akzeptanzkriterien anzupassen. Gewählte Maßnahmen müssen priorisiert und geplant werden.

Risikoakzeptanz Die gewählte Option und das verbleibende Restrisiko wird im Risikobehandlungsplan dokumentiert. Dieser wird den verantwortlichen Managern zur Prüfung vorgelegt. Geplante Maßnahmen und Risiken, die nicht die Risikoakzeptanzkriterien erfüllen, müssen explizit freigegeben werden. Es folgt faktisch die Umsetzung der geplanten Maßnahmen, welche jedoch formal nicht Teil des Prozesses ist, ähnlich wie bei Sicherheitsprozess des IT-Grundschutzes. Die ISO/IEC 27005 orientiert sich am Plan-Do-Check-Act Zyklus, wobei der definierte ISRM Prozess nur die Plan-Phase abbildet und die Implementierung streng genommen zur Do-Phase gehört, welche im übergreifenden ISMS abgebildet wird.

Risiken kommunizieren und Beratung Es müssen effektive Kommunikationswege mit relevanten Stakeholdern etabliert werden. Interessierte Parteien sollten über alle Veränderungen und Ergebnisse des RM Prozesses informiert werden. Diese können wiederum wichtige und für die Entscheidung über die Risikobehandlung relevante Informationen liefern. Durch das kontinuierliche Sammeln von Risikoinformationen und Einbinden der Stakeholder wird der Prozess verbessert und die Awareness bei den Beteiligten erhöht.

Risiken überwachen und überprüfen Alle bereits identifizierten Risiken müssen kontinuierlich überwacht werden. Neue Rahmenbedingungen, Veränderungen an Assets oder der Organisation, können die Bedrohungslage verändern. Auf der einen Seite liefern alle anderen ausgeführten Aktivitäten Eingaben aus dem inneren der Organisation. Auf der anderen Seite identifiziert die Aktivität selbst geänderte Rahmenbedingungen außerhalb der Organisation, z.B. rechtliche Vorgaben, welche an die Prozesse geliefert werden.

Prozessanalyse V: RiskIT

Der RiskIT ISRM Workflow [119] definiert fünf Aktivitäten. Diese sind im Framework selbst sequentiell dargestellt, jedoch wird bereits darauf hingewiesen, dass das keine Notwendigkeit ist. Organisationen können den Workflow als Vorlage verwenden, sollen ihn jedoch an die eigenen Bedürfnisse anpassen. Tatsächlich ist das Vorgehen im Framework auch nicht als aufeinander folgende Aktivitäten, sondern als lose Sammlung von Aufgaben beschrieben.

Kontext etablieren Im ersten Prozessschritt wird der Kontext des ISRM mit Hinblick auf die Ziele, Strategie und die Mission der Organisation definiert. Dazu gehört das Festlegen des Anwendungsbereiches der vom Prozess betroffenen Geschäftsbereiche. Weiterhin sind Kriterien zu definieren, um identifizierte Risiken einzuordnen und eine Entscheidung zu treffen, d.h. festlegen des Risikoappetits und der Risikotoleranz der Organisation.

Risikoidentifikation und Einschätzung Im ersten Prozessschritt der Risikoeinschätzung wird die Identifikation der Bedrohungen und Szenarien durchgeführt. Neue Risiken

sollen identifiziert werden, indem Bedrohungen mit potenziellen Auswirkungen auf die Geschäftsziele der Organisation betrachtet werden. Darauf aufbauend gilt es konkrete I&T Szenarien zu entwickeln, welche ein Risiko für die Organisation darstellen. Dabei schreibt das Framework kein Asset basiertes Vorgehen vor (Bottom-up Ansatz), sondern erlaubt auch ein Erstellen von Szenarien ausgehend von den Geschäftszielen (Top-down Ansatz).

Risikoanalyse und BIA Evaluation Um die Risikoeinschätzung abzuschließen, werden in der anschließenden Analyse für jedes Szenario die Frequenz und das Ausmaß der Bedrohung geschätzt. Die bewerteten Szenarien bilden die Basis für die Evaluation der Risiken. Dazu müssen die Szenarien ausgewertet und auf konkrete Geschäftsrisiken abgebildet werden, um den Schaden für die Organisation zu bestimmen, d.h. es folgt praktisch eine BIA.

Risikoreaktion Auf die eingeschätzten Risiken muss die Organisation eine angemessene Reaktion finden. Es gilt zu priorisieren, in welcher Reihenfolge die Risiken behandelt werden sollen, abhängig von den für die Organisation relevanten Einflussfaktoren. Bei der Auswahl einer Reaktion sind sowohl klassische Behandlungsmethoden möglich (vermeiden, reduzieren, teilen, transferieren oder akzeptieren) als auch das Vorgehen der Risikoaggregation. Dabei werden mehrere Risiken zusammengefasst, um ein integriertes Risikoprofil zu erhalten. Das aggregierte Risiko kann im Kontext des ERM gemeinsam mit anderen Risiken behandelt werden, falls die Organisation ein ERM etabliert hat. Die Entscheidungen werden im Aktionsplan dokumentiert und anschließend umgesetzt. Auch bei RiskIT zählt die Umsetzung der Behandlungsoption formal nicht mehr als Teil des Prozesses.

Risiken berichten und kommunizieren Entscheidungsträger und andere Stakeholder sollen zeitnah über Ergebnisse im Prozess informiert werden, insbesondere um aktiv Einfluss auf die weiteren Aktivitäten nehmen zu können. Weiterhin soll eine allgemeine Awareness in der Organisation geschaffen werden, die durch konsequente Kommunikation der Risikostrategie die Erwartungshaltung aller Beteiligten formt. Durch eine transparente Kommunikation der aktuellen Risiken und Reaktionen soll ein allgemeines Verständnis gefördert werden. Key Risk Indicators (KRIs) können als Metrik helfen, um über das Risikoprofil der Organisation zu berichten.

Prozessanalyse VI: COBIT

Das Framework COBIT [112] definiert mit neun die höchste Anzahl an Aktivitäten, welche auf zwei die zwei Teilbereiche Management und Durchführung aufgeteilt sind. Durch die Gliederung in die beiden Module *EDM03 Ensured Risk Optimisation* und *AP012 Managed Risk* mit jeweils unterschiedlichen Aufgaben unterscheidet sich die Struktur auf den ersten Blick stärker von den bereits analysierten Frameworks. Bei näherer Betrachtung zeigt sich allerdings, dass der Aufbau der einzelnen Prozessschritte doch sehr ähnlich zu den Anderen ist.

RM evaluieren (EDM03) Diese Aktivität kann als Vorbereitungsphase angesehen werden, wobei der Kontext der Organisation festgelegt wird. Dazu sind als erstes Risikoappetit und Risikotoleranz festzulegen. Dabei ist zu beachten, dass das Verhältnis zum ERM klar definiert und der Risikoappetit im ISRM nicht über dem Appetit der Organisation liegt. Letztlich müssen Rahmenbedingungen wie relevante Risikofaktoren, Rollen und Verantwortlichkeiten festgelegt werden.

RM steuern (EDM03) Es ist sicherzustellen, dass das ISRM in die operativen Prozesse der Organisation eingebunden wird. Dazu gehört das Erstellen eines Kommunikationsplans für die gesamte Organisation. Dieser muss angemessene Kommunikationswege definieren, um mit Verantwortlichen und relevanten Stakeholdern in Kontakt zu treten und diese über Risiken und Maßnahmen zu informieren. Es sind zeitnah Berichte über alle Risikoaktivitäten zu erstellen und an Entscheidungsträger weiterzuleiten.

RM überwachen (EDM03) Risiken oder Probleme im Umgang mit Risiken müssen an die verantwortlichen Personen berichtet werden. Dazu sind die Aktionen im ISRM kontinuierlich zu überwachen und entsprechende Metriken zu definieren. Stakeholder müssen in der Lage sein, den aktuellen Stand der Risikobehandlung und Status der Organisation einschätzen zu können.

Daten sammeln (AP012) In der ersten Aktivität des Moduls geht es um das Festlegen der Vorgehensweise und dem Sammeln von Risikoinformationen. Damit ergibt sich eine zweite Vorbereitungsphase, bei der zuerst eine Methode für das ISRM festgelegt wird. Weiterhin geht es um die Definition von Kategorien für die Einstufung von Risiken sowie internen und externen Faktoren zur Einstufung dieser. Zusätzlich enthält die Aktivität allerdings auch erste Teile der Risikoeinschätzung, bei der Risikoinformationen gesammelt und Risikoereignisse identifiziert werden.

Risiken analysieren (AP012) Basierend auf den identifizierten Ereignissen werden Risikoszenarien erstellt. Anschließend werden Eintrittswahrscheinlichkeit und Auswirkung eingeschätzt, letztere auf Basis der Geschäftskritikalität von Assets. Für alle Risiken, die über Risikoappetit oder Toleranz hinausgehen, muss eine Behandlungsoption (vermeiden, reduzieren, teilen, transferieren, akzeptieren) gewählt werden. Anschließend müssen die Ergebnisse der Auswertung und die Wirksamkeit der geplanten Maßnahmen evaluiert werden.

Risikoprofil erstellen (AP012) Die vorher erfassten Assets, Risiken, Risikoinformationen und Behandlungspläne müssen zentral gesammelt und dokumentiert werden. Die Organisation muss regelmäßig überprüfen, ob die erfassten Informationen noch aktuell sind und das so erstellte Risikoprofil aktualisieren. Zur kontinuierlichen Überwachung der Risiken müssen KRI definiert werden, welchen zur Erkennung von Trends geeignet sind.

Risiken benennen (AP012) Entscheidungsträger und relevante Stakeholder sind über die Ergebnisse der Risikoanalyse zu informieren und mit ausreichend Informationen zu versorgen. Insbesondere das komplette Risikoprofil sollte regelmäßig an die Stakeholder berichtet werden. Das Feedback von Stakeholdern und zusätzliche Risikoeinschätzungen wird in das Risikoprofil aufgenommen.

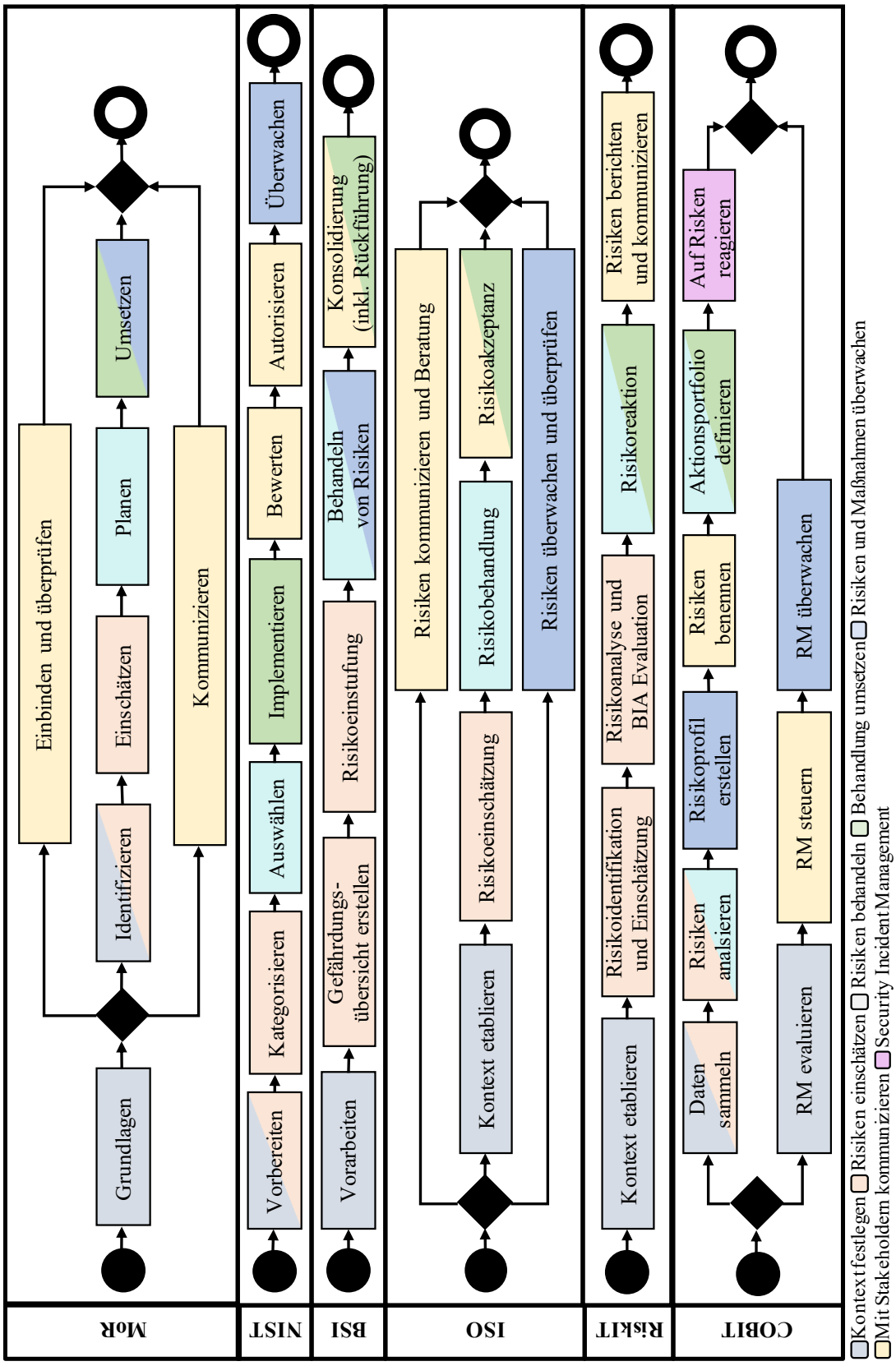
RM Aktionsportfolio definieren (AP012) In der Risikoanalyse beschlossene Maßnahmen sind im Maßnahmen-Inventar zu pflegen. Jede Organisationseinheit muss sicherstellen, dass die definierten Maßnahmen entsprechend umgesetzt werden. Alle Maßnahmen sind priorisiert als Projekt umzusetzen.

Auf Risiken reagieren (AP012) Diese Aktivität beschreibt den Umgang mit bereits eingetretenen Risiken, d.h. Sicherheitsvorfällen (Incidents). Vor Eintreten eines Vorfalls gilt es Prozeduren und Reaktionspläne zu definieren, die das Vorgehen im Ernstfall beschreiben. Dabei ist sicherzustellen, dass eine Kategorisierung und Bewertung von Incidents erfolgt. Für abgeschlossene Incidents muss die Ursache ermittelt, der Schaden bewertet und die Ergebnisse an Entscheidungsträger kommuniziert werden. Diese Aktivität ist eine Besonderheit in COBIT, da das Behandeln von Vorfällen üblicherweise als eigener ISM Prozess, dem Security Incident Management, gesehen wird.

6.1.2 Struktur der ISRM Prozesse

Aus der durchgeführten Analyse der einzelnen Prozesse lässt sich jeweils ein lineares Prozessmodell skizzieren. Die Struktur der Top-Level-Aktivitäten aus den Frameworks ist in Abbildung 6.1 dargestellt. Zur einheitlichen Darstellung wurde ein einfaches UML Aktivitätsdiagramm verwendet, welches jeweils die Hauptaktivitäten der Prozesse verknüpft.
Im direkten Vergleich ist zu erkennen, dass die verschiedenen Prozesse ähnlich strukturiert sind, auch wenn sich die Anzahl und Reihenfolge der Aktivitäten leicht unterscheidet. Eine Erklärung für diese Ähnlichkeit wäre, dass sich die meisten RM-Rahmenwerke an der ISO 31000 orientieren (Abbildung 2.4) und ihre grundlegende Struktur davon abgeleitet haben. Somit zeigt sich, dass die Frameworks zwar unterschiedliche Prozesse definieren, sich diese jedoch hauptsächlich in der Vorgehensweise (wie eine Aktivität durchgeführt wird) unterscheiden, jedoch nicht sonderlich im Ablauf (welche Aktivitäten durchgeführt werden). Somit lassen sich die Aktivitäten in den verschiedenen Prozessausprägungen klassifizieren, indem der Ablauf als Klassifikator herangezogen wird. Zur Erweiterung der visuellen Darstellung wurden nun alle Aktivitäten, welche vom Inhalt ähnlich sind, im Strukturvergleich gleichfarbig hervorgehoben. Es lässt sich erkennen, dass fast alle untersuchten Prozesse die gleichen sechs Aktivitätskategorien etablieren, wenngleich diese unterschiedlich aufgeteilt sind. Eine Ausnahme stellt lediglich die Aktivität *Auf Risiken reagieren* von COBIT dar. Diese wird allerdings im Folgenden nicht weiter betrachtet, da sie im ISM nicht Teil des ISRM, sondern des Security Incidents sein sollte.

Abbildung 6.1: Strukturvergleich der Aktivitäten in den Prozessen der ISRM Framework



Durch die Visualisierung wird die Ähnlichkeit der Prozessstrukturen noch einmal verdeutlicht. Oft genügt eine einfache Verschiebung der Sequenz nach links oder rechts, um die Darstellung eines anderen Frameworks zu erhalten. Ob ein Prozess als Reihenfolge von sequentiellen oder parallelen Aktivitäten dargestellt wird, hängt lediglich von der skizzierten Struktur im jeweiligen Framework ab. Letztlich spiegelt allerdings die Beschreibung der jeweiligen Prozessschritte wider, dass zumindest die Überwachung und Kommunikation von Risiken tatsächlich kontinuierliche Aktivitäten sind, welche während dem gesamten Prozessablauf durchgeführt werden müssen.

6.1.3 Ableitung eines generischen Prozesses

Generischer Prozess

Basierend auf dieser Klassifizierung kann nun ein mit allen Frameworks kompatibles, übergreifendes Prozessmodell erstellt werden. Der ursprünglich gezeigte, generische Prozess (Abbildung 2.6) definierte bisher lediglich vier Aktivitäten. Somit lassen sich nicht alle Kategorien direkt auf dieses Modell abbilden, sondern es sind zwei zusätzliche Prozessschritte notwendig. Da einige Frameworks jeweils zwischen Planung und Umsetzung der Risikobehandlung unterscheiden, sollte auch das Modell diese beiden separat darstellen. Diese Unterscheidung scheint insbesondere im ISRM sinnvoll zu sein, da Maßnahmen zur Verbesserung der IS die Geschäftsziele beeinträchtigen kann. Weiterhin sind Änderungen an Informationen sowie Technologie oft sehr komplex und können nicht immer zeitnah durchgeführt werden, anders als etwa Projektrisiken. Neben dieser Aufteilung kommt zusätzlich noch eine weitere Aktivität hinzu, die den Prozess unterstützen kann. Dabei handelt es sich um die Kommunikation mit internen und externen Stakeholdern, welche als wichtiger Steuerungsmechanismus explizit genannt werden sollte. Somit ergibt sich ein vereinheitlichter ISRM-Prozess aus insgesamt sechs Basisaktivitäten:

1. Kontext festlegen
2. Risiken einschätzen
3. Risiken behandeln
4. Behandlung umsetzen
5. Risiken und Maßnahmen überwachen
6. Mit Stakeholdern kommunizieren

Konzepte

Der abgeleitete Prozess kann nun mit den in Abschnitt 5.4.2 identifizierten Konzepten verknüpft werden, um das Prozessmodell zu vervollständigen. Die Konzepte sind essenzielle Entitäten, welche im Kontext des ISRM vorkommen sollten. Eingebunden in einen Prozess bedeutet das, dass sie einem direkten Zusammenhang mit den Aktivitäten stehen müssen. Um das zu nachzubilden, lassen sich die Konzepte in einem Prozessmodell als Inputs oder Outputs von Aktivitäten modellieren. Für einen wirksamen Prozess müssen mindestens alle Schlüsselaktivitäten integriert sein, da diese nicht weggelassen werden dürfen. Im Umkehrschluss bedeutet das, wenn die identifizierten Schlüsselkonzepte nicht sinnvoll in den Prozess eingebunden werden können, kann dieser nicht vollständig im Sinne eines allgemeingültigen Modells sein. Eine Darstellung des so entstandenen generischen Prozesses

bestehend aus den sechs Basisaktivitäten verknüpft mit den Konzepten ist in Abbildung 6.2 zu sehen. Nachdem Struktur und Farbgebung die Gleiche ist wie im vorherigen Strukturvergleich (Abbildung 6.1), ist ein einfacher Vergleich mit den jeweiligen Frameworks möglich.

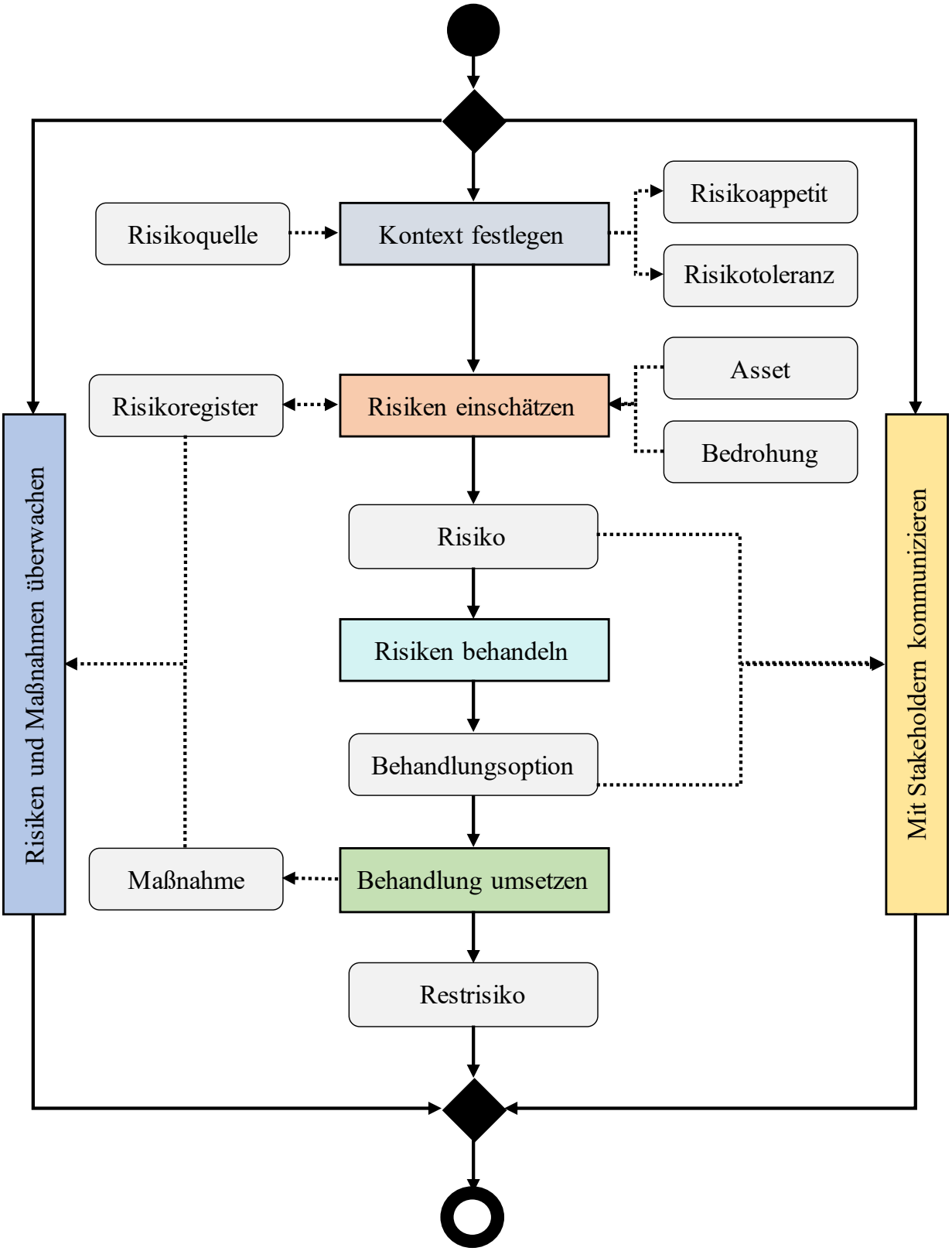
Einheitliche Frameworks

Im abgeleiteten ISRM-Prozess mit integrierten Konzepten konnten nicht nur die Schlüsselkonzepte, sondern alle im Konzeptdiagramm (Abbildung 5.2) erfassten Konzepte integriert werden. Nachdem diese beiden Entitäten lückenlos zusammengeführt werden konnten, ist das ein Beleg dafür, dass ein konsistentes Prozessmodell abgeleitet wurde. Die Zusammenführung von Aktivitäten und Konzepten ist insbesondere aufschlussreich, da bei deren Herleitung teilweise unterschiedliche Frameworks genutzt wurden. Wie vorher erläutert, definieren nur manche der Frameworks eine Terminologie und andere nur einen Prozess. Trotzdem scheinen die Frameworks einheitlich genug zu sein, um eine ähnliche ISRM Struktur zur erzeugen. Das ist eine wichtige Erkenntnis über die Interoperabilität der Frameworks, wie sie auch von der ENISA untersucht wurde [37, 38], da somit verschiedene Prozesse grundsätzlich kompatibel sein können. Dies kann die Zusammenarbeit verschiedener Organisationen im Bereich ISRM erleichtern und erlaubt die Erstellung übergreifender Managementkonzepte, die auf ähnlichen Annahmen aufbauen.

Externer Vergleich

An dieser Stelle lohnt sich ein kurzer Vergleich mit dem *Core Unified Risk Framework* von Wangen et al. [82], welches einen ähnlichen Ansatz mit anderem Anwendungsbereich gewählt hat. Das Framework dient der Bewertung der Vollständigkeit von Methoden zur IS-Risikoeinschätzung haben und enthält eine umfassende Liste aller dazugehörigen Aufgaben. Zur Erstellung wurden insgesamt 11 Frameworks untersucht, zu denen auch die hier betrachteten FAIR, NIST 800-30, RiskIT und ISO/IEC 27005 gehören. Das Framework inkludiert die hier genannten Aktivitäten *Risiken einschätzen* und *Risiken behandeln* in die Risikoeinschätzung. Zur Herleitung des Frameworks wurden die zu den Aktivitäten gehörenden Aufgaben aus allen untersuchten Frameworks identifiziert und tabellarisch verglichen. Auch wenn das Framework einen anderen Fokus und Detailgrad besitzt, so lassen sich Parallelen zum erstellten Modell erkennen. Es wird ebenfalls festgestellt, dass der Risikoeinschätzung ein Vorbereitungsschritt (Preliminary assessment) vorausgeht, in dem Rahmenbedingungen wie Scope, Kriterien, Ziele und Stakeholder definiert werden. Erst anschließend folgt die Identifikation von Assets, Schwachstellen, Bedrohungen, existierender Maßnahmen und resultierender Risiken. Die Inputs und Outputs der Aufgaben sind zwar detaillierter aufgeteilt, lassen sich jedoch grundsätzlich auf die in Abbildung 6.2 gezeigten Konzepte abbilden. Das Ergebnis der Risikoeinschätzung sind letztlich ebenfalls priorisierte Risiken mit Vorschlägen für die Risikobehandlung, was sich damit ebenfalls im Konzept *Risk Response* widerspiegelt. Somit lassen sich auch im Vergleich mit dem Core Unified Risk Framework keine Lücken im erstellten Prozessmodell identifizieren.

Abbildung 6.2: Abgeleiteter ISRM-Prozess mit integrierten Konzepten (Inputs/Outputs)



6.2 Identifikation kollaborativer Aufgaben

Das erstellte Prozessmodell (Abbildung 6.2) bildet nun die Ausgangslage für die weitere Untersuchung der Aktivitäten. Das Ziel des CISRM ist die koordinierte Ausführung des Prozesses innerhalb einer Allianz. Somit stellt sich die Frage, ob und welche (Teil-)Aktivitäten das Potenzial für die gemeinsame Durchführung besitzen. Gibt es solche, dann sind grundsätzlich zwei Möglichkeiten denkbar. Entweder, die Aktivität bzw. Teile davon sollten gemeinsam in der Allianz durchgeführt oder es sollten Schnittstellen zur Kommunikation bzw. zum Informationsaustausch etabliert werden, um die Aktivitäten zu synchronisieren. Es ist auch möglich, dass manche Aktivitäten nur innerhalb der Organisation (lokal) ausgeführt werden können bzw. nicht von einer kollaborativen Ausführung profitieren.

Perspektiven der Kollaboration

Bei der Kollaboration lassen sich die zwei Perspektiven einer verteilten und gemeinsamen Ausführung einer Aufgabe unterscheiden. Ein wechselseitiger Prozess kann etabliert werden, indem die Teilnehmer der Allianz unabhängig voneinander den ISRM Prozess durchführen und Kommunikationsschnittstellen in die Aktivitäten integrieren. Das ermöglicht die lose Verbindung mehrerer Prozesse, bei denen Risikoinformationen ausgetauscht und von den Partnern berücksichtigt werden. Zusätzlich besteht die Möglichkeit einer kollektiven Ausführung, bei der die Allianz einzelne Aufgaben gemeinsam bearbeitet. Beide Perspektiven sind relevant, um den größtmöglichen Mehrwert aus einem kollaborativen Prozess herauszuholen.

Kollaborativer Prozess

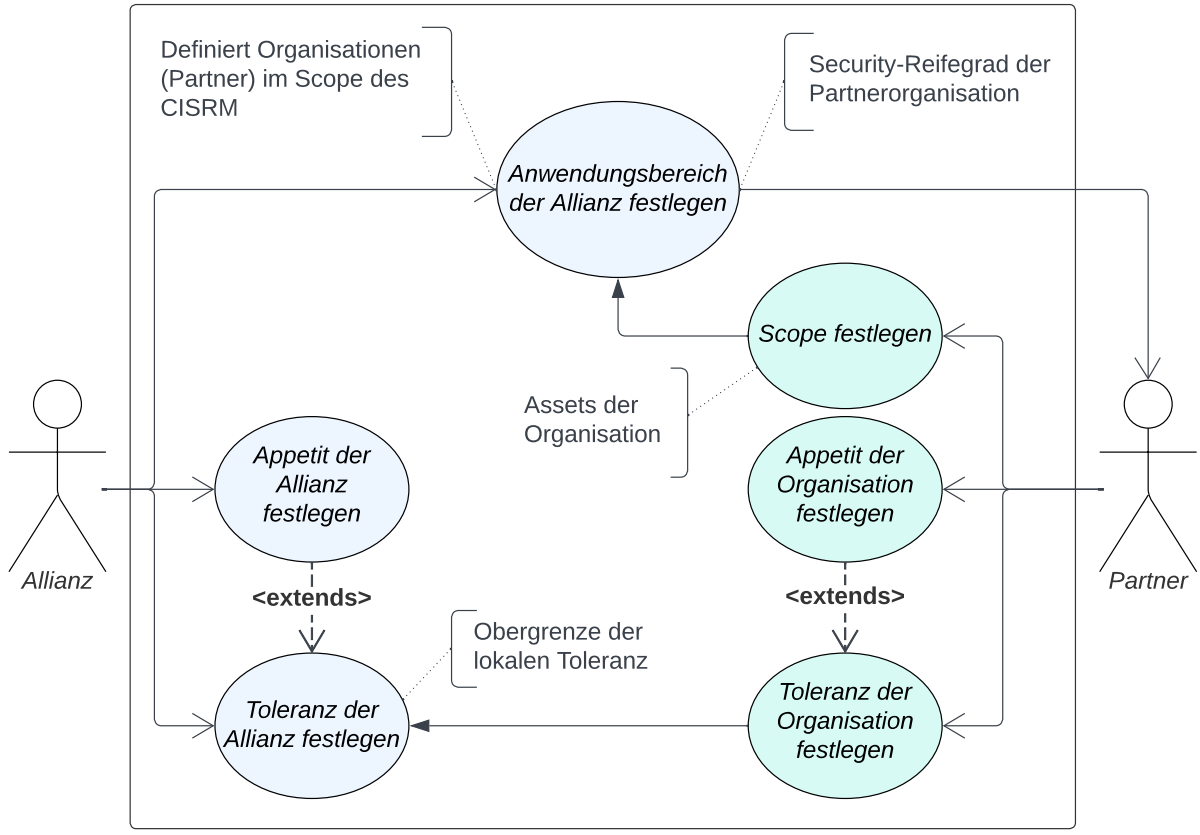
Es soll noch einmal betont werden, dass das angestrebte Konzept kein zentralisierter Prozess, sondern eine Verbindung verteilter Prozesse sein soll (CSF 5). Das Ziel ist es, die Prozesse miteinander zu verknüpfen, um einen Mehrwert für die teilnehmen Organisationen zu schaffen, der über das eigene ERM hinausgeht. Gleichzeitig sollen so wenig Abhängigkeiten wie möglich etabliert werden, damit die Organisationen maximal unabhängig voneinander agieren können. Trotzdem bleibt eine Zentralisierung und Standardisierung einzelner Aspekte auch in diesem Modell unvermeidbar.

Im Folgenden wird diskutiert, welche der sechs Aktivitäten ganz oder teilweise kooperativ ausgeführt werden könnten und an welchen Stellen Schnittstellen sinnvoll wären.

6.2.1 Aktivität 1: Kontext festlegen

Der Prozessschritt zum Festlegen der Rahmenbedingungen des Prozesses umfasst verschiedene Aufgaben, die maßgeblichen Einfluss darauf haben, wie die Allianz das gemeinsame Vorgehen aufbaut. Neben der Eingrenzung des Scopes als essenziellen Teil der Vorbereitung enthält die Aktivität drei Konzepte *Risikoquelle*, *Risikoappetit* und *Risikotoleranz*, die zu betrachten sind. Im ISRM ist das Ergebnis dieser Aktivität ein definierter Anwendungsbereich, d.h. es ist festgelegt welche Teile der Organisation im Prozess zu betrachten sind, sowie ein klares Eingeständnis der für die Organisation vertretbaren Risikohöhe. Die Erweiterung zum CISRM sollte im Kern die gleichen Themen erfordern, jedoch mit Blick auf die gesamte Allianz einzelne Aspekte vereinheitlichen. Abbildung 6.3 zeigt eine Übersicht der relevanten Aufgaben dieser Aktivität, welche im Folgenden diskutiert werden.

Abbildung 6.3: Verteilung der Aufgaben in der Aktivität *Kontext festlegen*



Scope Der erste wichtige Schritt ist das Festlegen des **Anwendungsbereichs** des ISRM. Da jede Organisation selbst entscheiden muss, welche Teilbereiche relevant sind, muss dies von jeder Organisation selbständig durchgeführt werden. Grundsätzlich ist davon auszugehen, dass jeder Partner über ein Business und damit relevante Assets verfügt, die für die anderen wichtig sind, da dies eine Voraussetzung für die Partnerschaft ist. Die Allianz sollte allerdings einschränken, ob ein Partner am gemeinsamen ISRM teilnimmt oder nicht. Dabei sollte insbesondere der Security-Reifegrad der Organisationen berücksichtigt werden. Ist der Level bzw. das Sicherheitsniveau der Organisationen im Anwendungsbereich zu unterschiedlich, dann werden die Teilnehmer nur einen geringen Mehrwert durch den Austausch von Risikoinformationen bzw. das gemeinsame Behandeln von Risiken erhalten (CSF 4). Eine Allianz sollte dies unbedingt am Anfang ihrer gemeinsamen Initiative berücksichtigen, um einen erfolgreichen CISRM Prozess zu etablieren.

Appetit Bei der Festlegung von **Risikoappetit und -toleranz** wird es komplizierter. Während die Risikotoleranz die maximale Risikohöhe eines einzelnen Risikos festlegt, trifft der Risikoappetit eine Aussage über die tolerierbare Summe der Restrisiken in der gesamten Organisation. Offensichtlich hängen diese Werte von der Unternehmensstrategie und wirtschaftlichen Stellung ab, weshalb sie sich von Organisation zu Organisation unterscheiden können. Gleichzeitig spielen die Werte eine maßgebliche Rolle für das gemeinsame ISRM.

Das Ziel des kollaborativen ISRM muss es sein, den Risikoappetit innerhalb der Allianz auf ein angemessenes Niveau zu senken. Dieser Wert muss für die gesamte Allianz festgelegt werden. Dabei spielt es allerdings keine Rolle, ob die einzelnen Partnerorganisationen intern mit einem niedrigeren oder höheren Appetit arbeiten.

Toleranz

Anders sieht es bei der **Risikotoleranz** aus, welche sowohl für die einzelne Organisation als auch für die Abstimmung in der Allianz relevant ist. So sollte die Allianz als Ganzes eine Toleranz festlegen, um nicht akzeptierbare Risiken gemeinsam zu behandeln. Diese muss auch gleichzeitig von den Organisationen übernommen und als lokaler Wert verwendet werden. Sie kann dann als Schwellwert fungieren, um zu beurteilen, welche Risiken an die Allianz weitergereicht werden sollten. Trotzdem besteht für die einzelne Organisation die Möglichkeit, eine lokale Risikotoleranz zu definieren, die unterhalb derer von der Allianz liegt, um Risiken früher zu behandeln. Die Wahl eines höheren Wertes ist in diesem Modell jedoch nicht vorgesehen, da die Kommunikation von Risiken ansonsten nicht koordiniert werden kann. Entsteht eine große Differenz zwischen den akzeptierbaren Risiken der Partner, dann ist eine abgestimmte Reaktion auf kritische Risiken schwer möglich.

Schlussfolgerung 1: Kontext festlegen

Die Allianz muss die Organisationen im Anwendungsbereich so auswählen, dass eine Kollaboration im CISRM für alle Teilnehmer sinnvoll erscheint. Die Partner müssen Risikoappetit und Risikotoleranz aufeinander abstimmen, indem innerhalb der Allianz eine Obergrenze festgelegt wird.

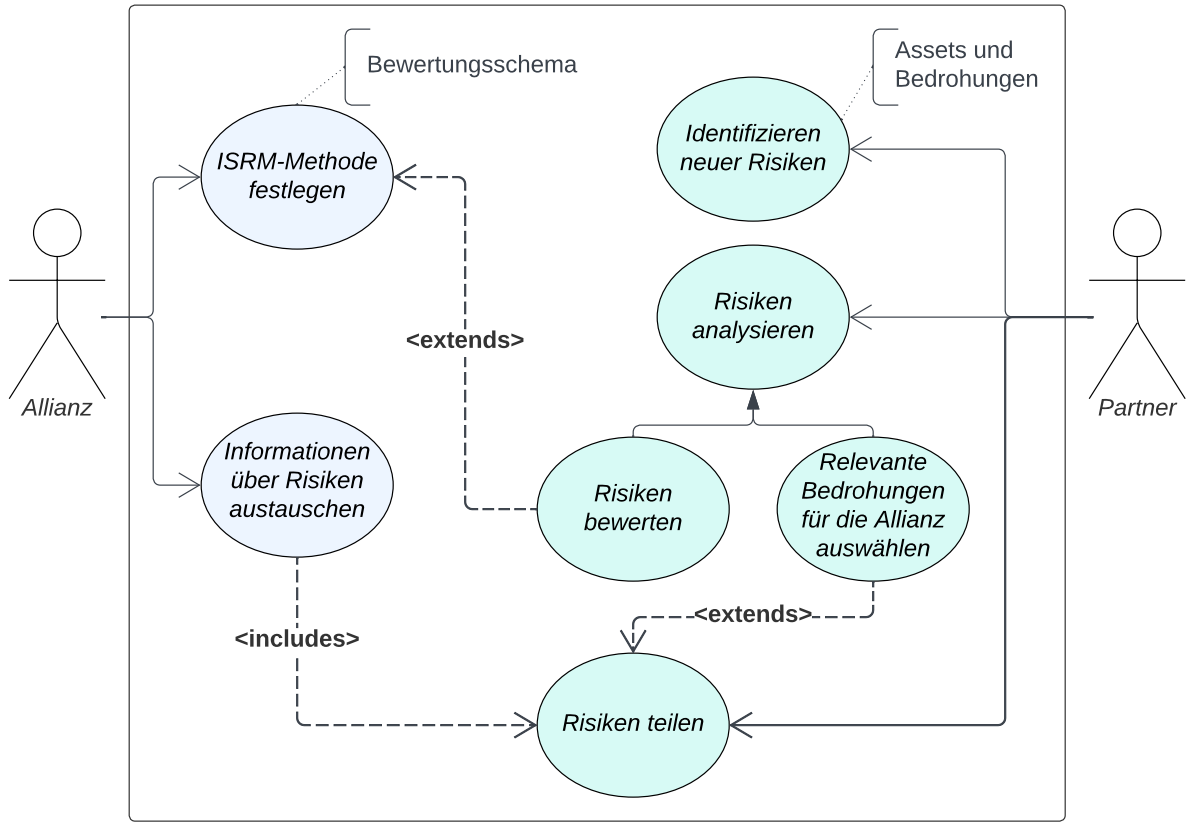
6.2.2 Aktivität 2: Risiken einschätzen

Im zweiten Prozessschritt werden Risiken identifiziert, analysiert und bewertet. Die relevanten Konzepte sind dabei *Asset*, *Bedrohung* und *Risikoregister*. Das Ergebnis dieser Aktivität im ISRM sind eine Liste (neu) bewerteter Risiken im Register der Organisation, welche im Anschluss behandelt werden können. Auf das CISRM übertragen sollte das Ergebnis eine Liste von, innerhalb der Allianz, vergleichbaren Risiken sein, die zwischen den Partnern ausgetauscht werden. Das führt dazu, dass am Ende alle Partner über die aktuelle Risikosituation innerhalb der Allianz informiert sind. Diese Informationen über Risiken können wiederum im lokalen ERM genutzt werden (Bedrohungsmodellierung). Abbildung 6.4 zeigt eine Übersicht der relevanten Aufgaben dieser Aktivität, welche im Folgenden diskutiert werden.

Identifizieren

Das **Identifizieren neuer Risiken** ist eine lokale Aktivität, die jede Organisation im Kontext des eigenen ERM durchführen muss. Dabei werden **Risiken** ermittelt, welche die eigene, nicht jedoch andere Organisationen betreffen. Abgesehen von SCRs erscheint es dabei nicht sinnvoll, die Risiken anderer Organisationen direkt zu betrachten. Es ist allerdings vorstellbar, auch solche Risiken zu identifizieren, welche die Allianz als Ganzes betreffen. Das heißt, Risiken können relevant sein, wenn sie die Allianz selbst gefährden oder mehrere Teilnehmer vom gleichen Risiko betroffen sind. Beides setzt voraus, dass die

Abbildung 6.4: Verteilung der Aufgaben in der Aktivität *Risiken einschätzen*



Risiken, die eine Organisation A identifiziert, vergleichbar mit denen sind, die eine Organisation B identifiziert. Die Problematik dabei ist, dass die Risiken von zwei oder mehr Organisationen nicht einfach aufeinander abgebildet werden können, da die zugrunde liegenden Szenarien bereits unterschiedlich sind. Es ist jedoch denkbar, die Rahmenbedingen der Risikoidentifikation so anzupassen, dass jede Organisation mit ähnlichen Parametern arbeitet. Die Eingaben **Assets** und **Bedrohungen** können dabei eine essenzielle Rolle einnehmen. Werden diese innerhalb der Allianz synchronisiert, dann ermöglicht das die Vergleichbarkeit der Ergebnisse. Eine Organisation wird dadurch nicht in der Ausführung der Aufgabe beeinflusst und kann weiterhin ihr eigenes Verfahren nutzen. Gleichzeitig können die Organisationen ihre Risiken leicht aufeinander abbilden und sicherstellen, dass nur für die Allianz relevante Risiken betrachtet werden.

Analysieren

Nachdem Risiken identifiziert wurden, gilt es diese zu einzuschätzen. Dazu ist eine zwischen den Partnern abgestimmte **Methode** unabdingbar. Es muss klar sein, wann ein Risiko für die Allianz relevant ist, damit dieses entsprechend kommuniziert wird. Damit das Ergebnis der Analyse überhaupt vergleichbar sein kann, müssen zumindest die grundlegenden Parameter für die Erstellung eines Risikos festgelegt sein. So wäre ein Risiko basierend auf Erwartungswerten und eines basierend auf Unsicherheit nicht direkt miteinander vergleich-

bar, da sie zwei unterschiedliche Konzeptbeziehungen beschreiben. Nachdem die Definition eines Risikos basierend auf der Berechnung von Eintrittswahrscheinlichkeit und Auswirkung im ISRM allerdings aktuell fest etabliert scheint, wie in Kapitel 5.4.1 beschrieben, stellt sich diese Problematik nicht. Es kann somit davon ausgegangen werden, dass alle Partner diese Definition bereits verwenden und problemlos verwenden können. Trotzdem könnte jedoch jede Organisation ein eigenes Schema zur Einstufung der Risiken verwenden.

Bewerten

Abgesehen von der formalen Definition ist die Berechnung der Werte und die resultierende Bewertung genauso relevant. Verschiedene ISRM Prozesse nutzen unterschiedliche Methoden. Es fängt an bei der Auswahl einer qualitativen oder quantitativen Bewertungsmethode. Wie in Kapitel 2.1 beschrieben, nutzen die meisten Frameworks, Industriestandards und somit auch Organisationen aktuell einen qualitativen Ansatz. Es ist allerdings nicht abzusehen, ob sich dieser Trend in Zukunft ändern wird. Doch selbst wenn zwei Organisationen die gleiche Bewertungsmethode nutzen, können diese trotzdem unterschiedlich ausgestaltet sein. Eine qualitative Bewertung kann etwa die Stufen *normal, hoch, sehr hoch* oder auch *gering, mittel, außergewöhnlich, extrem*. Eine quantitative Bewertung könnte stattdessen etwa auf monetären Werten basieren, die für zwei Organisationen komplett unterschiedlich sein können. Auch hier gilt, dass es keine zentrale Vorgabe der Methode durch die Allianz geben soll (CSF 5). Jede Organisationen soll weiterhin ihre bereits etablierte Methodik nutzen können, welche wahrscheinlich am besten zum jeweiligen Business und zur Unternehmenskultur passt. Somit muss eine Methode definieren werden, die es den Partnern erlaubt, ihre Ergebnisse zu vergleichen. Die Bewertung wird damit weiterhin lokal durchgeführt und anschließend auf das Bewertungsschema der Allianz abgebildet (etwa mit Hilfe der in Kapitel 7.4 vorgestellten Methode).

Informationen teilen

Es gilt weiterhin eine Kommunikationsschnittstelle zu definieren, damit die relevanten Risikoinformationen letztlich auch ausgetauscht werden können. Die Kommunikation ist bereits ein wichtiger Bestandteil dieser Aktivität und sollte nicht erst bei der Behandlung der Risiken erfolgen, obwohl sie dafür letztlich notwendig ist. Bis zu diesem Punkt erfolgte die Identifikation und Analyse der Risiken noch vollkommen autonom durch die Partner, analog zum klassischen ISRM. Da sich die Allianz zuvor auf eine gemeinsame Methode geeinigt hat, sind die Risiken der verschiedenen Organisationen jetzt jedoch miteinander vergleichbar. Ein erster Mehrwert kann somit generiert werden, indem die Partner über relevante Risiken in den Organisationen informiert werden, um über die aktuelle Risikosituation innerhalb der Allianz auf dem laufenden zu bleiben. Die Partner können diese Risiken wiederum für die eigene Risikoeinschätzung nutzen, da essenzielle Risiken anderer Organisationen in der Allianz wahrscheinlich auch für diese selbst relevant sind (CSF 1). Diese Annahme ist damit begründet, dass alle Partner einer ähnlichen Risikosituation ausgesetzt sind, da sich eine Allianz immer aufgrund einer Nähe der Organisation formt (siehe Kapitel 4.2). Wäre das nicht der Fall, würde ein Teilen von Risikoinformationen innerhalb der Allianz eher wenig Mehrwert liefern, da die bewerteten Risiken keine lokale Relevanz aufweisen. Da jedoch von einer Nähe als Voraussetzung ausgegangen wird, kann auch die Allianz als Ganzes die aggregierten Informationen nutzen, um ein aktuelles Bedrohungsmodell zu erstellen und an die Partner zu verteilen. Dadurch stehen den Teilnehmern deutlich mehr Informationen zur Risikoeinschätzung zur Verfügung, als wenn sie alleine Tätig wer-

den würden. Somit liefert die Kommunikation im Rahmen des CISRM an dieser Stelle bereits einen taktischen Mehrwert für die Organisationen im Anwendungsbereich.

Schlussfolgerung 2: Risiken einschätzen

Die Allianz muss sich auf Vorlagen für vergleichbare Assets, Bedrohungen und eine gemeinsame Methode zur Risikobewertung einigen. Die Ergebnisse der lokalen Risikoeinschätzung sollen zwischen den Partnern geteilt und von der Allianz als Grundlage für ein gemeinsames Bedrohungsmodell genutzt werden.

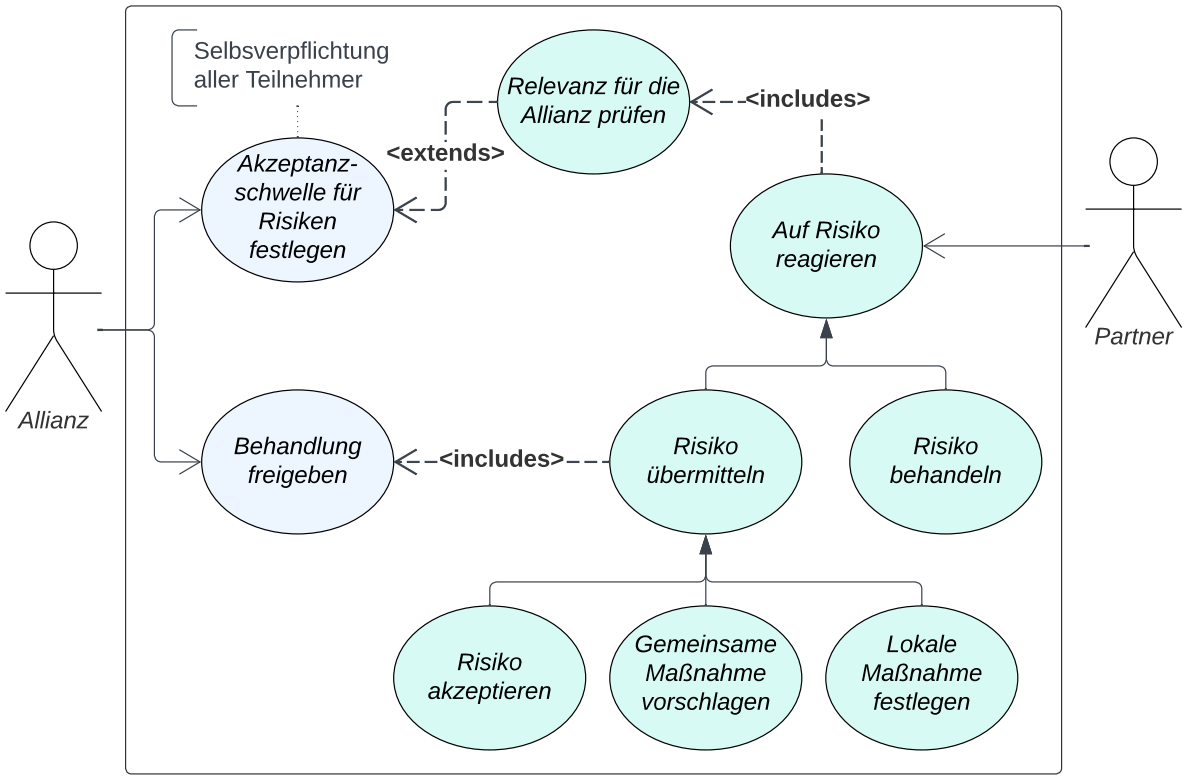
6.2.3 Aktivität 3: Risiken behandeln

Die Entscheidung über eine angemessene Risikobehandlungsoption und die Priorisierung von Maßnahmen ist sowohl für die einzelne Organisation als auch die Allianz relevant. Im klassischen ISRM soll auf Basis der durchgeführten Bewertung eine für die Organisation sinnvolle Reaktion ausgewählt werden. Ergeben sich dabei neue Maßnahmen, können die Verantwortlichen diese direkt genehmigen und veranlassen. Ebenso ist ein Akzeptieren durch die Owner problemlos möglich. Die Grundidee dieser Aktivität bleibt auch im CISRM erhalten, hier kommt jedoch besonders der Aspekt der organisationsübergreifenden Zusammenarbeit zu tragen. Dabei soll über die Risikobehandlung von für die Allianz relevante Risiken von allen Teilnehmern gemeinsam entschieden werden. Das schafft einen ersten Gegensatz zum Vorgehen als Teil des ERM innerhalb der Organisation, auch wenn die Ziele, das Risikoniveau zu verringern, weiterhin übereinstimmen. Neben dem reinen Austausch von Risikoinformationen ist ein weiteres Ziel des CISRM ein abgestimmtes Vorgehen über die Reaktion auf Risiken innerhalb der Allianz, um ein uniformes Sicherheitsniveau über alle Partner hinweg zu gewährleisten. Abbildung 6.5 zeigt eine Übersicht der relevanten Aufgaben dieser Aktivität, welche im Folgenden diskutiert werden.

Risiko Reaktion

Grundsätzlich wählt die Organisation weiterhin die beste Vorgehensweise im Kontext ihres ERM aus. Entscheidungen über die Risikobehandlung für die Allianz relevanter Risiken sollten allerdings mit den Partnern abgestimmt werden. Wenn die Allianz jedoch eine Methode definiert, um eine vergleichbare Bewertung zu ermöglichen, dann kann darauf aufbauend auch festgelegt werden, welche Risikohöhe relevant für die Allianz ist. In der Aktivität *Risiken einschätzen* wurde bereits festgelegt, dass die Partner eine gemeinsame Bewertungsmethode nutzen müssen, um eine Kommunikationsschnittstelle zum Austausch von Risikoinformationen etablieren zu können. Basierend auf der Risikotoleranz kann eine **Risikoakzeptanzschwelle** festgelegt werden, ab welcher Risiken von den Teilnehmern an die Allianz zu übermitteln sind. Dabei geht es nicht um die reine Information über das Risiko, sondern das Übertragen der Verantwortung über die Reaktion an die Allianz. Die Konsequenz ist, dass die Organisation nicht selbst eine **Behandlungsoption** auswählen darf, sondern diese mit den Partnern abstimmen muss. Nur so kann sichergestellt werden, dass das ursprünglich festgelegte Sicherheitsniveau erhalten bleibt und die Allianz nicht

Abbildung 6.5: Verteilung der Aufgaben in der Aktivität *Risiken behandeln*



durch von einzelnen Organisationen akzeptierte Risiken gefährdet wird[1]. Da das einen bedeutenden Eingriff in die Souveränität der Organisationen darstellt, müssen sich alle Partner auf den Schwellwert einigen und sich dazu bekennen (CSF 3). Dies nur in Kooperationsformen mit einer hinreichenden Vertrauensbasis gelingen, was eine Kerneigenschaft der strategischen Allianz ist (siehe Kapitel 3).

Behandlung

Bei der Wahl einer passenden Behandlungsoption sollten die Partner gemeinsam ein Vorgehen beschließen, dass den größten Mehrwert aus dem kollaborativen Prozess zieht. Es sind im kooperativen Kontext drei Szenarien denkbar, wenn eine Organisation ein relevantes Risiko teilt:

1. Die Organisation will das Risiko akzeptieren. Es muss bewertet werden, ob das Risiko sich auf die Allianz auswirken kann und dem Risikoappetit dieser entspricht.

2. Die Organisation wählt eine Sicherheitsmaßnahme, die lokal umgesetzt werden soll. In diesem Fall geht es lediglich um das Teilen von Risikoinformationen.

3. Die Organisation schlägt eine gemeinsame Risikobehandlung vor. Auch andere Partner, die von dem Risiko ebenfalls betroffen sind, können die Behandlung initiieren.

[1]Es ist die Grundannahme einer strategischen Allianz, dass ein essenzieller Schaden einer Organisation sich auch negativ auf die anderen Partner auswirkt, da deren Business eng miteinander verflochten ist

Anders als beim reinen SCRM werden hier insbesondere Risiken besprochen, welche keine direkte, sondern nur eine indirekte Auswirkung auf einen Partner oder die Allianz haben. Insbesondere beim Teilen der Risikoinformationen und dem Identifizieren geteilter Risiken liegt der große Vorteil des kollaborativen Ansatzes. Um Ressourcen zu sparen, können nicht nur gemeinsame Projekte gestartet, sondern auch existierende Maßnahmen geteilt werden.

Schlussfolgerung 3: Risiken behandeln

Es muss eine Schnittstelle definiert werden, um Risiken zu teilen, die über der Risikoakzeptanzschwelle liegen.

6.2.4 Aktivität 4: Behandlung umsetzen

In diesem Prozessschritt wird die vorher ausgewählte Behandlungsoption umgesetzt. Dies bezieht sich auf alle Optionen außer der Akzeptanz, da auch beim Vermeiden oder Teilen von Risiken letztlich eine Aktion durchgeführt werden muss. Im klassischen ISRM ist diese Aktivität leicht zu implementieren, da im Prozess beschlossene Sicherheitsmaßnahmen wie jeder andere Change[2] in der Organisation umgesetzt wird. Durch das Management muss lediglich eine Person festgelegt werden, welche für die Umsetzung verantwortlich ist. Diese erhält die notwendigen Ressourcen zur Implementierung des Projektes und übernimmt die Rolle des Projektleiters. Dieses Vorgehen wird in der kollaborativen Erweiterung etwas komplizierter, da Maßnahmen nicht nur von einer Organisation, sondern auch gemeinsam mit anderen Partnern umgesetzt werden sollen. Neben dem Teilen von Risikoinformationen ist es ein Kernbestandteil des CISRM, durch die gemeinsame Risikobehandlung Synergien zwischen den Partnern zu entwickeln und so den Ressourcenbedarf jedes Einzelnen zu reduzieren. Abbildung 6.6 zeigt eine Übersicht der relevanten Aufgaben dieser Aktivität, welche im Folgenden diskutiert werden.

Vorgehen zur Umsetzung

Inwiefern dieser Schritt kollaborativ ausgeführt hängt davon ab, welches Vorgehen in der vorherigen Aktivität gewählt wurde. So ist es möglich, neue Maßnahmen entweder organisationsintern oder kooperativ mit den Partnern zu implementieren. Es ergeben sich auch hier drei verschiedene Möglichkeiten, die im kollaborativen Prozess zu berücksichtigen sind:

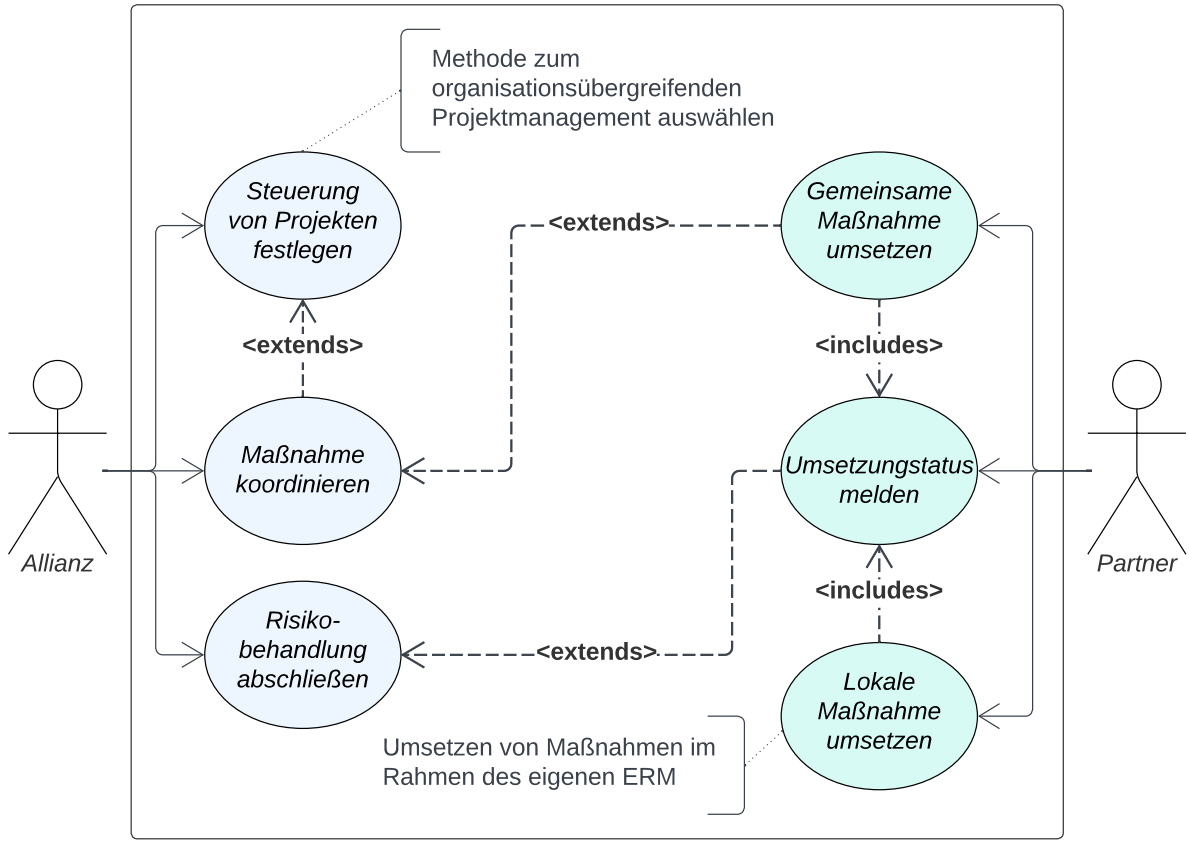
1. Wurde vorher keine Notwendigkeit einer kollaborativen Risikobehandlung festgestellt, dann folgt die Organisation weiter ihrem lokalen Prozess.

2. Implementiert eine Organisation eine Maßnahme alleine, dann ist auch keine weitere Koordination notwendig. Lediglich das Ergebnis sollte wiederum mit der Allianz geteilt werden, da die Erkenntnis anderen Partnern helfen kann.

3. Soll die Risikobehandlung kooperativ umgesetzt werden, gilt es ein gemeinsames Projekt zu starten und zu koordinieren.

[2]Ein Change beschreibt eine technische oder organisatorische Änderung innerhalb der Organisation

Abbildung 6.6: Verteilung der Aufgaben in der Aktivität *Behandlung umsetzen*



Kooperative Projekte

Das ISRM ist lediglich für Auswahl der Behandlungsoption, das **Festlegen des Vorgehens** und die anschließende **Initialisierung der Maßnahme** zuständig. Aufbau und Durchführung des Projektes zur Implementierung der Maßnahme sind kein Teil des Prozesses. Die Allianz muss sich auf eine geeignete Projektmanagementmethode einigen, um gemeinsame Projekte zu koordinieren. Dabei ist das organisationsübergreifende Projektmanagement (inter-firm projects) ein bereits lange und intensiv untersuchtes Thema [217], zu dem bereits umfängliche Methoden [218] existieren. Somit kann diese Projektmanagementmethode unabhängig vom CISRM gewählt und etabliert werden, ohne besondere Abhängigkeiten vom Prozess. Es muss jedoch sichergestellt sein, dass eine **Rückmeldung der Ergebnisse** erfolgt, um die Nachverfolgung von Risiken zu ermöglichen.

Maßnahmen

Eine Besonderheit bei gemeinsamen Maßnahmen ist, dass die Implementierung über mehrere Organisationen verteilt sein kann. Unabhängig von der gewählten Projektmanagementmethode muss ein Akteur die Steuerung des Projektes übernehmen. Dieser kontrolliert das Projekt zentral und sorgt für die notwendige Abstimmung zwischen den Partnern. Den Beteiligten bleibt damit nur die Verantwortung für die Umsetzung ihres lokalen Teils, was analog zur Umsetzung von Maßnahmen im ERM erfolgen kann. Nach erfolgreicher Umsetzung und Rückmeldung der Ergebnisse wird auch hier die Risikobehandlung abgeschlossen.

Mehrwert

Den Partnern ist durch die Nutzung des kollaborativen Prozesses ein Mehrwert entstanden, wenn sie beim Etablieren der Maßnahme weniger Ressourcen aufwenden mussten, als bei einer lokalen Umsetzung. Damit ist dies neben dem Teilen von Risikoinformationen in Aktivität 3 ein weiterer zentraler Aspekt des CISRM, welcher der Allianz einen Vorteil gegenüber dem klassischen ISRM liefert. Manche Projekte werden durch die gemeinsame Risikobehandlung erst ermöglicht, da sie zu groß für eine einzelne Organisation gewesen wären. Im ERM werden solche Risiken meist akzeptiert, mit dem Verweis darauf, dass eine Maßnahme wirtschaftlich nicht darstellbar wäre. Die gemeinsam etablierten oder genutzten Maßnahmen helfen den Partnern somit direkt, ihre eigenen Risiken einfacher zu behandeln.

Schlussfolgerung 4: Behandlung umsetzen

Die Partner müssen eine gemeinsame Strategie zur Initialisierung gemeinsamer Projekte festlegen und definieren, wie die Informationen an den Prozess gemeldet werden.

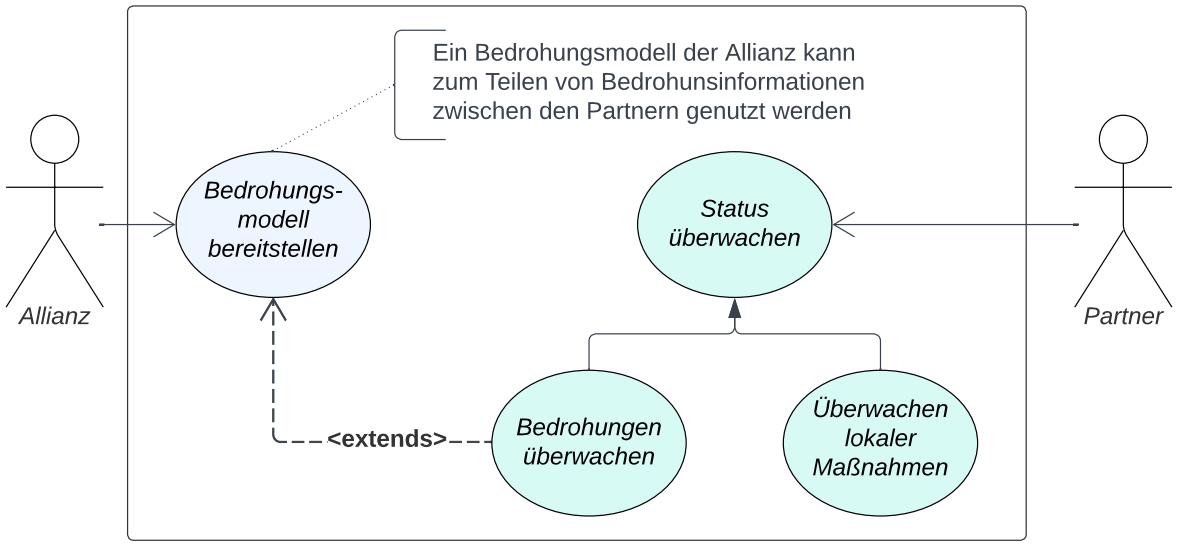
6.2.5 Aktivität 5: Risiken und Maßnahmen überwachen

Diese unterstützende Aktivität läuft parallel zur eigentlichen Erfassung und Behandlung von Risiken im Prozess. Dabei werden Risiken und Maßnahmen aus vorherigen Iterationen kontinuierlich überwacht, um auf Veränderungen reagieren zu können. Im ISRM wird diese Aktivität dadurch etabliert, dass jedes Risiko und jede Maßnahme einer verantwortlichen Person zugeordnet ist. Beim wertebasierten ISRM steht jedes Risiko und damit jede Maßnahme in Zusammenhang mit einem Asset. Die für das Asset verantwortliche Person hat damit ein intrinsisches Interesse an der Behandlung von Risiken, die dieses gefährden könnten. Somit ist diese auch zuständig für die regelmäßige Überprüfung des Risikostatus, welcher sich durch innere und äußere Einflüsse jederzeit ändern kann. Daran sollte sich im CISRM grundsätzlich nichts ändern, da die internen Verantwortlichkeiten der Organisationen nicht angetastet werden. Abbildung 6.7 zeigt eine Übersicht der relevanten Aufgaben dieser Aktivität, welche im Folgenden diskutiert werden.

Unabhängige Überwachung

Ändert sich die Wirksamkeit von Maßnahmen oder die aktuelle Bedrohungslage, dann müssen Risiken entsprechend neu bewertet werden. Das stellt grundsätzlich eine lokale Aktivität dar, welche den Organisationen selbst überlassen bleibt. Sollten sich dabei Änderungen an den Risiken ergeben, liefert dies den Input für die laufende Risikobehandlung oder die nächste Prozessschleife. Dadurch laufen aktualisierte Risiken, bei denen sich auch relevante Anpassungen für die Allianz ergeben, automatisch wieder in die gemeinsame Einschätzung. Hier sollte der verteilte Prozess vollständig analog zu dem in einer einzelnen Organisation funktionieren. Allerdings wäre auch eine Ausführung der Aktivität bezogen auf die Allianz betreffende Risiken als gemeinsame Aktion denkbar. Dabei könnte der Kontext der Bedrohungen für die Allianz ermittelt werden, etwa durch regelmäßige Aktualisierung eines gemeinsamen **Bedrohungsmodells**. Dieses kann dann wiederum von den Organisationen als Eingabe in die lokale Aktivität dienen, um die Bedrohungslage anzupassen. Ein solches Vorgehen würde den Partnern regelmäßig angemessene Bedrohungsinformationen

Abbildung 6.7: Verteilung der Aufgaben in der Aktivität *Risiken und Maßnahmen überwachen*



liefern, die sie alleine nicht hätten oder über eine zusätzliche Threat Intelligence Maßnahme beschaffen müssten.

Zentrale Überwachung

Weiterhin stellt sich die Frage, wer für die Überwachung von gemeinsam implementierten Maßnahmen (Aktivität 4) zuständig ist. Da die Allianz die Möglichkeit hat, Risiken durch die Umsetzung kooperativer Projekte zu behandeln, können potenziell übergreifende Maßnahmen entstehen. Die Charakteristik einer strategischen Partnerschaft ist es allerdings, dass sie einen Zusammenschluss unabhängiger Organisationen darstellt. Damit gibt es keine übergeordnete Instanz, welche die Verantwortung (Ownership) für Maßnahmen übernehmen könnte. Allerdings ist es unklar, ob überhaupt Maßnahmen entstehen könnten, die nicht direkt einzelnen Partnern zugeordnet werden können. Projekte können zwar gemeinsam durchgeführt werden, aber die Übernahme der Projektergebnisse obliegt einer oder mehreren Organisationen. Damit liegen die entstehenden Maßnahmen auch wieder im lokalen Zuständigkeitsbereich von diesen. Somit scheint es keine Notwendigkeit für eine übergreifende Aktivität zur Überwachung von Risiken und Maßnahmen innerhalb der Allianz zu geben.

Schlussfolgerung 5: Risiken und Maßnahmen überwachen

Die Allianz sollte ein Bedrohungsmodell bereitstellen und regelmäßig aktualisieren, damit die Partner die lokale Bedrohungslage daran ausrichten können. Dies liefert einen kollaborativen Mehrwert bei der regelmäßigen Überwachung von Risiken.

6.2.6 Aktivität 6: Mit Stakeholdern kommunizieren

Die Aktivität stellt die notwendigen Mechanismen zur Verfügung, um relevante Stakeholder über den Verlauf und die Ergebnisse des Prozesses informiert zu halten. Wie im Prozessmodell (Abbildung 6.2) zu sehen, sind bewertete Risiken und die gewählte Risikobehandlung wichtige Informationen, die zeitnah an die Stakeholder kommuniziert werden müssen. Jede Organisation sollte bereits entsprechende Kommunikationswege etabliert haben, um das ISRM zu unterstützen. Im CISRM gilt es nun lediglich, die Kommunikation bei Bedarf um potenzielle neue Stakeholder zu erweitern und zusätzliche Kanäle festzulegen. Zusätzliche Stakeholder sind mindestens die Partner selbst, welche über das Teilen der Risikoinformationen in den vorherigen Aktivitäten allerdings bereits eingebunden sein sollen. Vielmehr geht es darum, wie dieser Informationsfluss in der Allianz organisiert werden kann. Der nächste Abschnitt befasst sich detaillierter damit, wie diese Kommunikationswege mit den passenden Ansprechpartnern etabliert werden können.

Schlussfolgerung 6: Mit Stakeholdern kommunizieren

Die Partner müssen sich gegenseitig und die Allianz als Ganzes als externe Stakeholder erfassen. Es gilt festzulegen, welche Personen für die Kommunikation innerhalb der Allianz und zwischen den Organisationen verantwortlich sind.

6.3 Etablieren von Kommunikationswegen

Im vorherigen Abschnitt wurden die Aktivitäten des generischen Prozesses (Abbildung 6.2) genauer untersucht. Dabei sind verschiedene Aufgaben diskutiert worden, welche als Teil der Aktivität durchgeführt werden müssen. Die Analyse hat gezeigt, dass für einige eine lokale Ausführung, also innerhalb einer einzelnen Organisation, sinnvoll ist, während bei anderen auch ein kollaboratives Vorgehen, d.h. gemeinsam mit den Partnern, denkbar ist. In einigen Fällen zeigt sich, dass die Zusammenarbeit Vorteile gegenüber dem klassischen ISRM liefert. So liefert der gezielte Austausch von Informationen an den richtigen Schnittstellen einen Mehrwert, der sowohl die Partner als auch die Allianz als Ganzes voranbringen kann. Dieser Informationsaustausch ist grundsätzlich Teil aller Aktivitäten, jedoch insbesondere im Fokus der Aktivität *Mit Stakeholdern kommunizieren*. Es stellt sich die Frage, wie diese Kommunikation innerhalb der Allianz organisiert werden kann.

Herausforderung

Die Kommunikation ist das Kernthema bei der strategischen Zusammenarbeit von Organisationen. Der organisationsübergreifende (inter-organisatorische Kommunikation) Informationsaustausch unterscheidet sich dabei grundlegend vom Austausch innerhalb von Organisationen (intra-organisatorische Kommunikation). Auch hier ist der Grund wiederum die Unabhängigkeit der Partner und die daraus folgende Kommunikationsautonomie beim Austausch von Informationen. Während der Austausch innerhalb von Organisationen meist problemlos möglich ist, da diese die Kontrolle über die Daten behält, verlassen diese beim Austausch die Grenzen der Organisation und damit auch deren Verantwortungs- bzw. Einflussbereich. [187]

Inputs/ Outputs

Ein grundlegender Aspekt bei der organisationsübergreifenden Koordination von Risiken stellt die Kommunikation identifizierter und evaluierter Risiken dar. Wie in Abbildung 6.1 zu sehen, betrachten alle untersuchten Rahmenwerke die Kommunikation als eine eigene Aktivität innerhalb des ISRM Prozesses. Somit befinden sich die Aufgaben zum Austausch von Informationen immer außerhalb zu denen der operativen Aktivitäten der Risikoeinschätzung. Auf der einen Seite können die Outputs der Risikoeinschätzung als Input für die Kommunikation mit interessierten Parteien genutzt werden, auf der anderen Seite kann das erhaltene Feedback wiederum Input für die Risikoanalyse sein. Abgesehen von dieser Input-Output-Schnittstelle ist eine Integration der verschiedenen Aktivitäten allerdings nicht vorgesehen, da eine kontinuierliche Kommunikation während der Ausführung einer Aktivität nicht notwendig ist.

Verantwortlichkeiten

Während die Struktur des Kommunikationsflusses damit bereits definiert ist, stellt sich die Frage, wie dieser organisiert wird. Das Prozessmodell definiert, **wann** eine Kommunikation erfolgt (Zeitpunkt/Ereignis in der Aktivität) und **was** dabei zu übertragen ist, also die geteilte Information (Inputs/Outputs der Aktivitäten). Es fehlt eine Zuordnung, **wer** für die Durchführung der Kommunikation verantwortlich ist (Person innerhalb der Allianz/Organisation), sowohl als Sender als auch Empfänger der Informationen. Es gilt für jede Schnittstelle festzulegen, welche Rolle für die Kommunikation zuständig ist. Dabei ist insbesondere die Aufteilung der Zuständigkeiten zwischen Allianz und Organisation zu berücksichtigen. Diese Verantwortlichkeiten werden üblicherweise rollenbasiert festgelegt, wie es auch in den meisten ISRM-Frameworks der Fall ist. Organisatorische Rollen bilden

eine durch die Organisation vorgegebene Sammlung von Aufgaben, Befugnissen und Verantwortlichkeiten. Eine Rolle kann mehreren Personen zugeordnet werden und eine Person kann mehrere Rollen einnehmen. Aufgrund entgegengestzter Zielsetzungen kann jedoch bei manchen Rollen ein Interessenskonflikt bestehen, weshalb diese unterschiedlichen Personen zugewiesen werden sollten, um deren Unabhängigkeit zu gewährleisten.

Vorgehen

Die für die Kommunikation verantwortlichen Personen sollen daher als Rollen im Prozessmodell festgelegt werden. Im folgenden Abschnitt werden diese Rollen und deren Aufgabenbereich beschrieben. Dabei wird diskutiert, welche zusätzlichen Aufgaben diesen zugeordnet werden muss, um die Kommunikation und den Austausch von Risikoinformationen in der Allianz zu ermöglichen. Während die vorherige Analyse lediglich zwischen lokalen und gemeinsamen Aufgaben unterschieden hat, sollen die Aufgaben nun konkrete Akteure aus der Allianz oder den Organisationen übernehmen. Ziel ist es auch hier, möglichst keine neuen Kompetenzen zu vergeben, sondern existierende ISRM Strukturen zu nutzen. Die Verantwortlichkeiten können jeweils den gemeinsamen Aktivitäten (Kapitel 6.2) zugeordnet und anschließend als RACI-Matrix[3] dargestellt werden. Das Ergebnis stellt eine Übersicht über alle im kollaborativen Prozess notwendigen Rollen und Verantwortlichkeiten dar.

6.3.1 Klassische Rollen

Die Nutzung von Rollen zur Strukturierung von Verantwortlichkeiten ist ein Standardvorgehen bei der Definition von Prozessen. Jedes betrachtete Framework etabliert bestimmte Rollen und viele Organisationen nutzen oder adaptieren diese in ihrer internen Struktur. Jedoch sind weder die Rollenbezeichnungen noch deren Verantwortlichkeiten einheitlich definiert. Abhängig von der genutzten Literatur und auch dem Kontext der Organisation, etwa Unternehmenstyp und Branche, haben sich unterschiedliche Funktionen etabliert. Trotzdem existieren grundlegende Verantwortlichkeiten, die von einer Person abgedeckt werden müssen.

Literatur

Wie bereits bei den Begriffen ist es überraschend, dass keine einheitliche Definition von Rollen für das ISRM vorhanden zu sein scheint. Oftmals werden nur wenige Rollen verwendet oder explizit definiert. Dabei ist auch nicht immer klar, für welche Aufgaben diese genau verantwortlich sind. Auch ein Blick auf weitere RM Bereiche hilft dabei kaum weiter. Bereits Ende der 90er haben sich Colquitt et al. [219] mit der Rolle des *Risiko Managers* im integrierten RM auseinandergesetzt und in ihrer Studie gezeigt, dass diese zwar in vielen Organisationen existiert, aber keine klar definierten Charakteristika besitzt. Auch im ERM scheint ein explizit ernannter *Risiko Manager* bzw. ein *Chief Risk Officer* notwendig die Organisation zu sein [220], aber seine genauen Aufgaben bleiben unklar. Diese zwei Beispiele zeigen, dass es lediglich Einigkeit darin gibt, dass es im Unternehmen einen verantwortlichen für das RM geben sollte. Obwohl eine allgemeingültige Liste der Rollen im ISRM in der Literatur nicht zu existieren scheint, werden in der Realität trotzdem einige Funktionen häufig im Prozess etabliert. Hier zeigt sich wieder eine Diskrepanz zwischen den

[3]Darstellungsform einer Responsibility Assignment Matrix (RAM) mit den Verantwortlichkeiten Responsible, Accountable, Consulted, Informed

theoretischen Grundlagen und von Experten gelehrter und gelebter Praxis. Eine Studie zur Befragung von Organisationen mit existierendem ISRM Prozess, z.B. auf Basis ISO/IEC 27001 zertifizierter Unternehmen, könnte Aufschluss über die tatsächlich etablierten Rollen und deren Verantwortlichkeiten in der Praxis schaffen.

Frameworks

Abseits allgemeiner Literatur kann sich auch hier wieder auf die bereits untersuchten Frameworks (Kapitel 2.3) bezogen werden, von denen zumindest einige Beispiele üblicher Rollen liefern. RiskIT [119] enthält eine von COBIT [112] abgeleitete, umfassende Liste von 33 Rollen, die als Stakeholder im Prozess gelten. Davon sind jedoch viele nicht spezifisch für das RM, sondern sind generelle Managementrollen eines Unternehmens, z.B. der *Chief Financial Officer (CFO)* und andere C-Level-Executives. Auch das RMF [103] enthält eine Liste von 20 Rollen und Verantwortlichkeiten, die es als Schlüsselfunktionen für den Prozess ansieht. Diese enthalten ebenso allgemeine Managementrollen, weitere aus dem ISM und spezialisierte wie den *Risk Executive*. Die ISO [49] enthält keine explizite Sammlung von Rollen, sondern nennt diese bei Bedarf in den allgemeinen Begriffsdefinitionen. Im IT-Grundschutz [56] werden einige übergeordnete Funktionen des IS-Managements angegeben, aber keine besonderen für das ISRM. MoR [127] liefert sehr wenig Vorgaben dazu, wer genau eine bestimmte Aktivität durchführen soll. Es wird lediglich aufgefordert, dass die Organisation klare Rollen und Verantwortlichkeiten für die Bereiche Führung, Maßnahmen, Berichtswesen, Review und die Durchführung des Prozesses etablieren soll. Jedoch wird darauf hingewiesen, dass sowohl eine Rolle für das RM notwendig ist, als auch die Verantwortung des *Boards* essenziell ist. Der ENISA Prozess liefert keine zusätzlichen Informationen zu Verantwortlichkeiten im ISRM.

Rollen

Die genauen Rollen in der Literatur sind damit insgesamt eher schwach definiert und können nicht vollständig von existierenden Standards abgeleitet werden, wie es bei der Terminologie oder dem Prozess der Fall gewesen ist. Trotzdem ist es notwendig einen Überblick über die häufig vorgefundenen Funktionen im ISRM zu geben, um deren Aufgaben zu verstehen und diese auf den kollaborativen Prozess anzuwenden. Nach genauerer Betrachtung der in der Literatur genannten Rollen und den in den Aktivitäten verlangten Aufgaben lassen sich tatsächlich generische Verantwortlichkeiten abstrahieren, die für das ISRM essenziell scheinen. Es wird angenommen, dass grundsätzlich mindestens vier Funktionen vorhanden sein sollten, um einen funktionsfähigen ISRM Prozess etablieren zu können. Das sind eine Person/Gruppe, welche

(R1) ein Risiko organisatorisch erfasst und fachlich bewertet;

(R2) die fachliche Verantwortung für ein Risiko bzw. dessen Risikoeinschätzung übernimmt;

(R3) die Gesamtverantwortung für die Risikobehandlung trägt;

(R4) den Prozess selbst koordiniert.

Weitere Rollen können je nach Organisation sinnvoll sein, um Aufgaben oder Entscheidungen besser zu verteilen, aber zumindest diese vier erscheinen im ISRM notwendig. Im Folgenden werden nun die grundlegenden Rollen gelistet und ihre Relevanz für den kollaborativen Prozess diskutiert.

Rolle: Risiko Redakteur

Der *Risiko Redakteur* ist in seiner Organisation verantwortlich für die Pflege der Risikodokumentation (R1). Er stammt üblicherweise aus der Fachabteilung und hat die operative Verantwortung für ein Asset, z.B. der Administrator eines Systems. Durch diese betriebliche Nähe zu den (Supporting) Assets versteht er deren technische oder organisatorische Details und erkennt relevante Bedrohungen am ehesten. Der *Risiko Redakteur* muss keine dedizierte Person sein, sondern kann auch zusätzlich von einer andern Rolle übernommen werden.

Relevanz Der Redakteur ist eine lokale Rolle, die innerhalb einer Organisation verantwortlich für die Risiken ist. Da innerhalb der Allianz keine Risiken dokumentiert werden, sondern lediglich die Risiken der Partner koordiniert, bestehen keine kollaborativen Aufgaben für diese Rolle. Der Redakteur ist jedoch auf der Empfängerseite aktiv, da die geteilten Informationen für ihn relevant sein können.

Rolle: Asset Owner

Der *Asset Owner* „should be responsible for the proper management of an asset over the whole asset lifecycle“ [97]. Er besitzt damit die fachliche Verantwortung für ein Asset innerhalb der Organisation (R2). Als Teil der mittleren Führungsebene kann er relevante Entscheidungen im Geschäftskontext selbständig treffen, weshalb er etwa auch als *Business Process Owner* [119, 112] oder *Primary Stakeholder* [122] bezeichnet wird. Bereits ab einer mittleren Größe ist es für das Top-Management essenziell, die Verantwortung für einzelne Werte an Vertreter aus dem Business zu delegieren.

Relevanz Der *Asset Owner* ist grundsätzlich eine essenzielle lokale Rolle innerhalb der Organisation, da sie im ISRM die Verantwortung für ein einzelnes Asset trägt. Damit ist sie allerdings auch relevant für das CISRM, da dieses letztlich auch auf dem gemeinsamen Schutz der Assets in der Allianz beruht. Die Risiken, die innerhalb der Organisation identifiziert werden, liefern letztlich die Grundlage für die gemeinsame Risikobetrachtung (Abbildung 6.4) bzw. deren lokale Behandlung, falls es sich nicht um ein für die Allianz relevantes Risiko handelt (Abbildung 6.5). In beiden Fällen werden die Maßnahmen, egal ob einzeln oder gemeinsam implementiert, vom zuständigen Asset Owner überwacht und kontinuierlich auf die geänderte Bedrohungslage reagiert (Abbildung 6.7).

Rolle: Risiko Owner

Der *Risiko Owner* ist eine „person or entity with the accountability and authority to manage a risk“ [67]. Er trägt damit die Gesamtverantwortung für ein Risiko innerhalb der Organisation (R3). Somit kann diese Verantwortlichkeit nur ein Mitglied der Leitung des Unternehmens einnehmen, der die entsprechende Entscheidungskompetenz besitzt, um Risiken zu akzeptieren. Das Top-Management, eine „person or group of people who directs and controls an organization (3.50) at the highest level“ [49], sollte entweder selbst die Rolle des Risiko Owners einnehmen oder eine leitungsnahe Person damit beauftragen. Die

Schwierigkeit dabei ist, dass die Hauptverantwortung (Accountability) für die Risikoakzeptanz normalerweise nicht delegiert werden kann, da am Ende nur die Geschäftsführung das unternehmerische Risiko tragen kann. Daher wird oftmals lediglich die Durchführungsverantwortung (Responsibility) übertragen, was für die Durchführung des Prozesses jedoch eher eine untergeordnete Rolle spielt. Während *Risiko Redakteur* und *Asset Owner* keinen einheitlichen Rollennamen besitzen, ist die Rolle des *Risiko Owners* weitgehend standardisiert.

Relevanz Da es sich beim *Risiko Owner* um einen Entscheidungsträger innerhalb der Organisation handelt, hat diese Rolle nur wenige Aufgaben im CISRM, da dort die Entscheidungen gemeinsam mit den Partnern gefällt werden müssen. Es ist sinnvoller, dass die Aufgaben in diesem Fall von einer Gruppe von Personen (siehe *Risiko Board*) oder einem Vertreter der Organisation (siehe *CISRM Beauftragter*) übernommen werden. Natürlich könnte dies von derselben Person in Personalunion durchgeführt werden. Die Aufgaben des lokalen *Risiko Owners* besteht eher darin, dass er die Verantwortung für die Entscheidungen trägt, welche beim Festlegen des Kontexts des Prozesses getroffen werden. Das beinhaltet insbesondere die Freigabe von Risikoappetit und Toleranz der eigenen Organisation und die Verpflichtung zu den in der Allianz ausgehandelten Rahmenbedingungen (Abbildung 6.3).

Rolle: Risiko Manager

Der *Risiko Manager* ist der Prozessmanager für den ISRM Prozess, d.h. „A role or individual responsible for the implementation of risk management for each activity at each of the organizational levels“ [127]. Er ist verantwortlich für die Definition und Steuerung des Prozesses innerhalb der Organisation (R4). Dazu gehört das Festlegen der Methodik in Abstimmung mit dem Risiko Owner, das beinhaltet die Freigabe der Bewertungsmatrix und der Risikoakzeptanzschwelle. Weiterhin koordiniert der *Risiko Manager* die Durchführung des Prozesses und sorgt für eine konforme Durchführung der Verfahren durch *Risiko Redakteur*, *Asset Owner* und *Risiko Owner.* Er unterstützt bei der korrekten Einstufung von Risiken, nimmt jedoch selbst keine aktive Rolle bei der fachlichen Bewertung ein. Ein übergeordneter Chief Risk Officer [112, 119] kann dabei verantwortlich für das gesamte ERM sein und Unternehmensvorgaben in den verschiedenen RM-Prozessen synchronisieren.

Relevanz Als zentrale Person für die Steuerung des ISRM in der eigenen Organisation ist der *Risiko Manager* ebenfalls essenziell für das CISRM. Im kollaborativen Prozess werden die Aktivitäten lediglich innerhalb der Allianz kommuniziert und die Risikobehandlung zwischen den Teilnehmern abgestimmt, aber jeder Partner führt weiterhin seinen lokalen Prozess aus. Damit ist der *Risiko Manager* dafür verantwortlich, den Austausch von Informationen gemäß den festgelegten Kommunikationswegen zu unterstützen. Bereits bei der Planung definiert er Risikoappetit und Toleranz der Organisation basierend auf Rahmenbedingungen, auf die sich die Partner geeinigt haben und legt diese dem *Risiko Owner* zur Freigabe vor (Abbildung 6.3). Letztlich liegt es an ihm, die in der Allianz beschlossene Methodik im organisationsinternen Prozess zu implementieren. Weiterhin bleibt er verantwortlich für die regelmäßige Risikoeinschätzung innerhalb der Organisation, ohne das sich

dadurch die Aufgaben für den *Risiko Manager* verändern würden (Abbildung 6.4). Bei der Behandlung von Risiken muss der *Risiko Manager* dafür sorgen, dass die Relevanz der Risiken für die Allianz geprüft wird, bevor eine lokale Freigabe oder Behandlung durchgeführt wird (Abbildung 6.5). Auch hier ist es seien Aufgabe, die Vorgaben der Allianz in der Risikobehandlung abzubilden.

6.3.2 Erweiterte Rollen

Gerade in kleineren Organisationen können die vier Rollen bereits ausreichend sein, um einen funktionierenden Prozess zu etablieren. Mit zunehmender Größe steigt auch die Komplexität des ISRM und eventuell werden zusätzliche Rollen benötigt, um die Effizienz des Prozesses zu steigern. Auch lassen sich manche Aufgaben sicherlich in separate Rollen auslagern oder neue Funktionsbereiche definieren, z.B. besondere Zuständigkeiten für Datenschutzrisiken. Im Kontext dieser Arbeit soll die Rollenübersicht jedoch möglichst einfach bleiben und nur die Rollen untersucht werden, die für den kollaborativen Prozess tatsächlich notwendig sein könnten. Daher werden im Folgenden drei weitere Rollen beschrieben, die oftmals im ISRM zu finden sind und die potenzial für die Anwendung im CISRM haben.

Rolle: Maßnahmen Owner

Der *Maßnahmen Owner* ist verantwortlich für die Planung und Steuerung einer in der Risikobehandlung freigegebenen Maßnahme. Grundsätzlich könnte dies als essenzielle Funktion angesehen werden, da immer jemand die Verantwortung für die Umsetzung übernehmen muss. Jedoch wird die Implementierung der Maßnahme häufig nicht als Teil des RM gesehen, sondern als eine Aktivität außerhalb des Prozesses. Dabei sollte trotzdem klar sein, dass in jedem Fall eine freigegebene Maßnahme der Output des Prozesses ist und die implementierte Maßnahme den Input für die zukünftige Überachung und nächste Iteration darstellt. Definitiv ist jedoch die Koordination Teil des Prozesses in der Aktivität *Behandlung umsetzen*, während die tatsächliche Umsetzung außerhalb des Prozesses geschieht.
Innerhalb der Organisation muss der *Maßnahmen Owner* sicherstellen, dass eine freigegebene Maßnahme tatsächlich umgesetzt wird. Er muss diese nicht selbst implementieren, trägt allerdings die Umsetzungsverantwortung. Somit kann der Owner sowohl eine Person mit technischer Leitung (z.B. ein Service Owner) sein oder auch nicht-technischer Leiter (z.B. ein reiner Projektmanager). Der *Maßnahmen Owner* sorgt für ein regelmäßiges Statusupdate, damit diese Informationen in die Bewertung des Risikos einbezogen werden können.

Relevanz Betrachten wir die Umsetzung der Maßnahme auch als Teil des Prozesses, bzw. zumindest die Tatsache, dass sie Koordiniert werden muss, dann spielt der *Maßnahmen Owner* auch im CISRM eine Rolle. Dabei geht seine Tätigkeit dabei grundsätzlich nicht weit über die Aufgaben hinaus, die er auch im lokalen ISRM übernimmt. Alle von der Allianz beschlossen Maßnahmen werden letztlich von einem oder mehreren Partnern getragen. Damit läuft die Umsetzung einer gemeinsamen Maßnahme analog zu einer Einzelmaßnahme,

nur das Erstere noch organisationsübergreifend koordiniert werden muss (siehe Projektmanager). Da diese Koordination allerdings die Mitwirkung aller Beteiligten erfordert, ergibt sich als zusätzliche Aufgabe für den *Maßnahmen Owner* die Kommunikation mit anderen Partnern (Abbildung 6.6). Auch bei Einzelmaßnahmen muss der Umsetzungsstatus an die Allianz zurückgemeldet werden.

Rolle: Risiko Board

Das *Risiko Board* ist eine Gruppe von Personen, die für die Freigabe und Akzeptanz von Risiken innerhalb der Organisation verantwortlich ist. In dargestellten Kontext bezieht sich sein Einfluss auf das ISRM, es könnte jedoch auch ein *Enterprise Risk Committee* [117, 112] geben, welches für das gesamte ERM zuständig ist. In jedem Fall ist die Idee, dass der *Risiko Owner* die Entscheidungsgewalt über die Risikobehandlung an das *Risiko Board* delegiert, wenn er nicht selbst auch Teil dieses ist. Der Vorteil bei einer Gruppe von Personen ist, dass so Vertreter verschiedener Verantwortungsbereiche, Manager und Business Owner zusammengebracht werden können, um eine gemeinsame Entscheidung zu treffen. Die kann nicht nur die Akzeptanz der Risikobehandlung erhöhen, sondern integriert auch bereits die notwendige Kommunikation mit *Stakeholdern*.

Relevanz Grundsätzlich ist das *Risiko Board* nur eine Alternative zur Entscheidungsfindung und Entlastung des *Risiko Owners*, die im lokalen Prozess etabliert werden kann. Wie organisationsinterne Entscheidungen im ISRM getroffen werden, soll für das CISRM keine Rolle spielen. Trotzdem scheint das Konzept ein sinnvolles Modell zur Risikobehandlung innerhalb der Allianz zu sein, bei dem sich auch die Partner auf ein gemeinsames Vorgehen einigen müssen. Denkbar ist daher ein auf der Idee aufbauendes *Allianz Risiko Board*, wie im nächsten Abschnitt beschrieben.

Rolle: Stakeholder

Häufig wird auch der *Stakeholder* als explizite Rolle im ISRM definiert. Dabei handelt es sich um eine „person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity“ [67]. Dies können sowohl Personen sein, welche in den Prozess eingebunden, über die Ergebnisse informiert werden oder von Risiken und Maßnahmen betroffen sind. Eine mögliche Erweiterung ist der *Secondary Stakeholder*, d.h. „Individuals or organizations that may be affected by events that occur to assets outside of their control“ [122]. In jeden Bereich des ERM sollte darauf geachtet werden, relevante Stakeholder einzubeziehen, um deren Wissen für den Prozess zu nutzen und die Ergebnisse in der Organisation zu verteilen.

Relevanz Im CISRM existieren keine besonderen Aufgaben für die Stakeholder der Organisation. Es lässt sich argumentieren, dass alle Partner in der Allianz grundsätzlich zusätzliche Stakeholder sind. Dabei sind jedoch nur die relevant, die als Teilnehmer in den Scope des CISRM aufgenommen wurden. Diese sollten jedoch aktiv in den Prozess eingebunden sein und bereits einen Vertreter entsenden, der für die Kommunikation verantwortlich ist (siehe *CISRM Beauftragter*). Somit sollte jede Organisation weiterhin ihre internen und

externen Stakeholder im Rahmen des ISRM einbeziehen, für den kollaborativen Prozess ist diese Rolle jedoch nicht notwendig.

6.3.3 CISRM Rollen

Die oben genannten Rollen sind nun diese, die im klassischen ISRM in den meisten Organisationen vorhanden sein sollten. Diese sind grundsätzlich nur für Aufgaben innerhalb des Prozesses der eigenen Organisation verantwortlich. Jedoch können die meisten davon genutzt werden, um einige zusätzliche Kommunikationsaktivitäten im Kontext des kollaborativen Prozesses zu übernehmen. Zur vollständigen Erweiterung hin zum CISRM innerhalb der Allianz fehlen allerdings noch weitere Funktionen, um alle in Abschnitt 6.2 beschriebenen Aktivitäten zu realisieren. Daher müssen zusätzliche Rollen definiert werden, die für die Inter-Kommunikation und Koordination der Aufgaben auf dieser Ebene verantwortlich sind. Wie auch die lokalen Rollen sind diese nur logisch getrennt definiert und können selbstverständlich auch von Personen/Gruppen mit einer zugehörigen Rolle in einer Organisation übernommen werden.

Rolle: Allianz Lenkungsausschuss

Die Allianz selbst ist keine Organisation und hat damit kein Top-Management, dass die Verantwortung (Accountable) für übergreifende Aktivitäten übernehmen kann. Damit gilt es eine Art Steuerungskreis zu etablieren, der die autoritäre Kontrolle über den kollaborativen Prozess übernimmt. Diese Gruppe ist verantwortlich für die Auswahl der Teilnehmer (Anwendungsbereich) und für das Einsetzen der restlichen CISRM Rollen, damit muss sie als erstes etabliert werden (Abbildung 6.3). Nur so kann sichergestellt werden, dass sich alle Teilnehmer im Prozess vertreten und respektiert fühlen. Diese Rolle wird immer dann aktiv, wenn Entscheidungen im Namen aller Partner getroffen werden müssen.

Zuweisung Es ist denkbar, dass in einer existierenden Allianz bereits ein Ausschuss etabliert wurde, der für die gemeinsamen Initiativen verantwortlich ist. Dieser wäre in der besten Postion, auch im Rahmen des CISRM steuernd tätig zu werden. Letztlich gibt jedes Unternehmen ein bisschen der eigenen Souveränität auf, wenn es sich auf das gemeinsame Vorgehen einlässt. Dies wird am besten vom Top-Management der Partner legitimiert. Allerdings ist das ISRM auch eine spezialisierte Managementfunktion, die nicht unbedingt von den Business-Leadern übernommen werden kann. Ein für den Bereich zuständiger C-Level-Executive (COO, CIO, CTO) wäre damit vermutlich die beste Wahl für die Entsendung in den Lenkungsausschuss.

Rolle: Allianz Risiko Board

Der Lenkungsausschuss besteht aus strategischen Führungskräften der Partner, die üblicherweise nicht in den operativen Prozess eingebunden werden. Gleichzeitig gibt es in der Allianz selbst keinen *Risiko Owner*, da die Risiken letztlich den einzelnen Organisationen

gehören. Damit ist es weiterhin notwendig zu definieren, wer für das Festlegen der Methode und die Freigabe der Risikobehandlung verantwortlich sein kann. Dazu kann ein Risiko Board auch auf Ebene der Allianz etabliert werden, um die Entscheidungen über Risiken zu treffen. Die Funktionsweise ist damit analog zu der einer lokal etablierten Gruppe.
Nachdem das Board durch den *Allianz Lenkungsausschuss* eingesetzt wurde, sollte es bei der Festlegung des Appetits und der Toleranz der Organisation federführend aktiv sein (Abbildung 6.3). Anschließend kann nur sie die Entscheidung treffen, welche ISRM-Methode von der Allianz genutzt werden sollte, eine taktische Entscheidung, die allerdings zu nah an der Umsetzung des Prozesses für den *Lenkungsausschuss* ist (Abbildung 6.4). Dazu gehört außerdem, die Akzeptanzschwelle für Risiken festzulegen und bei Risiken die darüber liegen, über die Freigabe der Risikobehandlung zu entscheiden (Abbildung 6.5). Ansonsten sollte das Board zumindest über relevante Vorgänge innerhalb der Allianz informiert werden.

Zuweisung Wie auch das Risiko Board innerhalb einer Organisation braucht auch das Board in der Allianz die notwendige Legitimation, um die Entscheidungen zu fällen. Da grundsätzlich kein Partner zu Durchführung verpflichtet ist, muss die entsprechende Vertrauensbasis untereinander vorhanden sein. Alle Teilnehmer müssen in den Prozess eingebunden werden und sollten auf das Ergebnis Einfluss haben können (CSF 3). Damit muss zwangsweise jede Organisation in der Gruppe vertreten sein, um das notwendige Commitment zu den Entscheidungen des Boards sicherzustellen. Jeder Partner sollte Business-Leader in das Risiko Board entsenden, die in der Lage sind, die übergreifenden Risiken für das eigene Business zu bewerten.

Rolle: CISRM Beauftragter

Für alle Aktivitäten ist es notwendig, dass es eine Person gibt, welche die Organisation im CISRM vertritt. Dazu gehört die Kommunikation zwischen den verschiedenen Rollen, wodurch er insgesamt die Schnittstelle zwischen dem lokalen und kollaborativen Prozess bildet. Er ist somit für die Durchführung der Aktivität *Mit Stakeholdern kommunizieren* im Kontext der Allianz zuständig. Bei der Einschätzung der Risiken ist er dafür verantwortlich, die Informationen über Bedrohungen und Risiken aus der Allianz in den lokalen Prozess einzubringen, bzw. zurückzumelden (Abbildung 6.4). Auch bei der Behandlung ist der *CISRM Beuftragte* derjenige, der für die Allianz relevante Risiken identifiziert und dem *Risiko Board* vorlegt (Abbildung 6.5). Letztlich übernimmt er auch die Gesamtverantwortung dafür, dass die vereinbarten Maßnahmen vom *Maßnahmen Owner* lokal umgesetzt werden (Abbildung 6.6).

Zuweisung Bei der Wahl einer Person für diese Rolle bestehen keine besonderen Einschränkungen. Sie sollte bereits in den ISRM Prozess innerhalb der Organisation eingebunden sein und einen Überblick über alle Risiken haben. Es ist daher naheliegend, dass der *Risiko Manager* einer Organisation auch die Rolle des *CISRM Beauftragten* übernimmt. Gerade bei größeren Organisationen macht es jedoch Sinn die Rollen zu trennen, um die Arbeitslast besser zu verteilen.

Rolle: Allianz Risiko Manager

Der *Allianz Risiko Manager* übernimmt die Hauptverantwortung für die Koordination der Risiken innerhalb der Allianz. Er ist damit das CISRM Pendant zum lokalen *Risiko Manager* innerhalb der Organisation. Das bedeutet, dass er grundsätzlich in allen Aktivitäten des CISRM involviert ist, aber keine fachliche Verantwortung für die Risiken oder Maßnahmen übernimmt. Seine Aufgabe ist es von Anfang an den Prozess mit aufzubauen und zwischen den *CISRM Beauftragten* zu vermitteln (Abbildung 6.3). Er stimmt mit dem *Allianz Risiko Board* eine geeignete Methode ab und koordiniert den Austausch der Risikoinformationen (Abbildung 6.4). Nach erfolgter Risikobehandlung ist er dafür zuständig die Ergebnisse abzustimmen und die Risikobehandlung abzuschließen (Abbildung 6.6). Letztlich muss er dafür sorgen, aus die erhaltenen Informationen in das Bedrohungsmodell der Allianz einfließen zu lassen (Abbildung 6.7). Bei der Aktivität *Mit Stakholdern kommunzieren* ist er die zentrale Anlaufstelle für die *CISRM Beauftragten* und stimmt alle Informationen mit diesen ab.

Zuweisung Als einzige hier eingeführte Rolle übernimmt der *Allianz Risiko Manager* vollständig eine Aufgabe innerhalb der Allianz, bei der er nicht einen Partner repräsentiert. Er ist damit als Prozessmanager unabhängig von allen Organisationen und nur der Allianz als Ganzes verpflichtet. Dabei stellt sich natürlich die Frage, zu welcher Organisation diese Person gehören kann, wenn sie keinen direkten Bezug zu dieser hat. Es wird weiterhin davon ausgegangen, dass die Allianz selbst nur ein logisches Konstrukt ist und die Partnerschaft nicht in der Lage ist, selbst Personen zu beschäftigen. Damit ergeben sich zwei Möglichkeiten, wie die Rolle vergeben werden könnte. So könnte die Rolle fest einer Person innerhalb einer der Partnerorganisationen zugeordnet werden. Die Partner können sich auf einen Mechanismus einigen, um die Organisation die den *Allianz Risiko Manager* stellt zu entschädigen. Der Vorteil dabei ist, dass eine Person sich intensiv einarbeiten und die notwendigen Kompetenzen erlangen kann, die gerade bei der Kommunikation notwendig sind. Alternativ könnte sie als wechselnde Rolle definiert werden, die nach einem festen Intervall einem anderen Partner zugeordnet wird. So könnte etwa jeder *CISRM Beauftragte* im Wechsel auch die Rolle des *Allianz Risiko Managers* übernehmen. Dieses Vorgehen passt eher zum kollaborativen Gedanken und könnte die Akzeptanz des Prozesses stärken. Die Wahl hängt letztlich vom Kontext und den Vorlieben der Partner ab.

Rolle: Allianz Projektmanager

In der Aktivität *Behandlung umsetzen* sollen gemeinsam beschlossene Maßnahmen von den Partnern umgesetzt werden (Abbildung 6.6). Dabei ist der *Maßnahmen Owner* verantwortlich für die Umsetzung einer Maßnahme innerhalb der eigenen Organisation. Lokal wird dieser durch den *Risiko Owner* beschlossen und der *Maßnahmen Owner* in Abstimmung mit dem *Asset Owner* zugewiesen. Im CISRM werden die Maßnahmen durch das *Risiko Board* der Allianz freigegeben und eventuell gemeinsame Maßnahmen beschlossen. Dabei können nicht direkt Personen aus den Organisationen den einzelnen Maßnahmen zugeordnet werden. Für Maßnahmen, die von nur einer Organisation durchgeführt werden, spielt dies

keine Rolle, da der *CISRM Beauftragte* das *Risiko Board* lediglich informiert. Allerdings sind an der Umsetzung einer gemeinsamen Risikobehandlung potenziell mehrere Organisationen beteiligt. Unabhängig von der gewählten Methode zum Inter-Projektmanagement muss daher ein Koordinator auf Ebene der Allianz bestimmt werden. Dieser übernimmt die Abstimmung zwischen den an der Umsetzung beteiligten Partnern.

Zuweisung Die Rolle des *Projektmanagers* kann grundsätzlich jede Person einnehmen. Die gewählte Projektmanagementmethode könnte ebenfalls Einfluss auf die Auswahl haben. Ansonsten ist sicherzustellen, dass die Person organisatorisch in der Lage ist, ein übergreifendes Projekt zu koordinieren. Dazu gehört auch, direkt an das *Risiko Board* zu berichten. Es wäre daher naheliegend, dass diese Rolle jeweils einem *CISRM Beauftragten* zugewiesen wird.

6.3.4 Verantwortlichkeiten der Rollen

Nachdem nun die ISRM Rollen beschrieben und ihre Anwendbarkeit im kollaborativen Prozess untersucht wurde, gilt es nun die genauen Verantwortlichkeiten im CISRM zu formalisieren. Dazu werden die Rollen den Aktivitäten des generischen Prozesses (Abbildung 6.2) zugewiesen, genauer gesagt den vorher identifizierten Aktivitäten (Abschnitt 6.2). Dabei wurde bereits für jede Rolle diskutiert, welche konkrete Aufgabe sie im Prozess unterstützen kann. Bisher ist jedoch noch unklar, welche Rollen-/Rechtebeziehung zwischen den Akteuren besteht.

Zur strukturierten Darstellung dieser Beziehungen soll eine RACI-Matrix verwendet werden. Dabei handelt es sich um ein einfaches Werkzeug zur tabellarischen Auflistung von Aktivitäten, denen jeweils eine oder mehrere Verantwortlichkeiten zugewiesen wird. In der Basisversion[4] der Matrix existieren vier verschiedene Verantwortlichkeiten: RACI

Responsible Die Person trägt die Verantwortung zur Durchführung der Aktivität. Das enthält mindestens die Steuerung, die tatsächliche Tätigkeit kann delegiert werden. Bestenfalls sollte nur eine Person responsible sein.

Accountable Die Person trägt die rechtliche Gesamtverantwortung für die Aktivität, d.h. sie ist letztlich rechenschaftspflichtig für die Ergebnisse. Es darf nur genau eine Person accountable sein.

Consulted Eine beliebige Anzahl an Personen unterstützen mit ihrem Wissen oder ihren Fähigkeiten bei der Planung oder Umsetzung der Aktivität.

Informed Alle relevanten Stakeholder, die über den Verlauf oder die Ergebnisse der Aktivität informiert werden sollten.

Gemäß dieser Aufteilung wurden den Rollen die für sie relevanten Tätigkeiten in jeder Aktivität zugewiesen. Tabelle 6.1 zeigt die Verteilung der Rollen und Verantwortlichkeiten auf die verschiedenen Aufgaben. Das Ergebnis ist eine vollständige Übersicht über alle Akteure und seine Tätigkeiten im CISRM. Ergebnis

[4] Andere Varianten führen zusätzliche Verantwortlichkeiten ein, z.B. Supported in RASCI

Tabelle 6.1: RACI-Matrix der Rollen und Verantwortlichkeiten für alle Aufgaben im CISRM

	Projektmanager	Risiko Board	Risiko Manager	Steering Committee	Asset Owner	CISRM Beauftragter	Maßnahmen Owner	Risiko Manager	Risiko Owner
Aktivität/Aufgabe	Allianz				Organisation				
Kontext festlegen									
Anwendungsbereich der Allianz festlegen			R	A					C
Scope der Organisation festlegen			C		C	A		R	
Appetit der Allianz festlegen		R	C	A		I			I
Appetit der Organisation festlegen						C		R	A
Toleranz der Allianz festlegen		R	C	A		C			I
Toleranz der Organisation festlegen					I	C		R	A
Risiken einschätzen									
ISRM-Methode festlegen		A	R			C		I	
Identifizieren neuer Risiken					R			A	
Risiken bewerten					R	C		A	
Relevante Bedrohungen [...] auswählen					I	AR		C	
Informationen über Risiken austauschen			AR	I		I			
Risiken teilen			I	I		AR		C	
Risiken behandeln									
Akzeptanzschwelle für Risiken festlegen		R	C	A	I	C		I	I
Relevanz für die Allianz prüfen						A		R	
Risiko behandeln					R			A	
Risiko übermitteln		I	I			AR			
Behandlung freigeben		AR	C		I	C		I	
Behandlung umsetzen									
Steuerung von Projekten festlegen			C	AR		C		I	
Maßnahme koordinieren	AR						I		
Gemeinsame Maßnahme umsetzen	A						R		
Umsetzungsstatus melden	I		I			A	R		
Lokale Maßnahme umsetzen		I	I			I	AR		
Risikobehandlung abschließen		I	AR			C			
Risiken und Maßnahmen überwachen									
Bedrohungsmodell bereitstellen			AR		I	I		I	
Bedrohungen überwachen					R			A	
Überwachen lokaler Maßnahmen					A		R		
Mit Stakeholdern kommunizieren	I	I	A	I	I	R	I	I	I

6.4 Gesamtdarstellung des Prozesses

Nachdem in diesem Kapitel die Einzelteile eines kollaborativen Prozesses entwickelt wurden, sollen diese nun zu einem Prozessmodell zusammengefügt werden. Der kollaborative Prozess erweitert den generischen Prozess (Abbildung 6.2) um die Informationsflüsse, welche zum Etablieren der identifizierten kollaborativen Aktivitäten (Abschnitt 6.2) notwendig sind. Weiterhin werden die Rollen und Verantwortlichkeiten (Tabelle 6.1) in das vollständige Prozessmodell eingebaut. Auf diese Art wird ein Modell für einen kollaborativen Prozess entstehen, der die jeweiligen Aufgaben und Funktionen der Partner bei einem verteilten Vorgehen darstellt.

BPMN

Zur Darstellung des Gesamtprozesses wird die Modellierungssprache Business Process Model and Notation (BPMN) verwendet. Dabei handelt es sich um einen offenen Standard [221] zur Modellierung von (Geschäfts-)Prozessen. Dieser eignet sich besser als etwa UML, um komplexe Zusammenhänge mit verschiedenen Rollen und Organisationen zu modellieren. Insbesondere organisationsübergreifende Prozessschritte und Informationsflüsse sind in der Notation enthalten und leicht zu skizzieren. Dabei stehen drei verschiedene Modelltypen zur Auswahl. Das Konversationsdiagramm dient der einfachen Beschreibung der Teilnehmer einer einzelnen Geschäftsaktivität. Beim Choreografiediagramm liegt der Fokus auf dem Nachrichtenfluss dessen sequenziellem Ablauf. Letztlich soll das Kollaborationsdiagramm einen Prozessablauf unter Berücksichtigung verschiedener Teilnehmer (Organisationen, Akteure) darstellen. Damit ist am besten geeignet, um den kollaborativen Prozess mit verschiedenen Rollen zu modellieren. In diesem Diagramm werden verschiedene Organisation von Pools repräsentiert, die Swimlanes für jeden am Prozess beteiligten Akteur beinhalten. Die genutzten Elemente (Activities, Gateways, Events, Data und Flows) sind in Abbildung A.1 gelistet werden wie im Standard beschrieben verwendet.

Teilmodelle

Zuerst wurde für jede Aktivität ein eigenes Modell erstellt, um die verschiedenen Abläufe unabhängig voneinander strukturiert darzustellen (siehe Anhang A). Im nächsten Schritt folgte die Modellierung der Sub-Prozesse als ein sequentieller Prozess, wobei die Tasks den Hauptverantwortlichen aus Sicht der Allianz zugeordnet wurden. Anschließend konnte durch Aggregation der einzelnen Modelle ein durchgängiger Gesamtprozess erzeugt werden. Dabei unterscheiden sich die Teilmodelle und das Gesamtmodell insofern, als die einzelnen Teile als unabhängige Prozesse dargestellt, jedoch bei der Zusammenführung zusätzlich verknüpfende Elemente eingefügt wurden.

Prozessmodell

Das so entstandene vollständige Prozessmodell des CISRM mit organisationsübergreifenden Kommunikationsflüssen zwischen den Rollen und Aktivitäten ist in Abbildung 6.8 zu sehen. Die zwei Pools zeigen die Ansicht der Allianz und der beteiligten Partnerorganisationen. Darin enthalten sind Swimlanes für jede zur Partei gehörenden Rolle. Die Verantwortlichkeiten wurden gemäß der RACI-Matrix (Tabelle 6.1) dargestellt. Eine Aufgabe wurde jeweils der Rolle zugeordnet, welche die Durchführungsverantwortung (Responsible) für diese besitzt. Entscheidungen wurden durch Conditional-Events bei den Entscheidern (Accountable) abgebildet, z.B. beim Steering Comittee zu sehen. Unterstützende Rollen (Consulted, Informed) sind im Kollaborationsdiagramm nicht relevant und wurden auch zur besseren Übersichtlichkeit nicht explizit modelliert. Die Kommunikationsflüsse verlau-

fen dabei innerhalb der Organisation/Allianz, zwischen Organisation und Allianz, sowie zwischen der Organisation und anderen Partnern.

Inputs

Ebenfalls im Modell zu sehen sind die verschiedenen Inputs und Outputs der Aktivitäten/Aufgaben (Datenblatt). Eine Besonderheit sind die speziell gekennzeichneten Input-Dateien (Datenblatt mit weißem Pfeil), welche dem Prozess als externe Ressourcen bereitgestellt werden. Dabei handelt es sich um in der Analyse (Abschnitt 6.2) identifizierte Prozessparameter, welche der Allianz beim Etablieren des CISRM helfen. So ist es etwa sinnvoll, den Security-Reifegrad der verschiedenen Partner zu kennen, um den *Anwendungsbereich der Allianz festlegen* zu können. In derselben Aktivität *Kontext festlegen* muss jeder Teilnehmer den *Scope festlegen*, wobei ein gemeinsames Asset-Modell helfen kann. Sobald die Allianz die gemeinsame *ISRM-Methode festlegen* muss, kann eine Basismethode diesen Schritt erleichtern. Letztlich kann auch ein existierendes Bedrohungs-Schema dazu genutzt werden, wenn die Allianz ein *Bedrohungsmodell bereitstellen* soll und die Partner dieses später zum *Identifizieren neuer Risiken* nutzen wollen. Daher kann es sinnvoll sein, diese Parameter bereits als Implementierungshilfen für das CISRM zur Verfügung zu stellen. Im nächsten Kapitel werden daher diese vier Ressourcen genauer betrachtet, um sie als Teil des kollaborativen Frameworks zu standardisieren. Auch die Projektmanagementmethode ist in diesem Zusammenhang ein Input, da die Allianz hier auf existierende Standards zum organisationsübergreifenden Projektmanagement zurückgreifen kann (und sollte), welche allerdings nicht weiter betrachtet werden.

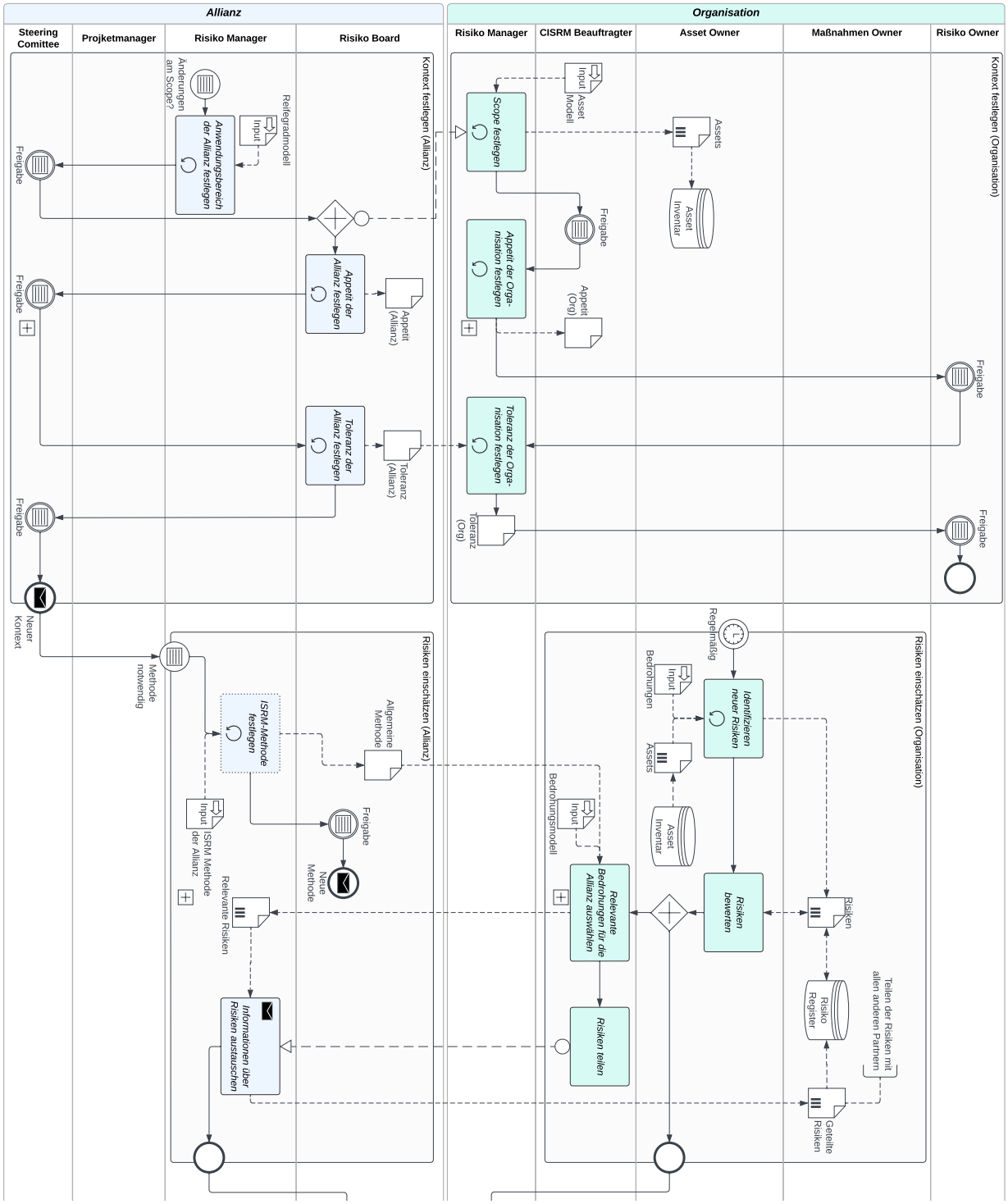
Prozessende

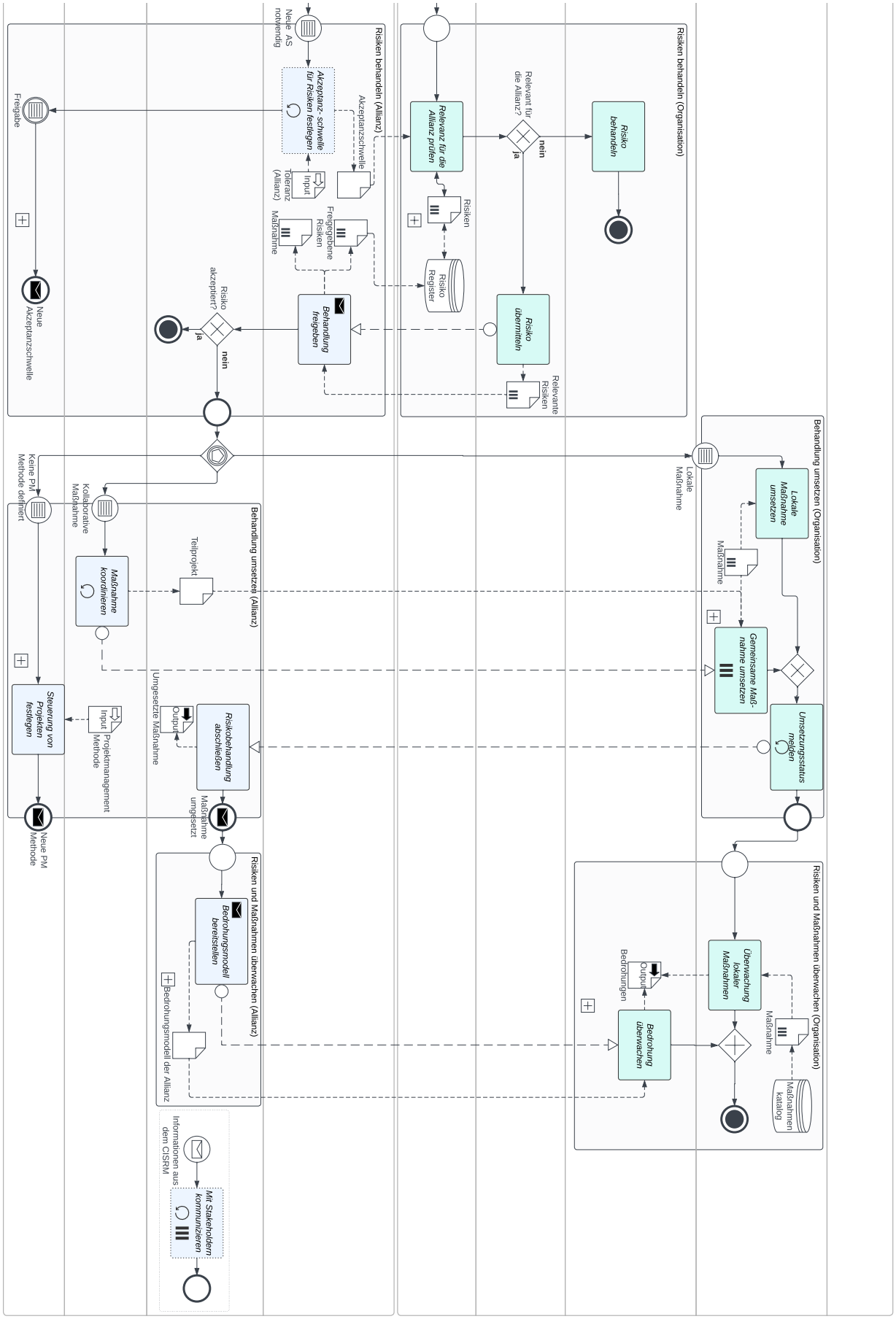
In der Aktivität Risiken behandeln gibt es zwei zusätzliche Endereignisse, die den Prozess vollständig terminieren. Der Erste findet sich nach der Überprüfung, ob ein Risiko für die Allianz überhaupt relevant ist. Zeigt sich dabei, dass dies nicht der Fall ist, da etwa die Risikoakzeptanzschwelle unterschritten ist oder die betroffenen Assets nicht im Scope sind, dann endet der kollaborative Prozess an dieser Stelle. Das Risiko wird unabhängig von der Organisation behandelt, d.h. es ist Teil des lokalen ERM jedoch nicht mehr des CISRM. Die zweite Stelle, an welcher der Prozess terminieren kann, ist nach Freigabe der Behandlungsoption. Hat sich das Risiko Board der Allianz für eine Akzeptanz des Risikos entschieden, dann wird dieses nicht weiter betrachtet. In beiden Fällen werden jedoch die bis dahin gesammelten Informationen an die Stakeholder kommuniziert, da sie den Organisationen bei der eigenen Risikoeinschätzung helfen können. Ansonsten endet der Prozess nach einem vollständigen Durchlauf aller Aktivitäten und beginnt anschließend erneut mit der regelmäßigen Risikobetrachtung.

Outputs

Der Prozess liefert drei für die Partner relevante Outputs. Zum einen sind es die Risikoinformationen, die in der Aktivität *Risiken einschätzen* von den Teilnehmern erzeugt und mit der Allianz geteilt werden. Diese können von jeder Organisation direkt als Input in das eigene ERM genutzt werden, unabhängig vom gemeinsamen Vorgehen. Die Allianz stellt damit eine *Sharing Community/Relationship* dar, welche zum *Threat Information Sharing* [44] genutzt werden kann, jedoch mit einer organisatorisch strategischen Perspektive. Ein weiterer Output sind gemeinsam behandelte Risiken (*Risiken behandeln*) bzw. die dabei implementierten Maßnahmen (*Behandlung umsetzen*). Im Gegensatz zum ISRM innerhalb der Organisation wird im CISRM versucht, Risiken möglichst gemeinsam zu behandeln. Langfristig sollen dadurch alle Teilnehmer von geteilten Ressourcen und

Abbildung 6.8: Vollständiges Prozessmodell des CISRM mit organisationsübergreifenden Kommunikationsflüssen zwischen den Rollen und Aktivitäten




Risiken behandeln (Organisation)
Risiko behandeln
Relevant für die Allianz?
nein
ja
Relevanz für die Allianz prüfen
Risiken
Risiko Register
Risiko übermitteln
Relevante Risiken
Risiken behandeln (Allianz)
Neue AS notwendig
Akzeptanz- schwelle für Risiken festlegen
Akzeptanzschwelle
Input
Toleranz (Allianz)
Freigegebene Risiken
Maßnahme
Behandlung freigeben
Risiko akzeptiert?
ja
nein
Freigabe
Neue Akzeptanzschwelle
Behandlung umsetzen (Organisation)
Lokale Maßnahme
Lokale Maßnahme umsetzen
Maßnahme
Gemeinsame Maß- nahme umsetzen
Umsetzungsstatus melden
Risiken und Maßnahmen überwachen (Organisation)
Überwachung lokaler Maßnahmen
Output
Bedrohungen
Bedrohung überwachen
Maßnahmen katalog
Keine PM Methode definiert
Kollaborative Maßnahme
Behandlung umsetzen (Allianz)
Maßnahme koordinieren
Teilprojekt
Steuerung von Projekten festlegen
Input
Projektmanagement Methode
Risikobehandlung abschließen
Output
Umgesetzte Maßnahme
Maßnahme umgesetzt
Neue PM Methode
Risiken und Maßnahmen überwachen (Allianz)
Bedrohungsmodell bereitstellen
Bedrohungsmodell der Allianz
Informationen aus dem CISRM
Mit Stakeholdern kommunizieren

vorhandenem Wissen profitieren, um Maßnahmen möglichst effektiv und ressourceneffizient zu etablieren. Letztlich sind auch die bewerteten Bedrohungen bzw. das gemeinsame Bedrohungsmodell der Allianz ein Output. Anders als die Risikoinformationen, geht es dabei nicht um das Teilen konkreter Risikoinformationen, sondern dem Erstellen eines gemeinsamen Lagebilds (Threat Modelling). Durch die Nähe der Organisationen zueinander kann ein gemeinsames Bedrohungsmodell die Situation aller Partner berücksichtigen und diesen in Summe mehr Informationen bereitstellen. Insgesamt liefern diese Outputs den Teilnehmern des CISRM einen Wissensvorsprung im Vergleich zu einer alleine agierende Organisation, welche vollständig auf die eigene Risikoeinschätzung und öffentliche Informationen zurückgreifen muss. Die gemeinsame Freigabe und Behandlung soll nicht nur Ressourcen besser verteilen, sondern auch das Sicherheitsniveau in der Allianz gleichmäßig erhöhen, wodurch die Teilnehmer eher vor SCRs geschützt sind.

Ergebnis

Bereits der aus den Frameworks abgeleitete, generische Prozess (Abbildung 6.2) kann großen Organisationen dabei helfen, ihr ISRM zu standardisieren. Er könnte isoliert genutzt dabei helfen, verschiedene ISRM Prozesse anzugleichen oder zu migrieren. Die Anwendung des kollaborativen Prozesses (Abbildung 6.8) hingegen liefert die Grundlage dafür, ein tatsächliches CISRM in einer Allianz aufzubauen. Insgesamt konnten in diesem Kapitel Teile der Forschungsfrage zur **Kommunikation** und **Kollaboration** beantwortet werden. Dabei wurden im Detail die folgenden Fragestellungen untersucht und diskutiert:

- Lässt sich auf Basis existierender ISRM-Frameworks ein allgemeiner Prozess ableiten, der als Grundlage für die Zusammenarbeit verwendet werden kann (Abschnitt 6.1)?
- Welche Aufgaben im ISRM könnten von einer kollaborativen Durchführung mit anderen Partnerorganisationen profitieren (Abschnitt 6.2)?
- Welche Rollen sind am ISRM beteiligt, welche Aufgaben übernehmen diese im CISRM und wie sollten die Verantwortlichkeiten zwischen den Organisationen und der Allianz aufgeteilt werden (Abschnitt 6.3)?
- Wie sieht ein vollständiger Prozess zum kollaborativen Umgang mit Risiken innerhalb der Allianz aus (Abschnitt 6.4)?

Theorie und Praxis

In der Analyse der Frameworks und ihrer Prozesse hat sich gezeigt, dass diese grundlegend die gleiche Struktur des ISRM definieren. Während sich die Literatur damit größtenteils einig zu sein scheint, wie das ISRM aufgebaut sein sollte, ist doch eine Diskrepanz zu der gelebten Praxis erkennbar. An einigen Stellen, etwa der Definition der Rollen, scheinen die Frameworks nicht den Stand widerzuspiegeln, der heute in vielen Organisationen umgesetzt wird. Vielleicht existiert hier allerdings auch noch kein Standard, der sich in der Industrie durchgesetzt hätte oder die Implementierung des Prozesses ist zu stark abhängig vom Kontext der Organisation. Diese Einsicht ist konsistent mit den Erkenntnissen von Olechowski et al. [222], die auch den Eindruck gewonnen haben, dass RM Literatur es bisher nicht geschafft hat bewährte Verfahren zu liefern, die synchron mit der gelebten Praxis sind. Dabei ist ihre Erklärung dafür, dass das RM (im Projektmanagement) oftmals nicht

strukturiert eingesetzt wird, ein fehlender Wirksamkeitsnachweis der Frameworks: „What results is an ad-hoc application of risk management processes, if there is any application at all; there is both a lack of legitimacy and a lack of unity towards one common best practice understanding.“ Unabhängig von der Ursache ist jedoch klar, dass das ISRM noch keinen Reifegrad erreicht hat, in dem es einen allgemeingültigen Industriestandard gibt, den Organisationen ‚off the shelf‘ implementieren könnten.

Ausblick

Das erstellte kollaborative Prozessmodell bildet gemeinsam mit der im letzten Kapitel vorgestellten Terminologie den Kern des CISRM Frameworks. Im Folgenden werden nun noch die zusätzlichen Informationen betrachtet, die als wertvolle Inputs in den Prozess identifiziert wurden. Dabei gilt es einfache Schemata für die Struktur eines Reifegradmodells, einer gemeinsamen Bewertungsmethode, einheitlicher Assetkategorien und eines anpassbaren Bedrohungsmodells zu erstellen. Diese ergänzen das Framework als unterstützende Ressourcen für den kollaborativen Prozess. Sie erlauben es den Organisationen ihre jeweiligen Risikoelemente (Assets, Bedrohungen, Risiken) vergleichbar zu machen und einen einfachen Mehrwert aus den gemeinsamen Informationen zu ziehen (CSF 6), wodurch sie letztlich das Teilen von Risikoinformationen (CSF 1) im Prozess erst ermöglichen.

Kapitel 7

Leitfaden zur Erstellung von geteilten Ressourcen

Inhaltsangabe

CISRM Prozess

Das vorherige Kapitel behandelte den Prozess des klassischen ISRM und zielte darauf ab, diesen so zu erweitern, dass er in einem interorganisationalen Kontext nutzbar wird. Durch die Analyse verschiedener Vorgehensweisen wurde dabei ein erweitertes Prozessmodell für das CISRM erstellt, welches existierende Modelle um spezifische Schnittstellen ergänzt. Diese Schnittstellen erweitern bestimmte Aktivitäten, sodass eine kollaborative Ausführung einzelner Aufgaben in der Allianz möglich wird. Durch veränderte Verantwortlichkeiten existierender ISRM Rollen und Definition einiger Neuer für das CISRM, konnten die Zuständigkeiten für die kollaborativen Aktivitäten klar zugewiesen werden. Durch diese klare Aufteilung, die per Design größtenteils kompatibel zu existierenden Prozessen und Verantwortlichkeiten ist, können Organisationen ihr existierendes ISRM nutzen und ein CISRM innerhalb der Allianz aufbauen.

Standardisierung

Das dazu definierte kollaborative Prozessmodell (Abbildung 6.8) kann grundsätzlich ohne weitere Hilfsmittel verwendet werden, um einen interorganisationalen Prozess innerhalb einer Allianz aufzubauen. Bei der Analyse der Prozesse und Diskussion der Aktivitäten (Abschnitt 6.2) ist jedoch aufgefallen, dass einige Prozesselemente für eine Kompatibilität der unabhängigen ISRM Prozesse formalisiert werden sollten. So erfordert bereits die Kommunikation von Risikoinformationen zwischen den Partnern einen gewissen Grad der Standardisierung, damit alle Parteien vergleichbare Informationen bereitstellen und die Datenbasis sinnvoll nutzen können. Bei Risiken bedeutet das insbesondere, dass sie auch inhaltlich miteinander vergleichbar sein sollten, damit sie einer anderen Organisation als dem Ersteller einen Mehrwert liefern. Das heißt, dass im CISRM mindestens eine Spezifikation der Kerndaten eines Risikos (Bedrohungen, Assets, Bewertungsmethode) notwendig ist. Die Allianz sollte sich daher beim Aufbau des gemeinsamen Prozesses auf die notwendigen Rahmendaten einigen.

Bedrohungen

Wie bereits in Kapitel 2 dargestellt, liefert die Grundlage für die Erstellung von Risiken immer eine Bedrohung und ein von dieser betroffenes Asset. Beide bilden damit die Basiselemente eines Risikos und sind somit essenziell, wenn es um den Austausch von Risikoinformationen geht. Eine Einzelorganisation kann für ihr ISRM dabei jede beliebige Bedrohung betrachten, die für sie sinnvoll erscheint. Sollen die bereitgestellten Risikoinformationen jedoch auch den anderen Partnern einen Mehrwert liefern, dann müssen die zugrundeliegenden Bedrohungen auch eine Relevanz für diese haben und miteinander vergleichbar sein (Abbildung 6.4). Weiterhin wurde im letzten Kapitel eingeführt, dass der Vorteil des CISRM nicht nur der Informationsaustausch, sondern insbesondere die gemeinsame Risikobehandlung ist (Abbildung 6.5). Auch dabei hilft der Organisation die gemeinsame Sicht auf die Bedrohungslage in Form eines Bedrohungsmodells für die Allianz (Abbildung 6.7). Dazu wird ebenfalls ein vergleichbarer Bedrohungskatalog benötigt, um diese zwischen den Partnern abzustimmen.

Assets

Die innerhalb der Allianz behandelten Risiken werden insbesondere dann relevant, wenn klar ist, welche Assets für die Allianz als Ganzes von Bedeutung sind. Somit ergibt sich auch der Bedarf von einheitlichen Asset-Kategorien innerhalb der Allianz. Bereits bei der ersten Aktivität, dem Festlegen des Kontexts (Abbildung 6.3) des CISRM, muss jeder Partner den Scope des eigenen ISRM festlegen. Dabei ist es entscheidend zu berücksichtigen, welche Assets nicht für ihn, sondern auch für die Allianz einen Wert haben könnten.

Es ist anzunehmen, dass die Organisationen zwar unterschiedliche Assets, aber ähnliche Assetklassen besitzen. Diese sind möglicherweise unterschiedlich definiert und strukturiert, weshalb eine Bedrohung in den Organisationen unterschiedliche Assets betrifft. Somit ist es für eine Organisation nicht möglich direkt festzustellen, wie sich das Risiko eines Partners auf die eigene Organisation auswirken würde. Auch hier wäre es für den Austausch der Risikoinformationen und die gemeinsame Risikobehandlung somit hilfreich, wenn sich die Assets der Partner vergleichen oder aufeinander abbilden lassen.

Methode

Am Ende der Risikoeinschätzung liegt die Bewertung des identifizierten Risikos. Dazu wird vorher eine Risikomethode definiert, die vom Grundsatz entweder quantitativ oder qualitativ ist, dabei jedoch beliebig ausgestaltet werden kann. Da jede Organisation bereits ihr eigenes ISRM etabliert hat, haben sie auch bereits eine Methode definiert, welche sich wahrscheinlich von denen der Partner unterscheidet. Somit ist die durchgeführte Risikobewertung der einzelnen Organisationen im Ergebnis schwer miteinander zu vergleichen. Jedoch ist es auch für die gemeinsamen Aktivitäten erforderlich, dass die ermittelte Risikohöhe innerhalb der Allianz nutzbar ist. Der für die gemeinsame Risikobehandlung festgelegte Schwellwert muss nicht einheitlich sein, jedoch mindestens für jeden Partner in das eigene Vorgehen übersetzbar sein. Die Allianz sollte daher bereits am Anfang eine gemeinsame Methode festlegen, welche von den Partnern genutzt werden kann ((Abbildung 6.4)).

Reifegrad

Ebenfalls ist es bereits im ersten Prozessschritt des CISRM notwendig, den Anwendungsbereich der Allianz festzulegen (Abbildung 6.3). Dabei sind klare Kriterien notwendig, um zu entscheiden, welche Partner in den gemeinsamen Prozess eingebunden werden. Es wurde etabliert, dass die Partner etwa den gleichen Reifegrad im ISM aufweisen sollten, damit alle beteiligten Organisationen vom gemeinsamen Vorgehen optimal profitieren. Das heißt, selbst wenn die Allianz als Ganzes die Grundvoraussetzungen für das gemeinsame Vorgehen erfüllt (Abbildung 4.4), sollte im ersten Schritt die inhaltliche Eignung geprüft werden. Somit sollte ein für die Allianz sinnvolles Reifegradmodell gewählt werden, dass die Partner zur Bewertung der eigenen ISM-Kompetenz nutzen können. Nur kompatible Partner sollten in das CISRM einbezogen werden, andere sollten einen vergleichbaren Reifegrad anstreben.

Framework

Die oben genannten Elemente stellen letztlich keinen Teil des CISRM Prozesses dar, sondern lediglich Inputs, die in den Prozess eingehen müssen. Jede Allianz muss diese letztlich selbst festlegen und zwischen den Partnern abstimmen. Dabei sollten insbesondere Aspekte wie Branche, Region oder Zweck der Allianz berücksichtigt werden. Im Rahmen des vollständigen CISRM Frameworks aus Abbildung 3.1, sollen jedoch ein grundlegendes Konzept bereitgestellt werden. Dieses liefert den Allianzen, die einen kollaborativen Prozess aufbauen wollen, ein Muster für die notwendigen Ressourcen.

Vorgehen

In diesem Kapitel sollen die genannten Ressourcen definiert werden, um sie als Teil des kollaborativen Frameworks bereitzustellen. Dies beinhaltet eine allgemeine Methode zur Risikobewertung sowie ein klares Schema für Assets und Bedrohungen. Weiterhin wird das Vorgehen zur Nutzung eines Reifegradmodells vorgestellt. Das Ergebnis vervollständigt das CISRM Framework mit optionalen Hilfsmitteln, die einer Allianz zu Verfügung stehen.

7.1 Bewertung des Sicherheitsniveaus der Partner

Die erste Aktivität, welche am Beginn des kollaborativen Prozesses steht, ist das *Kontext festlegen* (Abbildung 6.8). Darin enthalten ist die Aufgabe *Anwendungsbereich der Allianz festlegen*, die im Verantwortungsbereich der Allianz liegt. Der *Allianz Risiko Manager* ist für die Durchführung verantwortlich und liefert die notwendigen Vorarbeiten zur Entscheidung durch den *Lenkungsausschuss* (Tabelle 6.1). Das Ziel ist es, aus der Menge aller Partner diejenigen auszuwählen, mit denen ein wirksames CISRM aufgebaut werden kann.

ISM Reifegrad

Dabei wurde bereits etabliert, dass die Teilnehmer im CISRM auf die Partner mit einem vergleichbaren ISM-Reifegrad beschränkt werden sollte. Dieser Reifegrad ist ein sinnvolles Kriterium zur Auswahl der Partner, da der Austausch von Risikoinformationen und die gemeinsame Risikobehandlung sonst nicht immer sinnvolle Ergebnisse liefert. Die Partner versuchen durch das gemeinsame CISRM letztlich effizienter zu sein, als sie es alleine im ISRM wären. Trotzdem bleibt es natürlich weiterhin relevant, ein einheitliches Sicherheitsniveau innerhalb der Allianz zu etablieren. Dabei stellt sich sicherlich auch die Frage, ob eine Organisation mit einem deutlich geringen Reifegrad überhaupt Teil der einer kollaborativen Partnerschaft sein sollte, oder diese die Allianz eher in Gefahr bringt. Bei der Auswahl der Partner handelt es sich jedoch um eine strategische Entscheidung der Organisationen und die Bewertung einer IOR ist nicht teil dieser Arbeit.

Geringer Reifegrad

Ist der Reifegrad einer Organisation deutlich geringer als der der Gruppe, dann würden es dazu führen, dass das Bedrohungsmodell der Allianz mehr kritische Bedrohungen enthält, da der Partner weniger gut abgesichert ist. Weiterhin sind die von der Organisation geteilten Risikoinformationen für die restlichen Partner eventuell weniger relevant, da diese bereits vor vielen Risiken geschützt sind. Eine gemeinsame Methodik zu definieren, welche für alle Teilnehmer sinnvoll ist, gestaltet sich in diesem Fall als schwierig. Auf der anderen Seite ist anzunehmen, dass die von der Allianz geplanten Maßnahmen die schwächere Organisation überfordern würden, da ihr eventuell noch grundlegende Sicherheitsmaßnahmen fehlen. Somit ist davon auszugehen, dass Partner mit einem zu geringen Security-Reifegrad nicht am gemeinsamen CISRM teilnehmen sollten. Trotzdem gilt natürlich zu berücksichtigen, dass die Organisation innerhalb der Allianz eine wichtige Rolle einnimmt und ihre Assets trotzdem geschützt werden müssen. Schließlich war die Voraussetzung für das CISRM, dass es sich um eine kollaborative Beziehung (Kapitel 4) handelt, bei der die Teilnehmer von der gegenseitigen Zielerreichung abhängig sind. Somit ist der Ausschluss einer Organisation eventuell nicht zielführend. In diesem Fall sollte sich die Allianz darauf fokussieren, den schwachen Partner bei der Erhöhung des Reifegrades zu unterstützen.

Hoher Reifegrad

Dabei kann der gegenteilige Fall ebenfalls betrachtet werden. Hier ist der Security-Reifegrad einer Organisation deutlich höher als die der restlichen Allianz. In diesem Fall sind die vorherigen Argumente umgekehrt anwendbar und die Vor- und Nachteile verschieben sich. Es besteht hier die Möglichkeit, dass viele innerhalb der Allianz geteilten Risikoinformation für die Organisation nicht sonderlich relevant sind, da sie diese Risiken bereits alle betrachtet hat. Bei der gemeinsamen Risikobehandlung wird sie möglicherweise bereits viele Maßnahmen etabliert haben, die der Allianz helfen können. Sie kann damit ihren Wissens- oder Technologievorsprung mit den Partnern teilen.

7.1.1 Auswahl einer Bewertungsmethode

Im Bereich ISRM existieren bereits viele verschiedene Sicherheitsstandards, die klare Anforderungen an das ISM stellen. Das Problem dabei ist, dass diese Standards nur eine binäre Bewertung zulassen. Es kann meist nur die Aussage getroffen werden, ob eine Organisation konform oder nonkonform zum geforderten Standard ist. Eine quantitative Bewertung des Sicherheitsniveaus ist normalerweise nicht vorgesehen. Trotzdem kann die Auswahl der Partner natürlich auch auf dieser Basis erfolgen. Echte Reifegradmodelle zur Bewertung des ISM einer Organisation gibt es auf der anderen Seite nur wenige. Die existierenden betrachten meist eher allgemeine Geschäftsprozesse oder bestimmte Teilbereiche der IS wie die sichere Entwicklung. Auch in einem ISMS ist die Verwendung solcher Modelle aktuell nur im Kontext der kontinuierlichen Verbesserung einzelner Prozesse vorgesehen [223].

NIST CSF

Das NIST Cyber Security Framework (CSF) [224] liefert ein bekanntes und umfassendes Vorgehen, das Sicherheitsniveau einer Organisation schrittweise zu erhöhen. Das *Core Framework* enthält dabei eine Liste von Sicherheitsaktivitäten (andere Frameworks würden diese als Prozesse bezeichnen), welche in die fünf Funktionen *Identifizieren, Schützen, Detektieren, Reagieren und Wiederherstellen* aufgeteilt sind. Dabei wird insbesondere auf eine regelmäßige Selbsteinschätzung (Self Assessment) dieser Funktionen und Aktivitäten gesetzt. Grundsätzlich liefert das CSF auch die Möglichkeit, eine Organisation zu Bewerten und in Tiers von eins bis vier einzuteilen. Dies liefert jedoch nur eine grundsätzliche Übersicht über die Ausprägung des ISRM und es wird explizit darauf hingewiesen, dass es sich dabei nicht um Reifegrade handelt.

ISO 27001

Auch die bekannte ISO/IEC 27001 [12] setzt im Kern auf die kontinuierliche Verbesserung. Eine Organisation soll das Managementsystem etablieren und die Maßnahmen aus dem Anhang A umsetzen, zusätzlich zu etwaige Maßnahmen aus dem eigenen ISRM. Kontrolliert wird dieses System durch regelmäßige interne und externe Audits, bei denen ein Auditor die einzelnen Anforderungen der Norm prüft. Dieses Vorgehen ist nicht nur aufwendig, es liefert auch nur eine Aussage über die Compliance der Organisation zur ISO/IEC 27001, aber keine Aussage über ihren Reifegrad. Es ist nicht möglich anhand der Norm oder den Ergebnissen eines Audits zu sagen, ob zwei Organisationen ein vergleichbares Sicherheitsniveau haben. Trotzdem liefert sie eine Sammlung von Anforderungen und garantiert mindestens, dass eine Organisation alle notwendigen ISM-Prozesse etabliert hat.

C2M2

Eines der wenigen offenen IS Reifegradmodelle ist das Cybersecurity Capability Maturity Model (C2M2) [225]. Das Modell liefert eine große Sammlung an Anforderungen bzw. Sicherheitsmaßnahmen, die zu den meisten gängigen Standards kompatibel sind. Der Sicherheitsreifegrad wird dann in drei Stufen, den sogenannten „Maturity Indicator Levels“ abgebildet. Das Framework bietet ebenfalls eine sehr einfache Möglichkeit eine Selbsteinschätzung der Organisation durchzuführen. C2M2 ist sehr umfangreich und kann definitiv zur Einstufung der ISM-Reife verwendet werden, ist allerdings auch sehr komplex und könnte manche Allianz überfordern.

CCSMM

Das Community Cyber Security Maturity Model (CCSMM) wurde ursprünglich vom Center for Infrastructure Assurance and Security (CIAS) an der University of Texas at San Antonio (UTSA) entwickelt. Es bietet fünf Reifegradstufen, um das ISM Niveau einer Or-

ganisation zu bewerten. Dabei liegt der Fokus auf den Bereichen *Awareness, Information Sharing, Richtlinien und Planung*. Das Modell ist auf die Sektor-Kollaboration ausgerichtet und speziell auf die Anwendung in Sharing-Communities ausgelegt. Es eignet sich daher grundsätzlich gut für ein interorganisationales Vorgehen, ist auf der anderen Seite jedoch stark auf die Bindung zu US-Behörden ausgelegt.

Services

Weiterhin existieren viele Plattformen, welche die Bewertung des Sicherheitsniveaus einer Organisation mit den technischen Mitteln unterstützen. Eines der bekanntesten allgemeinen Reifegradmodelle ist etwa das Capability Maturity Model Integration (CMMI). Dieses erlaubt allerdings nur eine Bewertung der Reife von Prozessen. Es zwar Möglich, damit auch die Reife von Sicherheitsprozessen zu bewerten, allerdings nicht den Stand des ISM als solches. Eine exemplarische Entwicklung mit Fokus auf IS ist die CMMI Cybermaturity Platform von ISACA, welche die Einbindung der IS erlaubt. Auf Basis von CMMI erlaubt es die Auswertung der aktuellen Sicherheitsmaßnahmen und so die Ableitung eines Reifegrads. Dieses und ähnliche Tools können als Hilfsmittel genutzt werden, um den Reifegrad der Organisation zu bewerten.

Problematik

Obwohl unter den vorgestellten Frameworks sehr gute ISM Reifegradmodelle zu finden sind, ist auch deren Herkunft zu beachten. Bei allen vorgestellten Modellen handelt es sich um Publikationen von US-Organisationen, teilweise Behörden. Das stellt nicht grundsätzlich ein Problem dar, kann allerdings bei manchen internationalen Organisationen auf Widerstand stoßen. So hat sich etwa im GÉANT Projekt gezeigt, dass die Bereitschaft sich an US-Standards zu orientieren unter den NRENs eher gering. Ob diese Zurückhaltung begründet oder unbegründet ist spielt dabei eine untergeordnete Rolle, da die Akzeptanz der Partner bei einem kollaborativen Vorgehen notwendig ist. Dies gilt es bei Auswahl oder Erstellung eines Reifegradmodells zu berücksichtigen.

7.1.2 Essenzielle Sicherheitsbereiche

Grundsätzlich kann jedes beliebige Framework zur Eingrenzung des Scopes im CISRM verwendet werden. Haufe [223] definiert zwei Hauptkriterien für ein Reifegradmodell in einem ISMS, die dabei berücksichtigt werden sollten: (1) es sollte für alle Organisationen geeignet sein, unabhängig von ihrer Größe, ihren Zielen, ihrem Geschäftsmodell, ihrem Standort und ähnlichen Eigenschaften; (2) es ist international anerkannt und ermöglicht eine internationale Akzeptanz der später entwickelten Methode zur Bestimmung des erforderlichen Reifegrads. Gleichzeitig steht es der Allianz jedoch auch frei, die für sie relevanten Kriterien komplett selbst festzulegen. Dabei liefert etwa die *ISO/IEC 33004* [226] Anforderungen zur Erstellung eines Reifegradmodells. Der vorgestellte kollaborative Prozess ist Framework agnostisch, so das der Ursprung der Kriterien keine Rolle spielt. Dementsprechend kann eine Allianz jedes für sie sinnvolle Verfahren einsetzen, um die Teilnahmebedingungen am gemeinsamen CISRM zu definieren. Ein bereits existierendes und in der Allianz etabliertes Modell ist dabei zu bevorzugen, insbesondere wenn es die Besonderheiten der Organisationen und Branche berücksichtigt. Als eine Grundlage werden im Folgenden die essenziellen Sicherheitsbereiche genannt, die bei der Bewertung des Sicherheitsniveaus der Partner zu berücksichtigen sind.

Security Baseline

Aufgrund der mangelnden Anwendbarkeit der existierenden Frameworks wurde im Rahmen des GÉANT Projektes (bekannt aus Kapitel 3.2) ein eigenes ISM-Reifegradmodell entwickelt. Dieses Reifegradmodell und seine Verbindung zu anderen Standards und Regularien wurde bereits zuvor im Forschungsartikel „Leveraging Taxonomical Engineering for Security Baseline Compliance in International Regulatory Frameworks“ [227] beschrieben (die vollständige Architektur der Security Baseline ist in Abbildung B.1 zu sehen). Das Ziel war es, ein leichtgewichtiges Reifegradmodell zu entwickeln, um ein minimales Sicherheitslevel innerhalb der Allianz festzulegen und das Sicherheitsniveau der Partner vergleichbar zu machen. Entstanden ist dabei ein einfaches und trotzdem umfassendes Reifegradmodell, die Security Baseline [156]. Obwohl die Baseline spezifisch für den R&E Sektor entwickelt wurde, entstammen die dabei identifizierten Sicherheitskategorien aus einer Abstraktion existierender Standards und den praktischen Erfahrungen der teilnehmenden Organisationen. Dabei ergaben sich generische Sicherheitskategorien und Bereiche, welche als allgemeines Schema bei der Evaluation der ISM-Reife genutzt werden.

Kategorien

Abbildung 7.1 listet die Bereiche und Kategorien, die als entscheidend für die Bewertung des Sicherheitsniveaus identifiziert wurden. Es wurden vier essenzielle Bereiche identifiziert, welche für das ISM im Allgemeinen relevant sind: Richtlinien, Menschen, Bedrohungen und Betrieb. Diese Kategorien sind in fast allen Sicherheitsstandards existent, auch wenn sie oftmals anderes benannt oder durch spezifische Schwerpunkte abgewandelt wurden. Auch die neue Version der ISO/IEC 27001 [228] die im Jahr 2022 veröffentlicht wurde, verwendet nun mit den Bereichen „Organisational, People, Physical, Technological“ eine sehr ähnliche Struktur[1]. Eine Organisation sollte bei der Bewertung des Sicherheitsniveaus einer Organisation alle Aspekte berücksichtigen:

1. **Richtlinien**
   Die erste Kategorie enthält die Themen Führung und Steuerung der IS, welcher aus vier Themenblöcken besteht. Der wichtigste Faktor für ein erfolgreiches ISM stellt die Einbindung der obersten Leitung dar, um die notwendigen Regelungen in der Organisation zu etablieren. Diese Regelungen werden durch Sicherheitsrichtlinien abgebildet und geben den Rahmen für alle Aktivitäten in der Organisation vor. Abgeleitet von der allgemeinen Informationssicherheitsrichtlinien liefert eine die Richtlinie den Umgang mit Informationen und Technologien. Letztlich muss eine Organisation nicht nur die Regelungen festlegen und einhalten, die sie sich selbst auferlegt, sondern insbesondere externe Regularien.

2. **Menschen**
   Die zweite Kategorie beschäftigt sich mit dem wichtigsten Element für das ISM, den beteiligten Personen innerhalb und außerhalb der Organisation. Um sichere Prozesse aufzubauen und IS-Vorfälle zu vermeiden, muss das Personal und auch externe Personen entsprechend sensibilisiert und für ihre Aufgaben geschult sein. Dabei ist

[1] Zum Zeitpunkt der Erarbeitung der Kategorien im GÉANT Projekt war diese Einteilung noch spezifisch für die Security Baseline. Die inzwischen erfolgte Neuauflage der ISO/IEC 27001 mit ähnlicher Struktur bestätigen die Ergebnisse größtenteils

es genauso wichtig, dass bereits bei der Einstellung die Sicherheitsrichtlinien eingehalten und die neuen Beschäftigten entsprechend eingewiesen werden. Letztlich sind dabei nicht nur interne Personen, sondern auch die externen Dienstleister zu berücksichtigen und ein sicheres Netzwerk zu etablieren.

3. **Bedrohungen**
   Die dritte Kategorie enthält den umfassenden Umfang mit allen Arten von Bedrohungen für die Organisation. Dabei ist steht das interne ISRM natürlich im Zentrum und muss sicherstellen, dass das die Organisation in der Lage ist, Risiken zu erkenne und diese zu behandeln. Realisiert sich ein Risiko dennoch, dann muss die Organisation einen schnellen und effektiven Umgang mit den resultierenden Vorfällen gewährleisten. Letztlich muss die Organisation auch auf kritische Vorfälle vorbereitet sein und ihren Geschäftsbetrieb weiterlaufen lassen können.

4. **Betrieb**
   Die vierte Kategorie beschäftigt sich schließlich mit dem Betrieb der Organisation, insbesondere der dazu notwendigen Technologie. Grundsätzlich muss die Organisation die eigene Infrastruktur angemessen absichern können. Dabei können verschiedenste kryptografische Maßnahmen helfen, gespeicherte und übertragene Daten zu schützen. Es gilt außerdem den Zugriff auf alle Systeme so zu konfigurieren, dass unbefugter Zutritt verhindert wird. Diese und andere Sicherheitsmaßnahmen sind dabei nur wirksam, wenn die genutzte Software immer auf dem aktuellen Stand ist und Patches zeitnah eingespielt werden. Dazu ist es wiederum unerlässlich, dass die Organisation ein Vorgehen etabliert hat, um neue Schwachstellen zu identifizieren und schnell zu beheben.

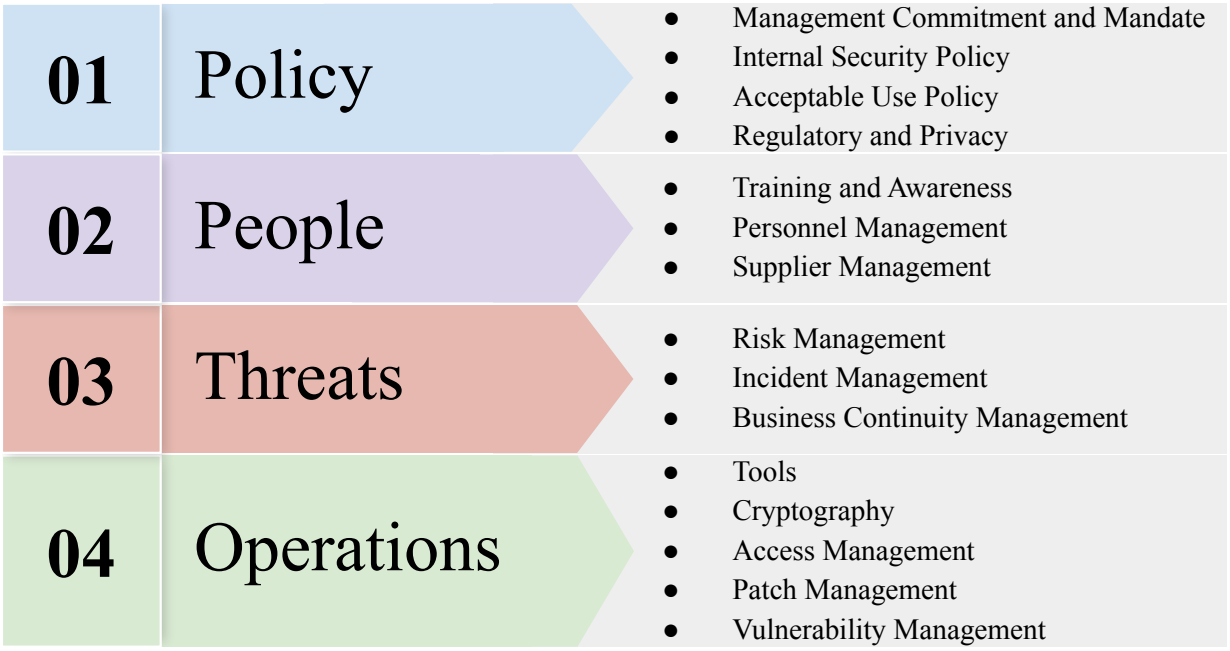
Vorgehen

Alle oben vorgestellten Kategorien und Unterbereiche sind essenziell für das ISM und sollten daher berücksichtigt werden, wenn die IS-Reife eines Partners bewertet wird. Die Festlegung und Messung des konkreten Reifegrads pro Kategorie erfolgt dabei durch die Allianz. Zur Evaluation kann ein beliebiges Modell genutzt oder auch eigene Kriterien definiert werden. Eine Variation verschiedener Standards und Modelle ist ebenfalls denkbar, solange alle genannten Bereiche einbezogen werden. Letztlich soll die Reifegradbewertung zu Beginn des CISRM Prozesses zwei Dinge zeigen. Erstens, ob bei den Partnern ein angemessenes ISM etabliert ist, so das er in der Lage ist sinnvolle Risiken zu formulieren. Zweitens, ob das Sicherheitsniveau vergleichbar zu dem der restlichen Allianz ist, damit alle Partner vom gemeinsamen Vorgehen profitieren können. Eine verbreitete Möglichkeit zur Abfrage der Reife der Partner ist dabei die Selbstauskunft.

Self-Assessment

Bereits die existierenden Reifegradmodelle setzen allesamt auf die Selbsteinschätzung als zentrale Bewertungsmethode. Im Gegensatz zur Konformitätsprüfung der Standards, bei denen die Prüfungen meist auf Stichproben basieren, werden dabei konkrete Bewertungskriterien bereitgestellt. Diese erlauben es Security Managern, den Reifegrad ihrer Organisation selbständig zu evaluieren, ohne dabei auf die subjektive Einschätzung zusätzlicher Auditoren zurückgreifen zu müssen. Das Ziel dieser Selbsteinschätzung ist dabei natürlich auch ein anderes als bei einer Konformitätsprüfung, da hier keine verbindliche Aussage

Abbildung 7.1: RS-1 Kategorien für die Reifegradbewertung [In Anlehnung an 156]



(im Sinne eines Lieferantenaudits) gegenüber Dritten getroffen werden soll, sondern die Ergebnisse der einen Messung dienen. Im Kontext der interorganisationalen Zusammenarbeit scheint dies ausreichen zu sein. Das notwendige Vertrauen zwischen den Partnern ist in einer kollaborativen Beziehung (Vertrauen in den guten Willen, Abbildung 4.4) bereits vorhanden, weshalb die Allianz auf die Ergebnisse einer Selbstauskunft vertrauen können. Die Ergebnisse der Selbsteinschätzung der Partner müssen dann verglichen werden, um zu ermitteln, ob das Sicherheitsniveau der Partner vergleichbar ist. Es kann sinnvoll sein, eine klare Grenze festzulegen, ab der die Zusammenarbeit im CISRM sinnvoll erscheint. Diese hängt jedoch stark von der Organisation und der Art ihrer Zusammenarbeit ab und ist daher eine Einzelfallentscheidung. Stellt sich nach der Prüfung heraus, dass eine oder mehrere Partner nicht den notwendigen Reifegrad für eine Zusammenarbeit besitzen, dann liegt es ebenfalls an der Allianz zu entscheiden, wie sie damit umgehen wollen. Entscheidung

Es wird allerdings empfohlen, erst in die kontinuierliche Verbesserung des ISM zu investieren. Die Allianz sollte auf ein ähnliches Sicherheitsniveau aller Partner hinzuwirken, um maximal von einem gemeinsamen Prozess zu profitieren. Schmidt und Mizani [165] zeigen dabei, wie auch andere ISM Prozesse und insbesondere der IS-Verbesserungsprozess in IORs genutzt werden können, um das Sicherheitsmanagement jeder Organisation durch die Zusammenarbeit zu stärken. Letztlich steht es der Allianz jedoch frei, jede beliebige Organisation einzubeziehen, wenn dafür ein weniger wirksamer Prozess von allen Partnern hingenommen wird. Verbesserung

7.2 Klassifikation von Bedrohungen

Bereits in der zweiten Aktivität des kollaborativen Prozesses *Risiken einschätzen* (Abbildung 6.8) geht es um die Erfassung und Bewertung neuer Risiken. Die erste Aufgabe *Identifizieren neuer Risiken* wird dabei verteilt von den Partnern im lokalen ISRM durchgeführt. Das Ergebnis bildet sowohl die Grundlage für den Austausch von Bedrohungsinformationen in der Aufgabe *Informationen über Risiken austauschen* als auch deren spätere Auswahl für die Behandlung. Relevante Risiken sind insbesondere solche, welche die Allianz als Ganzes bedrohen oder die auch andere Partner betreffen können. Somit basiert die Auswahl auf der vorangegangenen Aufgabe *Relevante Bedrohungen für die Allianz auswählen*. Wie in Abschnitt 6.2 diskutiert, setzt diese Aufgabe voraus, dass die identifizierten Risiken der Partner grundsätzlich miteinander vergleichbar sind. Am Ende des Prozesses steht weiterhin die Aktivität *Risiken und Maßnahmen überwachen*, bei der die Wirksamkeit der existierenden Maßnahmen und das Bedrohungslevel der Allianz geprüft wird. Eine identifizierte Möglichkeit, wie das CISRM einen Vorteil liefern kann, ist die Aufgabe *Bedrohungsmodell bereitstellen*. Auch diese erfordert, dass sich die Allianz grundsätzlich auf ein vergleichbares Bedrohungsmodell geeinigt hat. Aus diesem Grund sind die Bedrohungen ein Input in den kollaborativen Prozess, auf den sich die Allianz zur bestmöglichen Performanz einigen sollte[2].

Anforderungen an Bedrohungen

Ziel dieses Abschnitts ist es, ein generisches Bedrohungsmodell zu beschreiben. Dieses kann von der Allianz adaptiert werden, um vom gegenseitigen Informationsaustausch zu profitieren und die Risikoeinschätzung auf die Partner anzupassen (CSF 6). Die ist ein weiterer Baustein dafür, dass die Risiken der Partner zu vergleichbaren Risiken führen ((CSF 1)). Dabei ist es wichtig, den Partnern weiterhin die notwendige Freiheit bei der Durchführung ihrer internen Prozesse zu ermöglichen (CSF 5). Somit sollte auch die Auswahl der Bedrohungen nicht eingeschränkt und den Partnern ermöglicht werden, den für sie passenden Satz an Bedrohungen zu betrachten.

Klassifikation von Bedrohungen

Heute steht jeder Organisation bereits eine Auswahl an verschiedenen Bedrohungskatalogen zur Verfügung, die für das eigene ISRM genutzt werden können. Somit muss nicht jede Organisation bei Null starten, sondern kann auf existierendes Wissen in diesem Bereich zurückgreifen. Dies ist selbst dann von Vorteil, wenn die Organisation eine große Expertise im Bereich IS besitzt, da insbesondere Experten oftmals ihre eigenen Erfahrungen berücksichtigen, aber nicht die sich wandelnden Bedrohungsvektoren [229]. Im CISRM spielt es für den vorgestellten Prozess letztlich keine Rolle, welches Grundlage den Input für die Bedrohungen liefert. Dementsprechend wird an dieser Stelle nur eine kurze Übersicht über verschiedene etablierte Ressourcen geliefert. Wichtig für das kollaborative Vorgehen ist stattdessen, wie die verschiedenen Bedrohungen letztlich aufeinander abgebildet werden können. Dazu wird ein Klassifizierungsmodell für Bedrohungen vorgestellt und erklärt, wie dieses genutzt werden kann, um Bedrohungen zu standardisieren und relevante Bedrohungen für die Allianz auszuwählen.

[2]Es ist trotzdem denkbar, dass die Partner unterschiedliche Bedrohungen betrachten und den Prozessinput nicht angleichen, wenn sie die schlechtere Vergleichbarkeit der Risikoinformationen akzeptieren.

7.2.1 Typische Bedrohungen

Verschiedene Organisationen stellen verschiedenste Bedrohungskataloge bereit, die von den Partnern als Grundlage ihres ISRM verwendet werden können. Staatliche Behörden erstellen dabei meist generische Kataloge, welche für alle Arten von Organisationen und Branchen anwendbar sind. Spezialisierte Unternehmen oder Branchenverbände nutzen diese wiederum, um die Bedrohungen auf ihre jeweilige Zielgruppe anzupassen. Beide Arten von Katalogen haben ihre Relevanz und verschiedene Vorteile. Die Vorteile bei der Nutzung unterscheiden sich dabei zwischen IS Experten und Personen mit wenig Erfahrung, wobei für letztere gerade die spezialisierten Kataloge bei der Analyse hilfreich sind [230, 229]. Im Folgenden werden einige der häufig verwendeten generischen Kataloge vorgestellt.

BSI

Die BSI Gefährdungskataloge des IT-Grundschutz [52] sind eine (in Deutschland) häufig genutzte Quelle, um auf ihrer Basis eine Risikoanalyse durchzuführen. Insbesondere die elementaren Gefährdungen [231] liefern eine ausführliche Liste grundlegender Bedrohungen, welche von jeder Organisation berücksichtigt werden sollten. Der Katalog listet insgesamt 47 elementare Gefährdungen in verschiedenen Kategorien, die auf die meisten Organisationen zutreffen sollten.

ENISA

Im europäischen Raum zählt die ENISA zu einer der wichtigsten Instanzen zur Veröffentlichung von Bedrohungsanalysen. Ihre Threat Taxonomy [65] enthält ähnlich zu den deutschen Gefährdungskatalogen eine umfassende Liste von Bedrohungen aus verschiedensten Kategorien. Der jährlich erscheinende Threat Landscape Report [232] untersucht regelmäßig die Häufigkeit der Bedrohungen in verschiedenen Sektoren. Die Threat Taxonomy liefert insgesamt 184 generische Bedrohungen in sieben Kategorien.

NIST

Im angelsächsischen Raum liefert die NIST 800-30 [105] im Anhang D *Threat Sources* eine Übersicht über verschiedene Bedrohungsquellen und im Anhang E *Threat Events* die zugehörigen Bedrohungen. Die Bedrohungsquellen werden in vier Kategorien aufgeteilt mit 12 übergeordneten Akteuren. Insgesamt liefert das Framework 102 größtenteils technische Bedrohungen, wobei auch einige Umgebungsbezogene Bedrohungen berücksichtigt werden.

ISO

International enthält auch die ISO/IEC 27005 [98] eine Beispielliste typischer Bedrohungen für das ISRM. Die 43 enthaltenen Bedrohungen sind aufgeteilt in acht verschiedene Kategorien, die sowohl technische als auch umgebungsbezogene Bedrohungen beinhalten. Auch die ISO listet fünf verschiedene Bedrohungsquellen, welche als Auslöser für die Bedrohungen infrage kommen.

Auswahl

Jeder dieser Bedrohungskataloge ist grundsätzlich geeignet, um ihn im CISRM einzusetzen. Wie der Überblick zeigt, weichen die verschiedenen Frameworks bei der Definition der Bedrohungen nicht zu stark voneinander ab. Die verschiedenen Bedrohungen sind oftmals sehr ähnlich und unterscheiden sich eher in der Terminologie als im Inhalt. Deutlicher werden diese Unterschiede bei branchenspezifischen Katalogen. Trotzdem bleibt die Frage, wie sich die Bedrohungen zweier Kataloge direkt aufeinander abbilden lassen.

7.2.2 Modellierung der Bedrohungen

Im CISRM soll es jedem Partner ermöglicht werden, einen Bedrohungskatalog seiner Wahl zu nutzen. Werden jedoch die Risikoinformationen innerhalb der Allianz geteilt, stehen die Partner vor der Herausforderung, die gewonnen Informationen in das eigene ISRM zu integrieren. Je größer das Risikoverzeichnis einer Organisation ist, desto aufwändiger wird auch der Vergleich von verschiedenen Risiken miteinander.

Mapping

Dabei ist das Vorgehen zur Identifikation von Risiken immer gleich. Jedes Risiko wird von einer Bedrohung verursacht, die in ihrer Art auch die Auswirkung des Risikos bestimmt (Abbildung 5.2). Die Auswirkung ist damit im Gegensatz zu einer spezifischen Bedrohung generisch. Somit ist die Auswirkung einer Bedrohung auch die relevante Information, um verschiedene Risiken aufeinander abzubilden.

Modell

Ein generisches Klassifizierungsmodell zur Einordnung von Bedrohungen in verschiedene Kategorien wurde von Jouini et al. [63] zur entwickelt. Sie klassifizieren eine Bedrohung dabei anhand von fünf Dimensionen:

1. **Quelle der Bedrohung**
   Eine Bedrohung kann entweder eine interne (innerhalb der Organisation) oder externe (außerhalb der Organisation) Ursache besitzen.

2. **Auslöser der Bedrohung**
   Der Auslöser der schadhaften Aktion kann entweder menschlich, umweltbezogener oder technologischer Natur sein.

3. **Motivation des Angreifers**
   Bei einem menschlichen Angreifer kann weiterhin unterschieden werden, ob diese die schadhafte Aktion böswillig oder nicht-böswillig ausführt.

4. **Intention des Angreifers**
   Unabhängig von der Motivation kann eine Aktion durch einen Angreifer sowohl beabsichtigt als auch unbeabsichtigt gestartet werden.

5. **Auswirkung der Bedrohung**
   Letztlich führt das schadhafte Ereignis zu einer bestimmten negativen Auswirkung.

Auswirkungen

Das Modell von Jouini et al. [63] wurde später in der Arbeit[3] „Bedrohungsmodellierung im Kontext Informationssicherheit“ [233] weiterentwickelt und um zusätzliche Aspekte erweitert. Dabei wurden die Ausprägungen der Auswirkung leicht modifiziert. Während in der ursprünglichen Version sechs Dimensionen vorgeschlagen wurden, werden diese auf fünf reduziert. Dies betrifft sowohl die *Illegale Verwendung* als auch die *Rechteerweiterung*, da diese selbst noch keine Auswirkung einer Bedrohung darstellen. Es handelt sich lediglich um eine Vorstufe davon, bei der etwa eine Rechteerweiterung wieder zur *Zerstörung, Verfälschung, Diebstahl oder Offenlegung von Informationen* führen kann. Die restlichen

[3]Studentische Abschlussarbeit, die im Kontext des Promotionsvorhabens betreut wurde. Es wird auf die Originalergebnisse in Anhang B verwiesen.

Dimensionen orientieren sich an den fünf Typen von Auswirkungen aus der ISO/IEC 7498 [234]. Diese beziehen allerdings zusätzlich noch Ressourcen mit ein, während Jouini et al. [63] sich auf Informationen fokussiert. Während der Fokus eines ISMS klar auf dem Schutz der Informationen besteht, sollten auch potenzielle Schäden an anderen Ressourcen der Organisation nicht vollständig ausgelassen werden.

Klassifikationsmodell

Das adaptierte Modell zur Klassifikation von Bedrohungen ist in Abbildung 7.2 zu sehen. Es zeigt die fünf Dimensionen einer Bedrohung, die letztlich zu den immer gleichen Auswirkungen führen können. Dabei wurde jeder Auswirkung zusätzlich eines der drei IS Schutzziele (CIA) zugeordnet (Tabelle B.1). Das Klassifizierungsmodell ermöglicht eine einfache Zuordnung einer Bedrohung zu einer von fünf Auswirkungen, indem das Modell von links nach rechts durchlaufen wird. Somit erlaubt das Modell, verschiedene konkrete Bedrohungen wie z.B. Feuer oder Sabotage einer generischen Auswirkung zuzuordnen.

Dimensionen

Die verschiedenen Dimensionen des Modells können nun zur einfachen Referenz einer Bedrohung verwendet werden. Dazu wird eine Klasse als Listenobjekt dargestellt (Tabelle B.2), welche den Pfad durch die Dimensionen abbilden. So beschreibt etwa das 5-Tupel [ex,me,nb,ve,of] eine Bedrohung mit externer Quelle und menschlichem Auslöser, die nichtböswillig und unbeabsichtigt verursacht wurde und zu einer Offenlegung von Informationen führt. Auf diese Weise ist es nun möglich, jede beliebige Bedrohung durch ein solches generisches Objekt zu beschreiben. Dadurch entfällt letztlich die Notwendigkeit eines einheitlichen Bedrohungskatalogs in der Allianz.

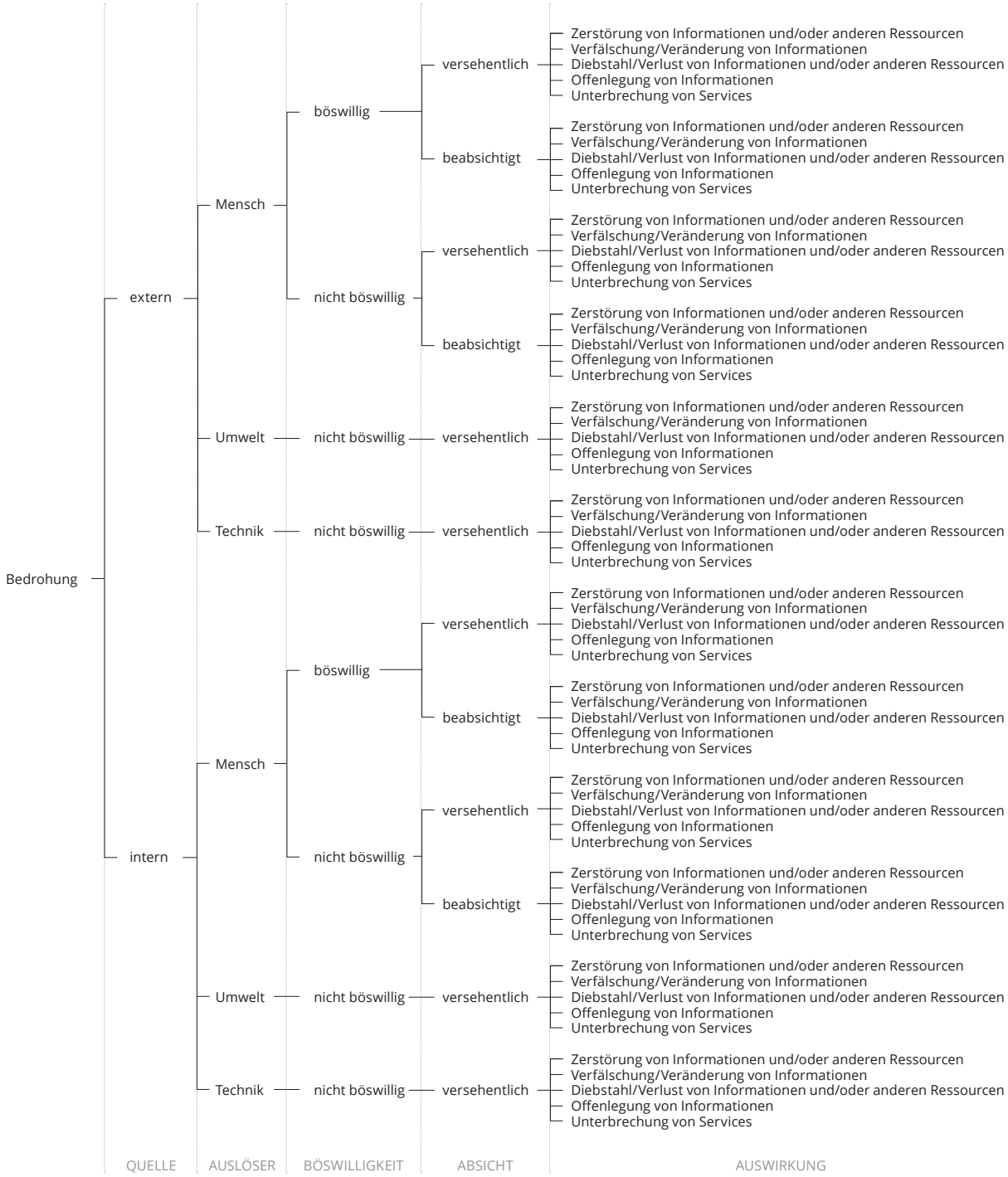
Auswahl von Bedrohungen

Die Allianz kann dieses Vorgehen nun zur Auswahl relevanter Bedrohungen nutzen. So können sich die Partner bereits beim Festlegen des Scopes darauf einigen, einzelne für sie nicht relevante Auswirkungen auszuschließen. Es wäre zum Beispiel denkbar, dass sich die Allianz nicht mit der Serviceerbringung beschäftigen will, da die Services der Organisationen zu unterschiedlich sind und diese keine Relevanz für die Partner haben. In diesem Fall würde man die Auswirkung *Unterbrechung von Services* komplett ausschließen und alle Bedrohungen mit dieser Auswirkungen werden zukünftig nicht mehr kommuniziert. Obwohl dies eine Möglichkeit ist, erscheint es wahrscheinlicher, dass eine Allianz anstatt einer Auswirkung einzelne Pfade ausschließt. So macht etwa das Teilen von umweltbezogenen Risiken hauptsächlich dann Sinn, wenn die Partner auch eine geografische Nähe zueinander haben, um von den gleichen Bedrohungen betroffen zu sein. Ist dies nicht der Fall, könnte die Allianz daher den Auslöser Umwelt ausschließen. Letztlich liegt es an der Allianz im Rahmen der Aktivität *Kontext festlegen* zu entscheiden, welche der Kategorien für sie sinnvoll sind.

Nutzung durch die Partner

Das Modell steht den Partnern in der Aktivität *Risiken einschätzen* bereit, um relevante Bedrohungen auszuwählen und die zugehörigen *Risiken teilen* zu können. Aufgabe der Allianz ist es, diese *Informationen über Risiken austauschen* zu können. Die Partner nutzen an dieser Stelle nun das Modell zum Mapping der eigenen Bedrohungen, um den Austausch von Risikoinformationen und die spätere Bewertung zu vereinfachen. Zur Identifikation von Risiken können die Partner dabei einen beliebigen Bedrohungskatalog als Basis wählen, wie im vorherigen Abschnitt beschrieben, welcher als Grundlage ihres internen ISRM dient. Zum Teilen der Risikoinformationen muss der verantwortliche Risikomanager lediglich der Bedrohung mit Hilfe des Modells ein 5-Tupel zuweisen, welches diese kategorisiert.

Abbildung 7.2: Klassifizierungsmodell für Bedrohungen [Original 233, In Anlehnung an 63]

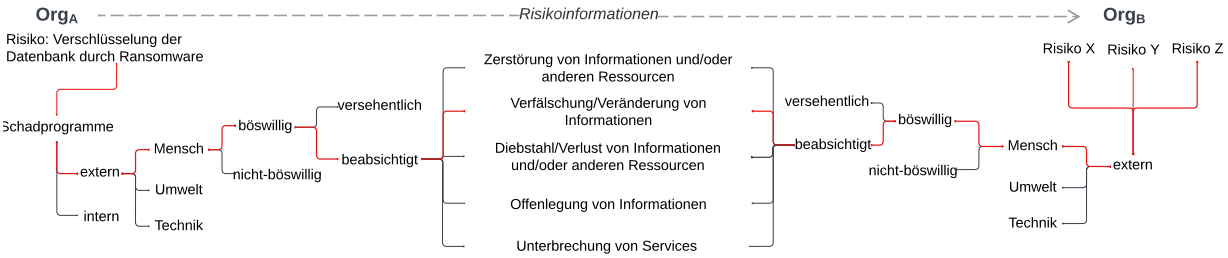


Mit der gleichen Methode können die geteilten Risikoinformationen nun analysiert werden, um herauszufinden, ob die Organisation dieses oder ähnliche Bedrohungen bereits bewertet hat. Ohne dieses Mapping wäre es für die Partner schwer die verschiedenen Risiken aufeinander abzubilden, insbesondere wenn diese bereits über ein umfangreiches Risikoverzeichnis verfügen.

Beispiel

Abbildung 7.3 zeigt dazu ein simples Beispiel, wie die Informationsübertragung stattfinden kann. Organisation A nutzt den Gefährdungskatalog des IT-Grundschutz [52]. Durch Analyse der Bedrohung *G0.39 Schadprogramme* identifiziert sie darin das Risiko *Verschlüsselung der Datenbank durch Ransomware*. Durch die Klassifikation mit Hilfe des Modells erhält sie eine extern verursachte Bedrohung mit menschlichem Auslöser, die böswillig und beabsichtigt zu einer Verfälschung/Veränderung von Information führt. Organisation B nutzt die ENISA Threat Taxonomy [65]. Durch Durchlaufen des Modells lässt sich dies auf verschiedene Bedrohungen aus diesem Katalog zuordnen, insbesondere *107 Malicious code/software/activity*. Somit kann Organisation B nun problemlos prüfen, ob sie bereits relevante Risiken identifiziert hat oder ob die erhaltenen Informationen die Bewertung verbessern können. Generell können alle Partner auf diese Weise die geteilten Risiken den eigenen Bedrohungen zuordnen. Dabei reicht es aus, die Modellierung einmal zu Beginn für den eigenen Bedrohungskatalog durchzuführen, um später eine schnellere Zuordnung zu ermöglichen[4].

Abbildung 7.3: Anwendungsbeispiel des Klassifizierungsmodells



Nutzung durch die Allianz

Weiterhin kann die Allianz das Modell zur Erstellung eines allgemeinen Bedrohungsmodells für die Allianz benutzen. Hier kann das Modell zur Erstellung einer spezifischen Eintrittswahrscheinlichkeit von Bedrohungen für die Allianz genutzt werden. Dazu wird in jeder Dimension in Abbildung 7.2 eine Variable zugewiesen (Tabelle B.3). Jeder Variable kann ein Wahrscheinlichkeitswert zugewiesen werden, welcher am Ende multipliziert wird, um die Wahrscheinlichkeit der Bedrohung zu erhalten:

$$p_{bedrohung}(U) = p_{quelle} \cdot p_{ausloeser} \cdot p_{boeswilligkeit} \cdot p_{absicht} \cdot p_{auswirkung}$$

Die Werte dazu werden von der Allianz festgelegt und im Rahmen der geteilten Risikoinformation kontinuierlich verbessert, um das Wissen der Partner einfließen zu lassen. Zur Festlegung der Wahrscheinlichkeitswerte gibt es keine Vorgabe, sinnvolle Werten müssen durch den Risiko Manager ermittelt werden. Es ergibt sich ein Bedrohungsmodell, welches

[4]Ein Beispiel auf Basis der ENISA Threat Taxonomy findet sich in Abbildung B.4

von allen Partnern zur Verbesserung der eigenen Bewertung verwendet werden kann. Dieses wird den Partnern in der Aktivität *Risiken und Maßnahmen überwachen* bereitgestellt und hilft ihnen, die lokale Aufgabe *Bedrohungen überwachen auszuführen*. Je mehr die Allianz in gemeinsame Ressourcen wie diese investiert, desto höher wird der Mehrwert des kollaborativen Prozesses im Vergleich zu einem individuell durchgeführten ISRM.

7.3 Definition von vergleichbaren Asset-Kategorien

Während die Allianz in ihrem Teil der Aktivität *Kontext festlegen* die teilnehmenden Partner auswählen muss (etwa mit Hilfe einer Reifegradbewertung), muss anschließend jeder dieser Partner den eigenen *Scope festlegen*. Dabei geht es um die Auswahl der Assets einer Allianz, die relevant für das CISRM sein könnten bzw. deren Mapping auf gemeinsame Assets.

Vergleichbarkeit

Es ist denkbar, dass die Partner unterschiedliche Assets besitzen und auch gleiche Assets unterschiedlich definiert haben. Das erschwert natürlich den Austausch von Risikoinformationen, da die Partner potenzielle Assets nicht direkt auf die eigene Organisation abbilden können. Auch hier kann und soll den Organisationen keine Vorgabe gemacht werden, wie sie ihren internen Prozess aufbauen und wie ihre Asset-Struktur im Detail aussieht. Was jedoch möglich sein sollte, ist zumindest auf oberster Ebene die Kategorien der Assets zu vereinheitlichen. Dadurch ergibt sich bereits eine vergleichbare Gruppierung die zur Einordnung und zum Filtern von Risiken genutzt werden kann.

Vorgehen

In diesem Abschnitt werden existierende Asset-Kategorien vorgestellt, die von der Allianz genutzt werden können. Diese sollten als Input in den CISRM Prozess eingehen und alle Partner müssen sich auf die Nutzung einigen. Auch hier ist es natürlich möglich, dass sich die Allianz unabhängig davon ihre individuellen Vorgaben zu den Assets setzt.

7.3.1 Existierende Asset-Kategorien

Verschiedene Standards und Frameworks liefern ihre eigenen Beispiele für Assets und einen Vorschlag diese zu kategorisieren. So definiert etwa die ISO/IEC 27005 [98] im Anhang B eine eigene Liste von Asset-Kategorien. Auch die BSI Standards [13, 56] arbeiten mit verschiedenen Klassen von Assets. Dabei macht keiner der Standards eine klare Vorgabe an die Kategorisierung von Assets, sondern bezeichnet die eigenen nur als Vorschläge. Zusammengefasst lässt sich sagen, dass sich diese meistens nur im Detail unterscheiden. Trotzdem ist es im Zuge der interorganisationalen Zusammenarbeit wichtig, dass sich die Allianz vorab Gedanken darüber macht, welche Kategorisierung sie im Prozess verwendet. Wie bereits zuvor erwähnt arbeitet auch die ENISA seit einiger Zeit an dem Thema des interorganisationalen ISRM. Dazu hat sie das *Interoperable EU Risk Management Framework* [38] veröffentlicht. Teil dieses Frameworks ist unter anderem die *Interoperable EU Risk Management Toolbox* [235], die unterstützende Materialien enthält. Darin findet sich wiederum mit dem *Asset Mapping* eine Liste von Asset-Kategorien, die im Folgenden vorgestellt wird.

Tabelle 7.1: Übersicht des Asset Mappings aus der ENISA EU RM Toolbox [235]

Typ	Kategorie	Beschreibung
P	Geschäftsprozesse, Funktionen, Services	Geschäftsprozesse, Funktionen, Services
P	Informationen und Daten	Informationen und Daten von Wert jeglicher Art (gespeichert, übertragen, usw.)
U	Hardware, Geräte und Ausrüstung	Alle physischen Elemente/Geräte/Ausrüstung die Geschäftsprozesse, Funktionen und Services unterstützen.
U	Software/Anwendungen	Software und Anwendungen
U	Personal	Entscheidungsträger, Nutzer, Entwickler, Administratoren, Betrieb, Wartungspersonal, Externe
U	Standort und Versorgung	Orte und Räumlichkeiten, Mobile Plattformen, Grundlegende Dienstleistungen und Versorgungseinrichtungen, die von externen Betreibern/Anbietern bereitgestellt werden, Strom- und Wasserversorgung usw.
U	Organisatorische Infrastruktur (inkl. ICT)	Organisatorische Infrastruktur einschließlich Rollen, Strategien, Verfahren und IKT-Dienste (Telekommunikation, Netzwerk, Cloud, Hosting usw.)

Kategorien

Die ENISA unterteilt klassisch in *primäre Assets* (Typ P) und *unterstützende Assets* (Typ U). Eine vollständige List der zugehörigen Kategorien und Beschreibungen ist in Tabelle 7.1 zu sehen. Die Kategorie *Informationen und Daten* sind im ISRM quasi obligatorisch. Die ENISA beschränkt sich auf zwei primäre Asset-Kategorien und vereint *Geschäftsprozesse, Funktionen und Services*. Bei den unterstützenden Assets finden sich weitere fünf Kategorien, die alle üblichen Assets und Bedrohungen abdeckt. Die EU RM Toolbox liefert damit eine solide Kategorisierung von Assets, welche für die meisten Organisationen funktionieren sollte.

ISO/IEC 27005

Damit unterscheidet sich die Klassifikation der ENISA tatsächlich nur im Detail von der ISO. Auch die ISO/IEC 27005 [98] setzt die gleichen Oberkategorien mit zwei vergleichbaren primären Assets. Ebenso existiert ein Pendant für jede unterstützende Asset-Kategorie: *Hardware, Software, Personal, Standort und Organisationsstruktur*. Zusätzlich definiert die ISO jedoch noch eine sechste unterstützende Kategorie, das *Netzwerk*. Dieses geht bei der ENISA in den Bereichen Hardware, Geräte und Ausrüstung sowie Versorgung und ICT auf. Letztlich scheint das Netzwerk als eigene Kategorie keinen zusätzlichen Mehrwert zu bieten, weshalb die Anpassung der ENISA sinnvoll erscheint.

Crowdsourcing

Die Idee des ENISA Asset Mappings ist es, eine Liste mit generischen Asset-Kategorien bereitzustellen. Diese soll dann genutzt werden, um einen Abgleich mit anderen Frameworks und deren Klassifizierung durchzuführen, welcher Teils von der Community bereitgestellt werden soll. Zum Zeitpunkt des Erscheinens gibt es jedoch nur zwei Mappings: die *ISO/IEC*

27005:2018 und die *IT Security Risk Management Methodology v1.2*. Die Schwierigkeit bei einem solchen Crowdsourcing Ansatz ist es, tatsächlich zeitnah verlässliche Daten zu erhalten und vor allem, diese Daten für alle Frameworks aktuell zu halten. Ob die ENISA mit diesem Vorgehen erfolgreich ist, wird sich noch zeigen müssen.

Nutzung

In jedem Fall liefert die EU RM Toolbox hier eine sinnvolle Liste von Asset-Kategorien. Aufgrund der Reichweite der ENISA und der Nähe zur etablierten Standardisierung der ISO ist zu erwarten, dass die definierten Kategorien von vielen Organisationen aufgegriffen und möglicherweise auch von anderen Frameworks adaptiert werden. Eine Nutzung im CISRM zur Synchronisation der Assets innerhalb der Allianz wird deshalb empfohlen.

7.3.2 Verwendung der Asset-Kategorien im Prozess

Die Abstimmung gemeinsamer Asset-Kategorien ist bereits beim Festlegen des Kontexts (Abbildung 6.3) notwendig, wenn die Partner festlegen sollen, welche ihrer Assets in den Scope des CISRM fallen. Später helfen vergleichbare Asset-Kategorien den Partnern dabei, die geteilten Risikoinformationen auf die eigenen Assets anzuwenden (Abbildung 6.4).

Scope

Der Scope des CISRM kann sehr einfach auf Basis der genannten ENISA Kategorien angepasst werden (Tabelle 7.1). Die Partner müssen gemeinsam festlegen, welche der genannten Kategorien relevant für die Allianz sind und können etwa bestimmte Kategorien ausnehmen. Während dieser Schritt bei den Bedrohungen sinnvoll ist, so ist es jedoch unwahrscheinlich, dass die Allianz eine gesamte Asset-Kategorie ausschließen kann. Analog sollte sich jede einzelne Organisation überlegen, ob alle Assets im Scope des CISRM sein sollten. Dazu können die eigenen Assets den neuen Kategorien zuordnen bzw. einfach ein Mapping ihrer existierenden Asset-Kategorien durchführen. Eine Einschränkung des Scopes könnte sich ergeben, wenn einzelne Kategorien von Assets keinen Einfluss auf die Sicherheit der Organisation oder der Allianz haben. Ähnlich wie auch bei der Scope Analyse gemäß der ISO/IEC 27001 und 27005, ist es jedoch in den meisten Fällen schwierig, Assets aus dem Scope des ISRM auszunehmen.

Bedrohungen

Ein weiterer Prozessschritt, bei dem die standardisierten Asset-Kategorien helfen, ist das Teilen von Risikoinformationen. Wie auch bei den Bedrohungen geht es darum, dass die Organisationen die bereitgestellten Daten der Partner möglichst einfach nutzen können. Durch das zuvor präsentierte Klassifizierungsmodell für Bedrohungen (Abbildung 7.3) ist eine einfache Zuordnung dieser aufeinander bereits möglich. Durch die einheitliche Verwendung der Asset-Kategorien bei der Kommunikation ist es dann ebenfalls möglich zu erkennen, ob ein Risiko eines Partners ebenfalls die eigenen Assets betreffen würde.

Mapping

Zur Nutzung im Prozess müssen die Partner intern keine Änderungen vornehmen, sondern ihre Risiken lediglich beim Teilen von Risikoinformationen einer der Asset-Kategorien der Allianz zuweisen. Durch die Kompatibilität der ENISA Toolbox zu existierenden Frameworks, sollten die meisten Organisationen ihre Asset-Kategorien leicht auf die generischen Kategorien abbilden können. So würden etwa sowohl Assets aus der Kategorie *Standort* (ISO) als auch *Infrastruktur* (BSI) beide in die Kategorie *Standort und Versorgung* fallen. Durch diesen einfachen Zwischenschritt wird die Zuordnung und Nutzung der Risiken in anderen Organisationen deutlich vereinfacht.

7.4 Auswahl einer gemeinsamen Methode

Ebenfalls in der Aktivität *Risiken einschätzen* (Abbildung 6.8) ist ein erster essenzieller Schritt das Festlegen einer Bewertungsmethode für die Allianz. Dabei geht es um die Auswahl einer Metrik für das ISRM, um vergleichbare Risiken zu generieren. Letztlich ist es das Ziel innerhalb der Allianz so viele Informationen über Risiken auszutauschen wie möglich und eine solide Grundlage für die gemeinsame Risikobehandlung zu legen.

Bewertung

Obwohl es den Partnern grundsätzlich selbst überlassen bleibt, welche Methode zur Risikobewertung sie intern verwenden, so ist es für das gemeinsame Vorgehen notwendig, sich zumindest in einigen Werten abzustimmen. Haben die Partner völlig unabhängige Methoden, welche zu einer nicht vergleichbaren Risikohöhe führen, dann bietet die Bewertung anderen Organisationen keinen Mehrwert. Beim Austausch der Risikoinformationen sollen die Partner jedoch von der existierenden Bewertung profitieren, da an dieser Stelle bereits viel Aufwand in die Analyse investiert wurde. Insgesamt nimmt die Effektivität des kollaborativen Prozesses und damit der Mehrwert für die Partner zu, je mehr der Daten sie wiederverwenden können. Dieses Ziel steht selbstverständlich im Kontrast dazu, die Individualität und Unabhängigkeit der Partner zu bewahren.

Behandlung

Ähnlich sieht es bei der gemeinsamen Risikobehandlung innerhalb der Allianz aus. Zum einen müssen die Partner wissen, ab welcher Risikohöhe über Risiken innerhalb des *Allianz Risiko Boards* entschieden werden sollte. Gleichzeitig ist es dort relevant ein gemeinsames Verständnis für die Dringlichkeit des Risikos zu haben. Beides funktioniert nicht, wenn alle Organisationen lediglich ihre eigene Bewertungsmethode verwenden. Es muss zumindest für alle Partner leicht erkennbar sein, ob es sich aus ihrer eigenen Perspektive um ein hohes oder niedriges Risiko handelt.

Vorgehen

In diesem Abschnitt wird eine allgemeine Methode für die Risikobewertung vorgestellt, welche von der Allianz als Input für den kollaborativen Prozess genutzt werden kann. Anschließend wird skizziert, wie die Partner diese Methode nutzen können, um damit ihre eigene Bewertung zu ergänzen. Auch hier kann die Allianz natürlich stattdessen ihre eigene Methode definieren. In jeden Fall sollte diese bei der Implementierung des CISRM zwischen den Partnern abgestimmt werden.

7.4.1 Die ENISA Methode

Auch hier bietet die *Interoperable EU Risk Management Toolbox* [235] in Form des *Risk-Impact Level Mappings* bereits eine Lösung. Dieses liefert eine allgemeine Risikomatrix, Definitionen zur Einstufung und einem Mapping zwischen verschiedenen Bewertungsmethoden. Wie auch bei den Asset-Kategorien bietet es sich auch hier an, für das CISRM auf diese Methode zurückzugreifen.

Toolbox

Tabelle 7.2 zeigt alle Wert der Methode aus der ENISA Toolbox. Dabei wird ein qualitatives Vorgehen zur Risikobewertung implementiert. Es werden klassische Werte auf Basis von Eintrittswahrscheinlichkeit und Auswirkung verwendet. Für beide Attribute werden die gleichen fünf Werte genutzt: sehr gering, gering, mittel, hoch, sehr hoch. Daraus ergibt sich dementsprechend eine 5x5 Matrix, mit wiederum fünf Stufen für die Risikohöhe.

Tabelle 7.2: Attribute der ISRM Methode aus der ENISA EU RM Toolbox [235]

Level	Risk	Impact	Likelihood
Very High	A threat event is predicted to have severe impact in business affairs.	A threat event leads to severe business impacts.	A threat event is highly likely to be materialized in the short term and associated with vulnerabilities because there are no adequate security measures to defend them.
High	A threat event is predicted to have harsh impact in business affairs.	A threat event leads to significant business impacts.	A threat event is likely to be materialized and associated with vulnerabilities because there are ineffective or obsolete security measures to defend them.
Moderate	A threat event is predicted to have moderate impact in business affairs.	A threat event leads to moderate business impacts.	A threat event is possible to be materialized and associated with vulnerabilities because there are security measures to defend them, but, better security measures could have been implemented.
Low	A threat event is predicted to have diminished impact in business affairs.	A threat event leads to minor business impacts.	A threat event is unlikely to be materialized and associated with vulnerabilities because there are good security measures to defend them.
Very Low	A threat event is predicted to have insignificant impact in business affairs.	A threat event leads to negligible business impacts.	A threat event is highly unlikely to be materialized and associated with vulnerabilities because there are effective security measures to defend them.

Einstufung

Zur Analyse der des Risikos werden für jedes Level entsprechende Bewertungskriterien bereitgestellt. Diese sind sehr generisch gehalten, sodass sie auf jede Art von Organisation zutreffen können. Die Bewertung der Auswirkung orientiert sich am Schaden für die Organisation und ihrer Stakeholder. Für die Eintrittswahrscheinlichkeit stehen hingegen keine harten Kriterien bereit, sondern die Abschätzung, ob ein Ereignis nun wahrscheinlich oder unwahrscheinlich ist, bleibt eher subjektiv. So ergibt sich bei einer einfachen multiplaktion von Eintrittswahrscheinlichkeit und Auswirkung eine Wertemenge von 1 bis 25.

7.4.2 Verwendung der Methode im Prozess

Insgesamt definiert die Toolbox hier also eine sehr klassische ISRM Methode, die erneut nicht sehr stark von den Vorgaben der ISO/IEC 27005 abweicht. Das ist positiv, da sie damit weit verbreitet ist und insgesamt so simpel, dass sie wahrscheinlich von den meisten Organisationen adaptiert werden kann. Sie liefert somit eine solide Grundlage als Vorlage im CISRM.

Anwendung

Obwohl mit der ENISA Methode somit bereits eine generische Methodik existiert, stellt sich die Frage, wie Allianzen diese nutzen können. Auch hier darf den Partnern keine Vorgabe gemacht werden, wie sie ihre Risiken zu bewerten haben. Jede Organisation hat ihrerseits ein ISRM etabliert und hat sich dementsprechend längst auf eine Methode zur Bewertung festgelegt. Diese zu ändern würde nicht nur einen hohen internen Aufwand bedeuten, sondern auch eine eventuelle Compliance zu dem von der Organisation gewählten Framework beeinflussen und so existierende Abhängigkeiten zu einem eventuell vorhandenen ERM stören. Daher sollte sich die Allianz bei Implementierung des CISRM auf eine Methode festlegen, welche dann genutzt wird, um die Risiken der Partner darauf abzubilden.

Appetit

An dieser Stelle muss sich die Allianz entscheiden, wie hoch ihr Risikoappetit bzw. ihre Risikotoleranz ist und ein entsprechendes Level festzulegen. Dabei ist zu bedenken, dass dies direkt die Risikotoleranz der Partner beeinflusst, da es eine Obergrenze für diese darstellt (Abbildung 6.3). Dies ist die Schwelle, ab der die Partner im Rahmen der Risikobehandlung ihre Risiken gemeinsam diskutieren würden. Hier bietet es sich in der ENISA Methode an, alles ab moderat zu betrachten (Risikohöhe ≥ 5), um nur wichtige Risiken zu diskutieren (unabhängig vom Teile der Risikoinformationen). Allerdings hängt das natürlich wiederum vom ISM Reifegrad der Allianz ab. Wie auch beim initialen Aufbau eines ISRM sollte hier ein langsamer Einstieg erfolgen, um die Teilnehmer nicht zu überfordern.

Abbildung

Wie in der Toolbox *Ranking Sample Library* zu sehen, ist es sehr einfach die Bewertung anderer Methoden auf die ENISA Methode abzubilden[5]. Die Quellmethode muss lediglich via Gleichverteilung auf die fünf Stufen der ENISA Methode abgebildet werden. Da keines der bekannten Frameworks mehr als fünf Risikolevel verwendet, ist es unwahrscheinlich, dass es dabei zu Problemen kommt. Wie auch bei den Assets reicht es, diese Abbildung vor dem Teilen der Risikoinformationen durchzuführen. Im Umkehrschluss können Risiken der Allianz so sehr einfach in die eigene Risikomethode überführt werden.

[5]Im Anhang (Tabelle B.5) findet sich das offizielle Beispiel aus der Toolbox, welches ein Mapping verschiedener Methoden zeigt

7.5 Zusammenfassung der Ressourcen

In diesem Kapitel wurden verschiedene gemeinsame Ressourcen diskutiert, die für das CISRM notwendig sind und als Input in den Prozess eingebracht werden müssen. Dazu wurden Vorschläge für verschiedene Prozessartefakte geliefert, die von Organisationen adaptiert werden können, um den Prozess zu realisieren.

Risikoinformationen

Die genannten Ressourcen sind allesamt notwendig, um die Risikoinformationen im kollaborativen Prozess auszutauschen. Unabhängig davon, ob die vorgestellten Leitfäden befolgt oder die Allianz sich ein eigenes Vorgehen definiert, so hilft die Standardisierung in jedem Fall bei einem einfachen Informationsaustausch. Letztlich müssen alle Informationen über ein Risiko von einer Organisation zusammengefasst und an die Partner übermittelt werden. Dies geschieht im Prozess über die Risiko Manager der Organisationen und der Allianz. Eine einfache Zusammenfassung der übermittelten Risikoformationen kann wie folgt dargestellt werden (JSON Format):

```
{
      "Risiko": {
            "Metadaten": {
                  "Titel": "Organisation",
                  "Beschreibung": "Organisation",
            },
            "Bedrohung": {
                  "Bedrohung: "Organisation",
                  "KategorieAuswirkung": "Allianz",
            },
            "Asset": {
                  "Asset": "Organisation",
                  "AssetKategorie": "Allianz"
            }
            "Einstufung": {
                  "Eintrittswahrscheinlichkeit": "Allianz",
                  "Auswirkung": "Allianz",
                  "Risikolevel": "Allianz
            }
      }
}
```

Werte

Die Organisation liefert dabei sowohl ihre eigenen Risikowerte (Organisation) sowie die adaptierten Werte (Allianz). Die Metadaten können bei Bedarf erweitert werden, aber die Organisation sollte mindestens einen Titel und eine Beschreibung des Risikos liefern. Ergänzt wird dieses durch die verwendete Bedrohung, die auf die Kategorie der Auswirkung abgebildet wird. Analog verhält es sich mit dem internen Asset der Organisation und der abgeleiteten Asset-Kategorie. Die internen Werte der Risikobewertung spielen für die Partner keine Rolle und können komplett weggelassen werden, wenn das Mapping auf die

generische Methode erfolgt ist. Im Ergebnis erhält jeder Partner alle Daten, die er braucht, um die Risikoinformationen im eigenen ISRM zu verwenden.

Scope

Ein Risiko soll nur dann geteilt werden, wenn das zugehörige Asset auch im Scope des CISRM ist, da es sonst für die anderen Partner keine Relevanz hat. Bei der gemeinsamen Risikobehandlung werden wiederum nur solche Risiken berücksichtigt, deren Risikolevel höher als der definierte Risikoappetit der Allianz ist. Dies sind die Risiken, über die das *Allianz Risiko Board* gemeinsam diskutieren sollte.

Zusammenfassung

Dieser Leitfaden über die Standardisierung der für den Austausch von Risikoinformationen notwendigen Ressourcen stellt die letzte Komponente des CISRM Frameworks dar. Zusammengefasst wurden in diesem Abschnitt die folgenden Fragestellungen untersucht und diskutiert:

- Welche ISM Aspekte sollten Allianzen beachten, wenn sie die Teilnehmer im Scope des CISRM anhand einer Reifegradbewertung auswählen (Abschnitt 7.1)?
- Lassen sich die Bedrohungen so klassifizieren, dass die Partner sie auf die eigenen Risiken abbilden können (Abschnitt 7.2)?
- Können standardisierte Asset-Kategorien dabei helfen, den Mehrwert der geteilten Risikoinformationen zu erhöhen (Abschnitt 7.3)?
- Wie kann eine gemeinsame Bewertungsmethode genutzt werden, um die Risikobewertungen der Partner vergleichbar zu machen (Abschnitt 7.4)?

Im folgenden Kapitel werden alle Komponenten des Frameworks aufgelistet und ihre Anwendbarkeit überprüft. Dazu werden die in Kapitel 3.3 definierten Anforderungen auf das Framework angewendet. Anschließend wird anhand des Fallbeispiels GÉANT (Kapitel 3.2) skizziert, wie das CISRM in einer realen Allianz aussehen könnte.

Kapitel 8

Evaluation des CISRM Frameworks

Inhaltsangabe

In dieser Arbeit wurde das CISRM als Erweiterung des ISRM vorgestellt. Dieses Konzept stellt einen Ansatz dar, die individuellen Prozesse mehrerer Organisationen miteinander zu verknüpfen. Die Grundidee dahinter ist es, dem zunehmenden Trend hin zu interorganisationalen Beziehungen Rechnung zu tragen (Kapitel 4.1) und deren Vorteile auch auf das ISM anzuwenden. Insbesondere in strategischen Allianzen, die eine sehr enge Beziehung zwischen den Partnern etablieren, lassen sich Synergieeffekte durch das Teilen von Informationen und die Durchführung gemeinsamer Aktivitäten herstellen. Da es sich dabei um einen neuen Ansatz handelt, stellt sich die Frage, wie zwei oder mehr Organisationen in der Praxis im Bereich ISRM zusammenarbeiten können. Daher wurde ein Meta-Framework für das CISRM entwickelt, welches Organisationen beim Aufbau eines kollaborativen Prozesses unterstützt.

Framework

Die vorherigen Kapitel liefern jeweils einen Baustein zur Implementierung eines solchen interorganisationalen CISRM. Die insgesamt vier Komponenten lassen sich zu einem Framework verknüpfen, welches den kompletten Lebenszyklus abbildet. Als Startpunkt hilft das Partnerschaftsmodell dabei zu bewerten, ob das CISRM in einer IORs überhaupt anwendbar ist (Kapitel 4). Ist das der Fall, dann liefern eine gemeinsame Terminologie (Kapitel 5), ein interorganisationaler Prozess (Kapitel 6) und dessen unterstützende Ressourcen (Kapitel 7) die notwendige Prozessarchitektur, um ein CISRM in einer Allianz zu etablieren. Alle Komponenten werden in diesem Kapitel gemeinsam behandelt, bewertet und angewendet.

Anforderungen

Es gilt nun zu evaluieren, ob das erstellte Framework tatsächlich geeignet ist, um die Idee eines CISRM zu verwirklichen. Dazu werden die zuvor in Kapitel 3 definierten CSFs und Anforderungen herangezogen. Diese wurden auf Basis existierender Kollaborationen aus der Praxis identifiziert und liefern Rahmenbedingungen für einen funktionierenden Prozess. Auch das durch das Framework definierte CISRM muss diese Anforderungen letztlich erfüllen, um einen wirksamen Prozess zu etablieren. Es wird daher in Abschnitt 8.1 bewertet, ob und wie gut die CSFs realisiert sind.

Fallbeispiel

Anschließend wird in Abschnitt 8.2 skizziert, wie ein das CISRM in einer konkreten Allianz aussehen könnte. Dies geschieht auf Basis des GÉANT Projektes, welches in Kapitel 3.2 vorgestellt wurde. Anhand dieses Fallbeispiels soll die konkreten Schritte aufgezeigt werden, um einen kollaborativen Prozess zu etablieren. Dabei werden die spezifischen Eigenschaften der Allianz berücksichtigt, welche sich natürlich von Fall zu Fall unterscheiden. Da das CISRM bisher noch nicht innerhalb einer Allianz implementiert wurde (was definitiv eine der essenziellen Folgearbeiten dieser Arbeit ist, Kapitel 9.3), kann an dieser Stelle noch kein realer Praxistest durchgeführt werden. Trotzdem kann anhand dieses Gedankenexperiments nachvollzogen werden, wie die konkreten Schritte in einer existierenden IOR aussehen würden.

8.1 Kritische Bewertung des Frameworks

In diesem Abschnitt erfolgt eine inhaltliche Evaluation des erstellten Frameworks. Dazu wird zuerst das komplette Framework mit seinen vier Komponenten zusammenfassend dargestellt. Für eine erste Prüfung werden die zuvor abgeleiteten CSFs auf das Framework abgebildet. Es gilt zu klären, ob das CISRM alle wesentlichen Eigenschaften besitzt, um einen wirksamen kollaborativen Prozess zu etablieren. Anschließend werden die konkreten Anforderungen einzeln überprüft und diskutiert, ob diese erfüllt sind. Basierend darauf folgt eine abschließende Bewertung, wie gut das Framework zum Aufbau eines gemeinsamen CISRM geeignet ist.

8.1.1 Zusammenfassende Darstellung des Frameworks

Bisher wurden nur die einzelnen Komponenten diskutiert, diese jedoch nie richtig in Zusammenhang gebracht. Ein vollständiger Überblick ist an dieser Stelle notwendig, um die Wirksamkeit des Frameworks als Ganzes bewerten zu können. Daher werden alle Teile des Frameworks und deren nutzen im Folgenden kurz beschrieben.

Framework

Das CISRM Framework stellt ein ISRM Meta-Framework zum interorganisationalen Kollaboration bereit. Um zu verstehen, wie die einzelnen Teile zusammenhängen zeigt Abbildung 8.1 eine grafische Darstellung des CISRM Frameworks. Es skizziert die Interaktionen zwischen den einzelnen Komponenten sowie die Schnittstelle des CISRM Prozesses in die ERM Prozesse der Partnerorganisationen.

Interaktionen

Das Framework wurde so konzipiert (Abbildung 3.1), dass die einzelnen Komponenten inhaltlich aufeinander aufbauen, aber trotzdem nicht voneinander abhängen. Sie unterstützen sich gegenseitig und helfen beim Aufbau eines gemeinsamen Prozesses, können bei Bedarf jedoch auch ersetzt werden. Weiterhin sind die einzelnen Komponenten inhaltlich abgeschlossen und können auch unabhängig vom restlichen Framework verwendet werden.

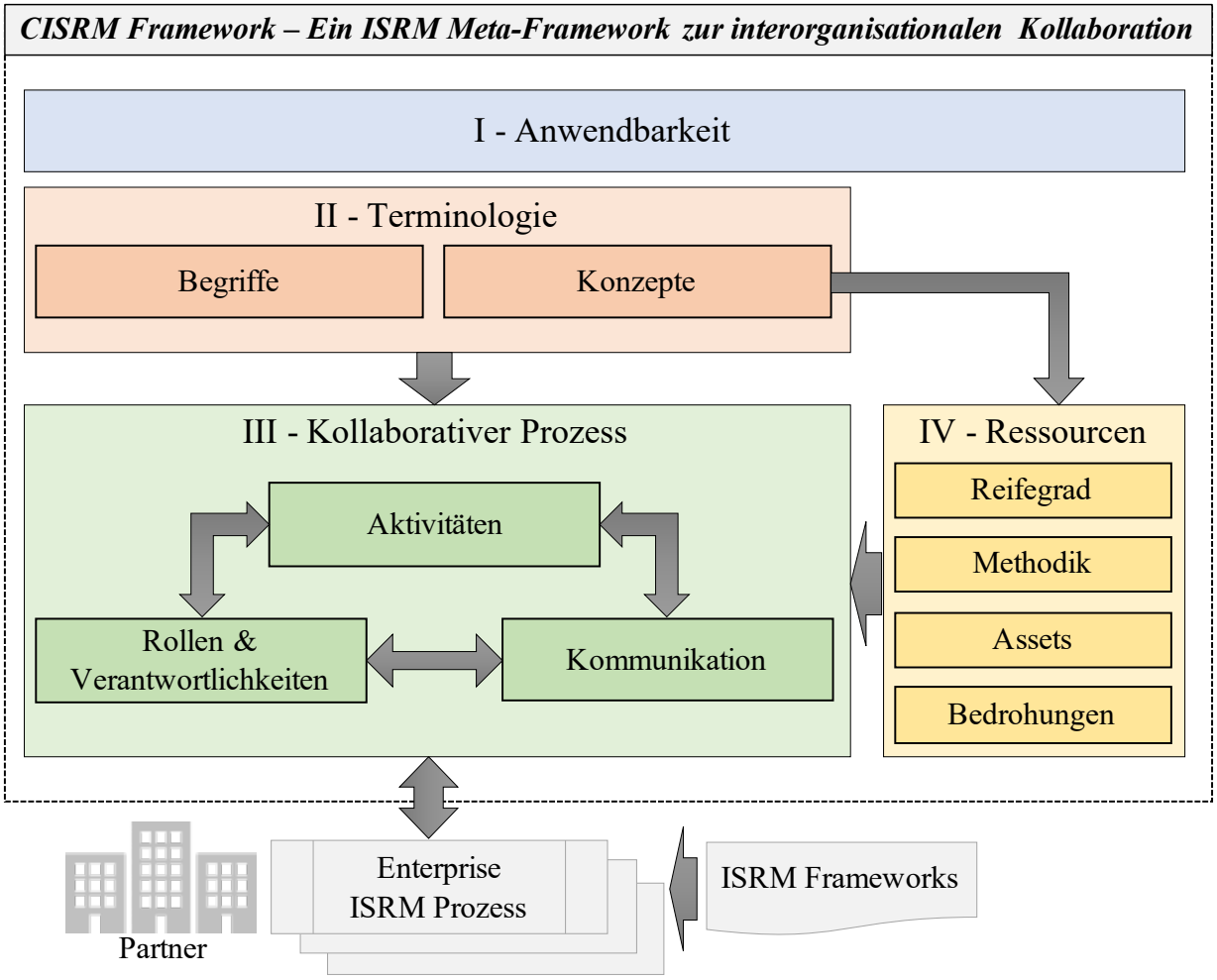
ERM

Im Sinne eines Meta-Frameworks sind die konkreten ERM bzw. die ISRM Prozesse innerhalb der Organisationen nicht vorgegeben. Schließlich basiert die ganze Idee der Zusammenarbeit auf einem lose gekoppelten Vorgehen innerhalb der Allianz. Jeder Partner muss vor Aufbau eines gemeinsamen CISRM erst einmal ein eigenes ISRM aufgebaut haben. Dieses kann grundsätzlich auf einem beliebigen Framework basieren, etwa einem der hier vorgestellten. Die einzelnen Prozesse werden durch Etablieren des gemeinsamen Prozesses miteinander verknüpft.

Komponente I - Anwendbarkeit

Die erste Komponente ist ein Modul zur Bewertung der Anwendbarkeit des CISRM. Dieses erlaubt es einer Organisation ihre bestehende IOR zu evaluieren und zu bewerten, ob diese geeignet ist, ein CISRM zu etablieren. Sind die Anforderungen an die Allianz erfüllt, dann können die restlichen Komponenten des Frameworks für den Aufbau eines gemeinsamen Prozesses genutzt werden. Hierbei fällt auf, dass diese Komponente selbst keine Verbindung zu den Anderen hat. Tatsächlich ist es so, dass

Abbildung 8.1: Struktur des Meta-Frameworks für interorganisationales ISRM



die Einschätzung der IOR auf Basis des Partnerschaftsmodells nur eine Vorbedingung ist, aber anschließend keine Rolle mehr für den Aufbau des Prozesses spielt.

Komponente II - Terminologie

Die zweite Komponente enthält eine generische Terminologie mit den essenziellen Begriffen und Konzepten des ISRM. Mit dieser können die Partner ihre Sprache auf ein allgemeines Fachjargon innerhalb der Allianz abbilden und gleichzeitig intern weiterhin das bisherige System verwenden. Dies ist die Voraussetzung für eine funktionierende Kommunikation, sowie das Verständnis der gemeinsamen Aktivitäten und Vorgehensweisen. Somit ist es notwendig, dass die Allianz eine gemeinsame Terminologie zur Verfügung hat, bevor ein Prozess etabliert werden kann.

Komponente III - Prozess

Die dritte Komponente definiert das Vorgehen im kollaborativen Prozess. Sie stellt zum einen Rollen bereit, welche innerhalb des CISRM vergeben werden müssen und

weist diesen entsprechende Verantwortlichkeiten zu, zu denen insbesondere die Kommunikation zwischen den Partnern gehört. Dies wurde in ein interorganisationales Prozessmodell integriert, welches die Aktivitäten der Allianz und der teilnehmenden Partner definiert. Dies bildet den Kern des CISRM und erlaubt es den Organisationen einen entsprechenden Prozess anhand dieser Vorlagen zu etablieren.

Komponente IV - Ressourcen
Ergänzend zur Vorherigen liefert die vierte Komponente Umsetzungsanleitungen für die im Prozess benötigten unterstützenden Ressourcen. Während der definierte Prozess einige Inputs erfordert, die von der Allianz geliefert werden müssen, liefert diese Komponente eine Hilfestellung, um diese zu erstellen. Dazu gehören die Grundlagen zur Bewertung der Reife der Partner, eine Möglichkeit die Bedrohungen innerhalb der Allianz zu vergleichen, eine standardisierte Methode und vergleichbare Assets.

8.1.2 Abbildung der CSF auf die Komponenten

Nachdem nun das Framework einmal zusammengefasst wurde, soll es Schritt für Schritt evaluiert werden. Im Folgenden werden nun die in Kapitel 3 definierten CSFs betrachtet, um die Vollständigkeit des Frameworks zu bewerten, ohne konkret auf die abgeleiteten Anforderungen einzugehen. Die Faktoren liefern jeweils abstrakte Ziele, die für die Wirksamkeit des CISRM notwendig erscheinen. Daher werden diese als Erstes auf die soeben beschriebenen Komponenten abgebildet.

CSF 1: Teilen von Risikoinformationen
CSF 1 soll einen unkomplizierten Austausch von relevanten IS-Risiken innerhalb der Allianz ermöglichen. Dies ist ein zentrales Feature des CISRM, da es dafür sorgt, dass die Partner einen Mehrwert aus den bereitgestellten Informationen der anderen Organisationen ziehen können. Dieser Faktor wird von Komponente III, dem kollaborativen Prozess, unterstützt. Hier wurde beim Design des Kommunikationsmoduls darauf geachtet, dass die Partner klar definierte Schnittstellen besitzen, um Risikoinformationen innerhalb der Allianz auszutauschen.

CSF 2: Standardisierung der Vorgehensweisen
Bei CSF 2 soll ein einheitliches Verständnis des ISRM und seiner Inhalte innerhalb der Allianz herbeigeführt werden. Eine gemeinsame Sprache ist die Grundvoraussetzung dafür, dass zwei Parteien überhaupt miteinander kommunizieren können. Somit muss selbst in einem unabhängigen Prozess, der so wenige Aspekte wie möglich standardisieren soll, eine minimale Wissensbasis geschaffen werden. Die einheitliche Terminologie in Komponente II zielt genau darauf ab. Obwohl die Partner im CISRM an ihren eigenen Prozessen und Prozessframeworks festhalten können, ermöglicht die Verwendung von einheitlichen Begriffen eine standardisierte Kommunikation. Gleichzeitig ist sichergestellt, dass die Partner trotz unterschiedlichen Vorgehensweisen immer ein einheitliches Verständnis der wichtigsten Konzepte haben.

CSF 3: Gemeinsame Entscheidungen
Laut CSF 3 muss die Risikobehandlung von für die Allianz relevanten IS-Risiken zwischen den Partnern abgestimmt werden. Dies sorgt in einem interorganisationalen Prozess dafür, dass alle beteiligten Organisationen sich auf den getroffenen Entscheidungen gegenüber verpflichtet fühlen. Dieser Aspekt wird ebenfalls in Komponente III, dem kollaborativen Prozess berücksichtigt. Das Modul Rollen & Verantwortlichkeiten definiert Vertreter für alle am Prozess beteiligten Partner und gibt diesen ein Mitbestimmungsrecht in allen Aspekten der Kollaboration.

CSF 4: Teilen von Risiken und Vorteilen
In CSF 4 liegt der Fokus auf der gemeinsamen Risikobehandlung. Es soll sichergestellt werden, dass die Allianz und deren Teilnehmer tatsächlich vom kollaborativen Vorgehen profitieren, indem die Partner sich Risiko und Vorteile teilen. Dieser Faktor wird maßgeblich durch Komponente I erfüllt. Bereits bei der Auswahl der Partner soll durch das Partnerschaftsmodell sichergestellt werden, dass nur kollaborative Beziehungen ein CISRM einführen. Nur in diesen Allianzen sind die Partner eng genug miteinander verbunden, um tatsächlich von gemeinsamen Risiken und Vorteilen zu profitieren.

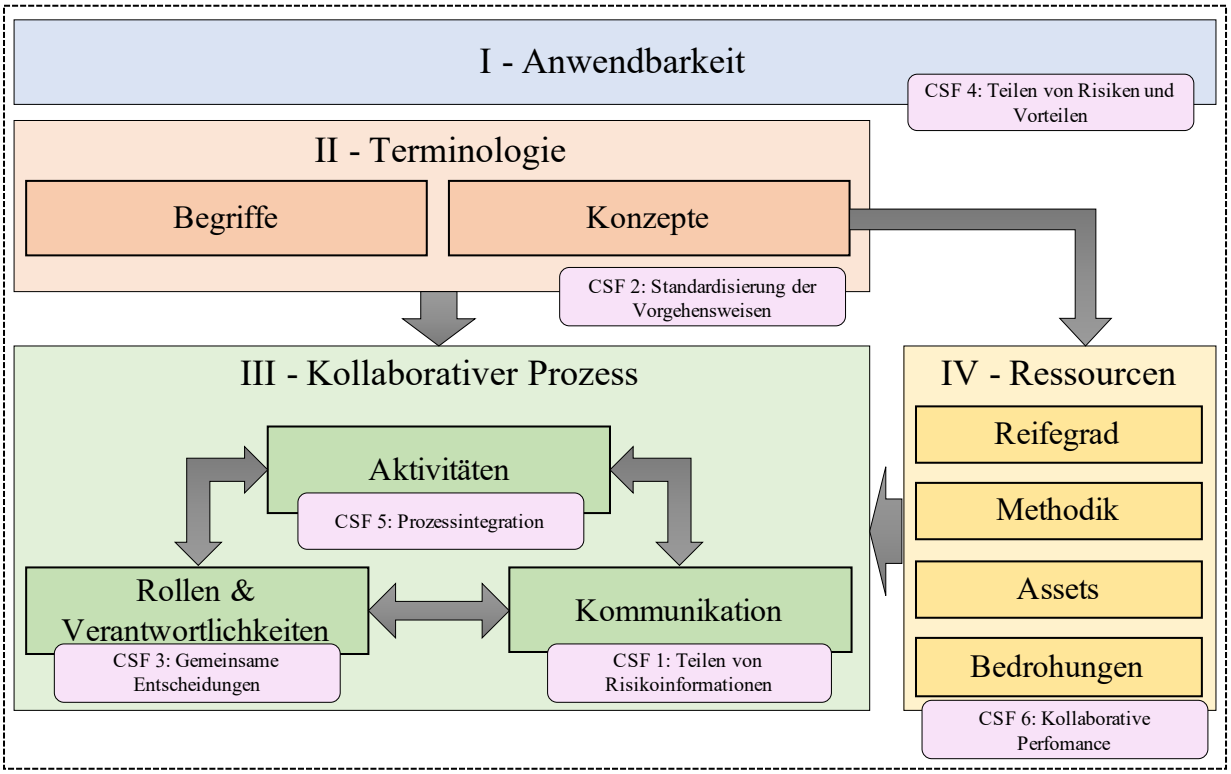
CSF 5: Prozessintegration
CSF 5 zielt auf ein möglichst liberales Prozessmodell ab. Dabei soll ein kollaborativer Prozess innerhalb der Allianz existierende ISRM Implementierungen der Partner integrieren, ohne deren internes ERM negativ zu beeinflussen. In Komponente III kommen an dieser Stelle die Aktivitäten des kollaborativen Prozesses zum Tragen. Das erstellte Prozessmodell wurde so gestaltet, dass es auf den Aktivitäten eines generischen Prozessmodells aufbaut. Dadurch wurden lediglich fünf Kernaktivitäten verwendet, die grundsätzlich Kompatibel zu den meisten ISRM Prozessen sein sollten.

CSF 6: Kollaborative Leistungssysteme
Letztlich soll CSF 6 das Risikoniveau der Allianz für alle Partner transparent gestalten und die Auswirkungen von Bedrohungen nachvollziehbar machen. Dies wurde als wichtiger Faktor erkannt, da die Allianz nur von einem gemeinsamen CISRM profitieren kann, wenn auch die Leistung der Partner miteinander vergleichbar ist. Dieser Aspekt wurde daher in Komponente IV, den unterstützenden Ressourcen berücksichtigt. Darin sind Vorschläge enthalten, um die Inputs in den Prozess möglichst transparent zu gestalten und alle Elemente vergleichbar zu machen.

Darstellung

Gemäß dieser Analyse lassen sich die CSF schematisch auf das kollaborative Framework (Abbildung 8.1) abbilden, wie in Abbildung 8.2 dargestellt. Es ist zu sehen, dass nicht jeder CSF von genau einer Komponente erfüllt wird, sondern CSF 1, CSF 3 und CSF 5 alle drei im kollaborativen Prozess berücksichtigt wurden. Insgesamt konnten jedoch alle sechs CSF durch das Framework realisiert werden, sodass das zugrunde liegende Ziel (Tabelle 3.1) erfüllt werden kann. Somit enthält das Framework alle Aspekte, die gemäß der Literatur [29] von einem CRM zu erwarten wären.

Abbildung 8.2: Mapping der CSFs auf das kollaborative Framework



8.1.3 Abgleich mit dem Anforderungskatalog

Basierend auf den CSFs und den kollaborativen Szenarien wurden in Kapitel 3 konkrete Anforderungen an das Framework definiert, welche in Tabelle 3.2 gelistet sind. Während die CSFs bestimmte Bereiche beschreiben, die das Framework zwingend abdecken muss, damit das etablierte CISRM wirksam sein kann, enthalten die Anforderungen spezifische Forderungen, wie der Prozess etabliert sein muss, um erfolgreich zu sein.

R1.1 *Die Risikoeinschätzung der Partner muss zu vergleichbaren Risiken führen.*
Für die Kommunikation ist es wichtig, dass die Risiken innerhalb der Allianz vergleichbar sind. Dies wird im Prozess durch das Festlegen einer gemeinsamen Methode sichergestellt, was Teil der Aktivität *Risiken einschätzen* (Abbildung 6.4) ist. Ein Vorschlag für eine generische Methodik liefern die unterstützenden Ressourcen.

R1.2 *Es muss geregelt sein, welche Risiken innerhalb der Allianz relevant sind*
Nur wenn die Organisationen wissen, welche Art von Risiken sie teilen sollen, können ihre Partner davon profitieren. Dies wird ebenfalls durch die Aktivität *Risiken einschätzen* (Abbildung 6.4) adressiert, welche auch dafür sorgt, dass relevante Bedrohungen für die Allianz ausgewählt werden.

R1.3 *Es muss ein strukturiertes Vorgehen existieren, um Risikoinformationen zwischen den Partnern auszutauschen.*
Es muss einen klar definierten Weg geben, um Risiken innerhalb der Allianz zu kommunizieren. Auch hier liefert der Prozess als Teil von *Risiken einschätzen* (Abbildung 6.4) einen klaren Kommunikationspfad und den *CISRM Beauftragten* als verantwortliche Rollen. Eine Hilfestellung, um Risikoinformationen anhand der Bedrohungen aufeinander abzubilden, liefern die unterstützenden Ressourcen.

R2.1 *Die Partner müssen im CISRM über eine einheitliche Sprache verfügen.*
Die Kommunikation im Rahmen des CISRM muss innerhalb der Allianz nachvollziehbar sein. Daher liefert die Terminologie eine Liste von Kernbegriffen (Tabelle 5.1), welche die Unklarheit zwischen verschiedenen semi-standardisierten Begriffe beseitigt.

R2.2 *Die Kernelemente des ISRM müssen innerhalb der Allianz standardisiert sein.*
Obwohl nicht direkt in das ISRM der Partner eingegriffen werden sollen, so muss innerhalb der Allianz klar sein, wie die jeweils anderen Konzepte funktionieren. Analog zu den Begriffen liefert die Terminologie eine Übersicht der für das CISRM notwendigen Schlüsselkonzept (Abbildung 5.2). Dies hilft den Partnern ein einheitliches Verständnis von den ISRM Konzepten zu erhalten. Die unterstützenden Ressourcen liefern außerdem konkrete Vorschläge zu Standardisierung von Assets innerhalb der Allianz.

R2.3 *Die internen Prozesse der Partner dürfen nicht durch die einheitliche Sprache [R2.1] oder standardisierten Elemente [R2.2] beeinträchtigt werden.*
Damit ein interorganisationaler Prozess zu den existierenden Enterprise-Prozessen kompatibel ist, darf er keine komplett neue Sprache fordern. Daher enthalten die definierten Kernbegriffe (Tabelle 5.1) lediglich ein Mapping von häufigen ISRM Begriffen. Dies erlaubt es den Partnern innerhalb der Allianz einheitlich zu kommunizieren und dies auf die interne Sprache abzubilden.

R3.1 *Über relevante Risiken [R1.2] muss innerhalb der Allianz entschieden werden.*
Kern den CISRM ist es, die Risikobehandlung von einer einzelnen Organisation auf die Allianz zu übertragen. Daher liefert der Prozess in der Aktivität *Risiko behandeln* (Abbildung 6.5) einen Weg, Risiken zu übermitteln und gemeinsam Freizugeben.

R3.2 *Jeder Partner muss Einfluss auf die Freigabe der Risikobehandlung haben.*
Die Übernahme der Entscheidungsgewalt über die Risikobehandlung stellt einen Eingriff in die Autonomie der Organisationen dar, welche nur akzeptiert wird, wenn alle Partner auch an der Entscheidung mitwirken dürfen. Daher sind im Prozess alle Partner gleichermaßen mit eingebunden. Dazu existiert die neue Rolle des *Allianz Risiko Boards*, welche von Vertretern der Partner besetzt ist.

R3.3 *Die Entscheidungsfindung muss die Autonomie der Partner bei der Risikobehandlung gewährleisten.*
Trotz der Kollaboration innerhalb der Allianz handelt es sich bei den Partnern um unabhängige Organisationen, die auch im Kontext der Zusammenarbeit selbständig agieren wollen. Dies wurde im Prozess zu berücksichtigt und den Partnern wurden möglichst viele Freiheiten eingeräumt. Trotzdem liegt es in der Idee des CISRM, dass die Partner durch die Zusammenarbeit ihr Sicherheitsniveau verbessern. Deshalb bleibt eine Selbstverpflichtung zur Einhaltung der getroffenen Entscheidungen notwendig.

R4.1 *Die Partner müssen ein Interesse am Erfolg der Allianz haben.*
Eine Grundvoraussetzung für eine Zusammenarbeit im CISRM ist es, dass die Partner überhaupt am Wohlergehen der Allianz und der Organisationen darin haben. Da das nichts ist, was innerhalb des Einflussbereiches des ISM liegt, ist es eine Vorbedingung für den Aufbau eines gemeinsamen Prozesses. Das Partnerschaftsmodell (Abbildung 4.4) definiert die notwendigen Eigenschaften für eine Allianz, die sicherstellen, dass dieses Interesse auch gegeben ist.

R4.2 *Jeder Partner muss einen Vorteil durch die Reduktion von IS-Risiken haben.*
Analog zum Interesse an der Allianz müssen die Partner auch direkt von der Risikoreduktion durch das CISRM profitieren. Auch hier helfen die im Partnerschaftsmodell (Abbildung 4.4) definierten Eigenschaften. Insbesondere durch die gegenseitige Abhängigkeit und gemeinsamen Ziel ist sichergestellt, dass die Reduktion von Risiken auch vorteilhaft für die Partner ist.

R4.3 *Die Allianz muss das gemeinsame Umsetzen von Maßnahmen ermöglichen.*
Ein weiterer Vorteil, den die Allianz im CISRM liefern kann, ist es auch gemeinsame Maßnahmen zur Reduktion von Risiken zu implementieren. Der kollaborative Prozess enthält dazu die Aktivität *Behandlung umsetzen* (Abbildung 6.6), welche übergreifende Maßnahmen koordiniert.

R5.1 *Ein Prozessmodell für das CISRM muss kompatibel zu etablierten ISRM Standards und Frameworks sein.*
Das ISRM wurde bereits von vielen nationalen und internationalen Organisationen standardisiert. Deren Vorgaben sind weit verbreiten und werden von den meisten Organisationen umgesetzt, weshalb an dieser Stelle kein völlig neues Vorgehen definiert werden sollte. Dies wurde dadurch berücksichtigt, dass das Prozessmodell auf Basis eines generischen Prozesses (Abbildung 6.2) definiert wurde, welches von den bekanntesten Frameworks abgeleitet wurde. Die verwendeten Aktivitäten sollten damit bereits Teil jedes ISRM sein.

R5.2 *Ein bereits implementierter Prozess muss einfach erweiterbar sein.*
Wenn Organisationen im ISRM zusammenarbeiten wollen, dann haben sie bereits einen internen Prozess etabliert, den sie auch weiterhin verwenden wollen. Das CISRM

stellt nicht viele Anforderungen an den existieren Prozess. Es werden einige zusätzliche Rollen definiert und bekannte Rollen erhalten zusätzliche Verantwortlichkeiten. Die Kommunikationsschnittstellen benötigen zwar organisatorische Änderungen, aber das Vorgehen erfordert keine grundlegenden Änderungen am existierenden ISRM.

R5.3 *Das CISRM muss den Partnern weiterhin die Ausführung ihrer internen Prozesse ermöglichen und darf diese nicht beeinträchtigen.*
Unabhängig vom gemeinsamen CISRM werden die Partner weiterhin ihre internen Prozesse unabhängig voneinander ausführen wollen. Der erstellte kollaborative Prozess (Abbildung 6.8) stellt daher lediglich ein Bindeglied dar, welches die unabhängigen ISRM Prozesse miteinander verknüpft. Durch die einheitliche Terminologie können diese leicht integriert werden.

R6.1 *Das Sicherheitsniveau der Allianz muss sich durch das CISRM langfristig verbessern lassen.*
Ziel des CISRM ist es, durch die das Teilen von Risikoinformationen und die koordinierte Risikobehandlung das Sicherheitsniveau der Allianz zu erhöhen. Daher schlägt das Framework die Durchführung einer IS-Reifegradbewertung als Teilnahmebedingung für den gemeinsamen Prozess vor. Dabei sollte die Reife der Partner in den wichtigsten ISM Kategorien (Abbildung 7.1) berücksichtigt werden. Der homogene Reifegrad führt dazu, dass die Partner maximal von den geteilten Risikoinformationen profitieren können. Gleichzeitig herrscht innerhalb der Allianz ein vergleichbares Bedürfnis nach Sicherheitsmaßnahmen. Auf dieser einheitlichen Basis erlaubt das CISRM den Organisationen ihr Sicherheitsniveau gemeinsam zu verbesserb.

R6.2 *Die IS-Assets der Partner müssen miteinander vergleichbar sein.*
Da das klassische ISRM wertebasiert ist, stellen verschiedene Organisationen mit unterschiedlichen Assets eine Herausforderung für die Vergleichbarkeit dar. Das Framework schlägt daher die Definition von vergleichbaren Asset-Kategorien (Tabelle 7.1) vor, um verschiedene Assets aufeinander abbilden zu können. Dies erleichtert die Verwendung der geteilten Risikoinformationen.

R6.3 *Die Partner müssen das Bedrohungsmodell der Allianz verstehen.*
Innerhalb der Allianz sollte es ein ähnliches Verständnis für die Kritikalität von Bedrohungen geben, um die Risikobewertung zu verbessern. Daher sieht der Prozess in der Aktivität *Risiken und Maßnahmen überwachen* (Abbildung 6.7) explizit die Erstellung und Verteilung eines Bedrohungsmodells vor, welches bei der Einschätzung von Risiken hilft. Die generische Methode aus den unterstützenden Ressourcen unterstützt die Klassifikation letztlich.

Ergebnis Tabelle 8.1 zeigt das Ergebnis des Abgleichs des Frameworks mit dem Anforderungskatalog. Es zeigt sich, dass alle Anforderungen an das CISRM erfüllt werden können. Somit ist das Framework grundsätzlich geeignet, einen kollaborativen Prozess im interorganisationalen Kontext zu etablieren.

Tabelle 8.1: Abgleich des Frameworks mit dem Anforderungskatalog

ID	Anforderung	Komponente	Erfüllt
R1.1	Die Risikoeinschätzung der Partner muss zu vergleichbaren Risiken führen.	K1, K4	Ja
R1.2	Es muss geregelt sein, welche Risiken innerhalb der Allianz relevant sind.	K3	Ja
R1.3	Es muss ein strukturiertes Vorgehen existieren, um Risikoinformationen zwischen den Partnern auszutauschen.	K3, K4	Ja
R2.1	Die Partner müssen im CISRM über eine einheitliche Sprache verfügen.	K2	Ja
R2.2	Die Kernelemente des ISRM müssen innerhalb der Allianz standardisiert sein.	K2, K4	Ja
R3.3	Die internen Prozesse der Partner dürfen nicht durch die einheitliche Sprache [R2.1] oder standardisierten Elemente [R2.2] beeinträchtigt werden.	K2	Ja
R3.1	Über relevante Risiken [R1.2] muss innerhalb der Allianz entschieden werden.	K3	Ja
R3.2	Jeder Partner muss Einfluss auf die Freigabe der Risikobehandlung haben.	K3	Ja
R3.3	Die Entscheidungsfindung muss die Autonomie der Partner bei der Risikobehandlung gewährleisten.	K3	Teils
R4.1	Die Partner müssen ein Interesse am Erfolg der Allianz haben.	K1	Ja
R4.2	Jeder Partner muss einen Vorteil durch die Reduktion von IS-Risiken haben.	K1	Ja
R4.3	Die Allianz muss das gemeinsame Umsetzen von Maßnahmen ermöglichen.	K3	Ja
R5.1	Ein Prozessmodell für das CISRM muss kompatibel zu etablierten ISRM Standards und Frameworks sein.	K3	Ja
R5.2	Ein bereits implementierter Prozess muss einfach erweiterbar sein.	K2, K3	Ja
R5.3	Das CISRM muss den Partnern weiterhin die Ausführung ihrer internen Prozesse ermöglichen und darf diese nicht beeinträchtigen.	K2, K3, K4	Ja
R6.1	Das Sicherheitsniveau der Allianz muss sich durch das CISRM langfristig verbessern lassen.	K3, K4	Ja
R6.2	Die IS-Assets der Partner müssen miteinander vergleichbar sein.	K4	Ja
R6.3	Die Partner müssen das Bedrohungsmodell der Allianz verstehen.	K4	Ja

8.1.4 Diskussion der Ergebnisse

In diesem Abschnitt wurde eine Bewertung des CISRM Frameworks auf Basis der CSF und Anforderungen durchgeführt. Der Abgleich hat gezeigt, dass das Framework alle geforderten Aspekte berücksichtigt. Somit ist es grundsätzlich dazu geeignet, ein funktionierendes CISRM zu etablieren.

CSF

Alle CSF konnten erfolgreich auf die vier erstellten Komponenten abgebildet werden. Damit ist das Framework zumindest im Sinne der Literatur ‚vollständig' und enthält alle Bestandteile, die von einem CISRM zu erwarten sind. Dabei bleibt zu berücksichtigen, dass diese CSF aus den Beobachtungen von Friday et al. [29] für das CRM abgeleitet wurden. Da bis heute jedoch kein tatsächlicher CRM Prozess existiert ist unklar, ob diese tatsächlich vollständig sind.

Anforderungen

Die Anforderungen können fast alle als erfüllt betrachtet werden. Lediglich R3.3 konnte nur teilweise erfüllt werden. Hier war die Anforderung, die Autonomie der Partner bei der Risikobehandlung zu gewährleisten. Obwohl in Komponente III ein Prozessmodell definiert wurde, welches die Unabhängigkeit der Partner berücksichtigt, sind diese nicht vollständig frei. Die Allianz legt am Anfang die Kriterien fest, welche Risiken mit der Allianz geteilt und welche einer gemeinsamen Risikobehandlung unterzogen werden. Die Entscheidung über diese Risikobehandlung trifft das *Allianz Risiko Board*, in dem allen Partner vertreten sind. Nun ist es obligatorisch, dass die Partner die getroffene Entscheidung auch akzeptieren und umsetzen. Wenn sich nicht alle Teilnehmer des CISRM zur Einhaltung der durch das Board gewählten Risikobehandlung verpflichten, dann kann das gemeinsame Vorgehen nicht erfolgreich sein. Trotz dieser Einschränkung, sollte sich daraus in der Praxis jedoch kein Problem ergeben. Bereits durch die Voraussetzung, dass es sich bei der Allianz um eine kollaborative Beziehung handeln muss, sind wichtige Eigenschaften sichergestellt. Neben der gegenseitigen Abhängigkeit und der Nähe der Organisationen sorgt insbesondere das Vertrauen zwischen den Partnern (Goodwill Trust) dafür, dass diese sich gegenseitig unterstützen und schützen wollen. Es ist daher davon auszugehen, dass die Organisationen gewillt sind, einen Teil ihrer Entscheidungsgewalt an die Allianz zu übertragen und gleichzeitig, dass die anderen Partner nichts gegen den Willen eines anderen Partners entscheiden werden.

Abschluss

Somit lässt sich sagen, dass das CISRM Framework vollständig im Sinne der Themenstellung und Anforderungsanalyse ist. Die einzelnen Komponenten liefern jeweils einen Mehrwert, der das ISRM erweitert und Funktionen, die bereits unabhängig genutzt werden können. Jedoch helfen sie erst zusammen dabei, einen interorganisationalen Prozess zu etablieren, um mehrere ISRM Prozesse zu verknüpfen. Im folgenden Abschnitt wird nun erklärt, wie eine Allianz das Framework in Praxis anwenden kann.

8.2 Fallbeispiel: CISRM im GÉANT Projekt

Nachdem nun das komplette Framework beschrieben und auf Vollständigkeit geprüft wurde, soll in diesem Abschnitt dessen Anwendung beschrieben werden. Dazu wird der Aufbau eines kollaborativen Prozesses beispielhaft anhand einer realen Allianz skizziert. Als Fallbeispiel dient dabei das GÉANT Projekt, welches bereits in Kapitel 3.2 vorgestellt wurde. Nachfolgend werden die einzelnen Schritte beschrieben, welche GÉANT unternehmen muss, um ein CISRM zu etablieren. Der grundsätzliche Ablauf ist im SIPOC-Diagramm[1] in Abbildung 8.3 grafisch dargestellt. Das Vorgehen wird nun auf die Situation im GÉANT Projekt angewendet.

8.2.1 Anwendbarkeit des CISRM in der Allianz prüfen

Der erste Schritt beginnt mit der Prüfung, ob die IOR für ein CISRM geeignet ist. Dies ist die Vorbedingung, um überhaupt mit dem Aufbau eines kollaborativen Prozesses zu beginnen. Stimmen die Rahmenbedingungen der Beziehung nicht, dann ist ein Erfolg des CISRM unwahrscheinlich. An dieser Stelle kommt die erste Komponente des Frameworks zum Einsatz.
Die Anwendbarkeit des CISRM in einer IOR wird mit Hilfe des Partnerschaftsmodells (Abbildung 4.4) geprüft. Dabei kann GÉANT wie folgt eingeschätzt werden:

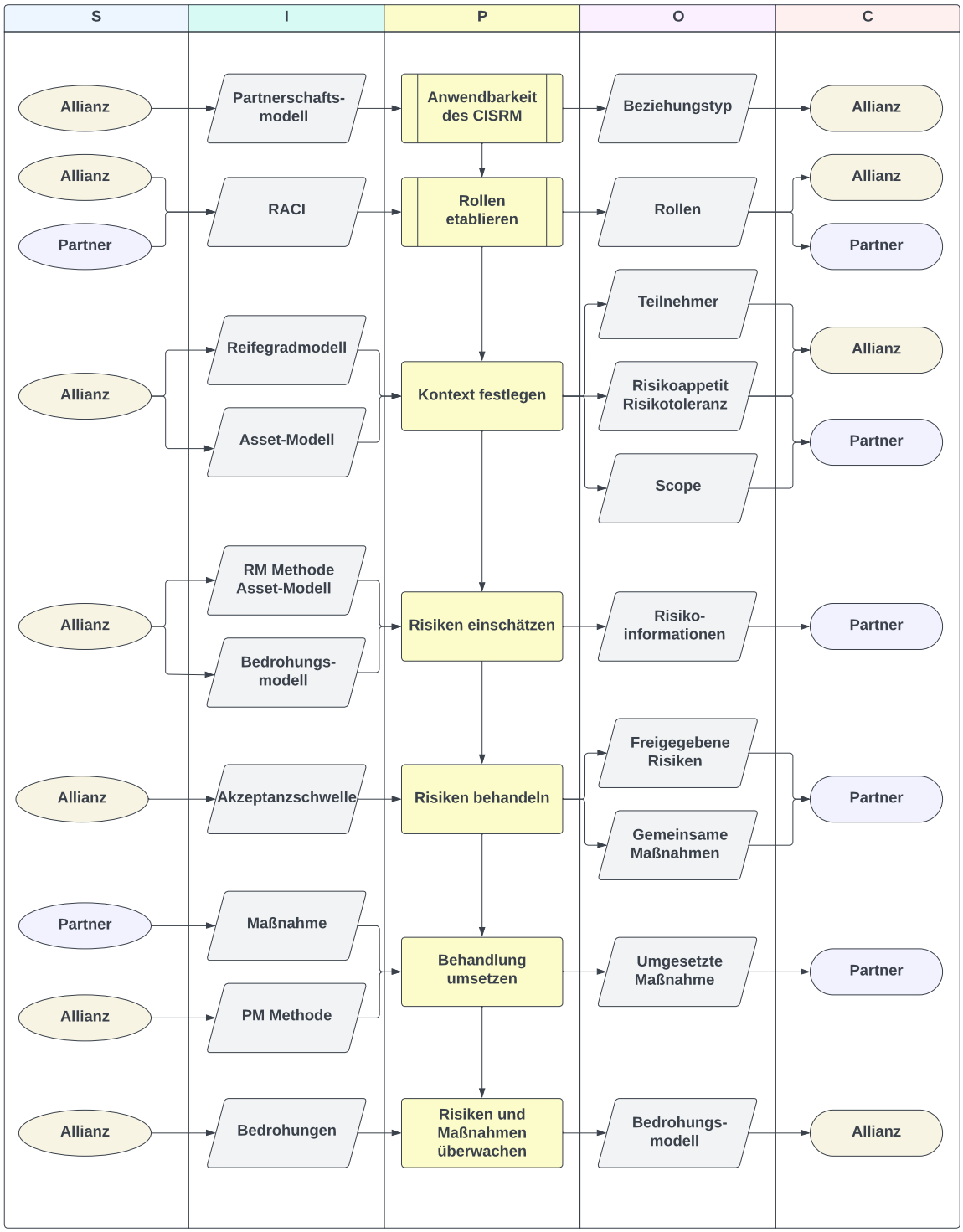
Interesse Das Geschäftsziel eines NREN ist es, den R&E Einrichtungen im eigenen Land die notwendige digitale Infrastruktur und darauf basierende Services bereitzustellen, um Bildung und Lehre zu fördern. Die NRENs arbeiten in verschiedenen Themenfeldern zusammen, die direkt deren Geschäftsziele unterstützen, welche für alle Partner gleich sind. Die Ziele der NRENs sind somit nicht nur aneinander ausgerichtet, sondern größtenteils dieselben.

Abhängigkeit Im Kontext von GÉANT werden unter anderem interorganisationale Services bereitgestellt, insbesondere das gemeinsame Netz, welche keiner der Partner alleine erbringen könnte. Die Zusammenarbeit ermöglicht den Organisationen an vielen stellen erst ihr Geschäftsmodell. Gleichzeitig werden die föderierten Services jedes NRENs wertvoller, je mehr Partner beteiligt sind. Somit ist eindeutig eine gegenseitige Abhängigkeit gegeben.

Nähe Da die NRENs in verschiedenen Staaten agieren, existiert keine geografische Nähe. Dafür ist eine hohe technologische Nähe gegeben, da die Partner sowohl im gleichen Sektor operieren als auch ihren Kunden ähnliche Produkte bereitstellen. Weiterhin herrscht bei den NRENs eine vergleichbare Unternehmenskultur. Dabei haben sich die Organisationen durch die bereits lange bestehende Zusammenarbeit sehr stark aneinander angepasst. Eine sehr hohe organisatorische Nähe ist erkennbar. Insgesamt ist eine hohe Nähe zwischen den Partnern gegeben.

[1] Lean Six Sigma Werkzeug aus dem Supplier Management zur abstrakten Darstellung von Geschäftsprozessen mit den Werten Supplier, Input, Process, Output und Customer

Abbildung 8.3: Darstellung der einzelnen Schritte zum Etablieren des CISRM



Autorität Wie bereits angesprochen handelt es sich bei GÉANT an sich um ein vertragsbasiertes Joint Venture. Die Teilnahme daran ist freiwillig und etabliert keinen Einfluss über die gemeinsamen Aktivitäten hinaus. Abstimmungen zum gemeinsamen Vorgehen werden demokratisch und gleichberechtigt getroffen. Die gesamte Zusammenarbeit basiert auf institutionellem Vertrauen zwischen den NRENs, sowie persönlichem Vertrauen innerhalb der Allianz, welches über viele Jahre etabliert wurde. Somit ist die Autorität definitiv als vertrauensbasiert anzusehen.

Vertrauen Durch die jahrelange Zusammenarbeit in der gleichen Branche und an ähnlichen Projekten, ist ein Vertrauen in die Kompetenzen der Partner auf jeden Fall gegeben. Darüber hinaus ist die Zusammenarbeit allerdings auch darauf ausgerichtet, als Allianz langfristig erfolgreich zu sein. Viele Teilnehmer investieren Ressourcen in das Projekt, ohne davon einen sofortigen oder direkten Vorteil zu erhalten. Es kann somit argumentiert werden, dass das Vertrauen in den guten Willen bei der Partner vorhanden ist.

Somit erfüllt GÉANT alle Eigenschaften einer kollaborativen Beziehung. Die Allianz ist daher geeignet, um ein gemeinsames CISRM zu etablieren und kann die notwendigen Schritte zum Aufbau eines interorganisationalen Prozesses einleiten.

8.2.2 Rollen & Verantwortlichkeiten etablieren

Es gilt nun die benötigten Rollen für den Prozess festzulegen. Dabei handelt es sich um eine mehrstufige Aufgabe vor und während des Prozesses. Als Erstes muss die Allianz die Entscheidung treffen, ein CISRM aufzubauen. Bereits beim Aufbau des Prozesses müssen bereits das Steering Comittee und der (Interims) Allianz Risiko Manager bestimmt werden, da diese eine aktive Rolle beim Festlegen des Anwendungsbereichs spielen. Da das Allianz Risiko Board aus Vertretern der Teilnehmer bestehen soll, kann dieses erst etabliert werden, wenn die Partner für das CISRM ausgewählt wurden. Analog können auch die Rollen in den Organisationen erst nach Festlegen des Anwendungsbereichs etabliert werden. Der genaue Ablauf der Aktivitäten ist im Prozessmodell (Abbildung 6.8) dargestellt. Zur vereinfachten Darstellen werden nun jedoch alle Rollen beschrieben und anschließend erst der Kontext erklärt.

Rollen der Allianz

Steering Comittee

Als Erstes muss das Steering Comittee definiert werden, welches die weiteren Rollen legitimiert. Ein solches Gremium ist üblicherweise bereits vorhanden, da es notwendig zur Steuerung der gemeinsamen Unternehmung ist. In GÉANT existiert als oberstes Kontrollorgan die *General Assembly*, welche mit Vertretern aller NRENs besetzt ist und das Projekt steuert. Es ist daher naheliegend, dieses Gremium zu nutzen und ihm die Rolle des CISRM Steering Comittee im CISRM zuzuweisen. Die General Assembly beschließt somit im ersten Schritt den Aufbau eines CISRM in GÉANT. Anschließend ernennt sie einen Risiko Manager, welcher mit dem Aufbau des Prozesses beauftragt wird.

Risiko Manager

Wie beschrieben gibt es zwei verschiedene Optionen, den Allianz Risiko Manager zu bestimmen (Abschnitt 6.3). Entweder als wechselnde Rolle zwischen den Partnern oder als feste Position bei einem der Partner. Durch die besondere Konstellation, dass es zum GÉANT Projekt auch noch die GÉANT Association gibt, bietet es sich an, die Rolle des Risiko Managers fest zu vergeben. Als Verband ist die GÉANT Association im Besitzt ihrer Mitglieder und wird durch diese finanziert, stellt allerdings trotzdem eine unabhängige Organisation dar. Sie ist damit in einer optimalen Position, den Risiko Manager für die Allianz dauerhaft zu stellen. Dies reduziert den Mehraufwand durch zusätzliche Koordination und sorgt für einen konsistenten Prozess.

Risiko Board

Das Risiko Board selbst ist zwar eine formale Rolle der Allianz, besteht in seiner Gesamtheit allerdings vollständig aus Vertretern der Partner. Es liegt damit in der Verantwortung der einzelnen NRENs einen Repräsentanten in das Risiko Board zu entsenden. Die Person sollte auch innerhalb der Organisation die notwendigen Kompetenzen besitzen, um über die Behandlung von Risiken entscheiden zu dürfen. Die meisten NRENs haben bereits einen Chief Information Technology Officer (CISO) bestimmt, der oftmals sogar schon im Rahmen der *Special Interest Group Information Security* mit GÉANT verbunden ist. Er stellt damit einen guten Kandidaten dar, um diese Rolle zu übernehmen.

Projektmanager

Wie auch beim Risiko Manager bietet es sich in GÉANT an, einen Projektmanager innerhalb der Association einzusetzen. Da die genutzte Projektmanagementmethode nicht vorgegeben ist, gibt es hierbei keine Einschränkungen. Die Association hat bereits ein Partner Relations Team etabliert, welches in Kontakt mit allen NRENs steht und bereits jetzt interorganisationale Aktivitäten koordiniert. Es ist somit naheliegend, den CISRM Projektmanager in diesem Team anzusiedeln, da er hauptsächlich koordinierende Aufgaben zwischen den Maßnahmen Ownern übernimmt.

Rollen der Organisation

Standardrollen

Neben den neuen Rollen für die Allianz müsse auch die Organisationen bestimmte Rollen definieren oder deren Verantwortlichkeiten erweitern. Da bereits bei allen Partnern ein ISRM vorhanden sein muss (was eine Vorbedingung für ein CISRM ist), sollten in der Organisation bereits Rollen wie Asset Owner, Maßnahmen Owner, Risiko Manager und Risiko Owner bekannt sein. Hier muss lediglich Awareness für den kollaborativen Prozess geschafften werden und den Personen die neuen Aufgaben hinsichtlich Kommunikation erklärt werden.

CISRM Beauftragter

Neu dazu kommt lediglich die Rolle des CISRM Beauftragten, der die Kommunikation im kollaborativen Prozess übernimmt. Da es sich bei den NRENs um Kleine und mittlere Unternehmen (KMU) ohne riesige Sicherheitsteams handelt, ist anzunehmen, dass sie diese Rolle zusätzlich dem internen Risiko Manager zuweisen.

8.2.3 Kontext des Prozesses festlegen

Nach dem Vergeben der Rollen Steering Comittee und Allianz Risiko Manager wird der gemeinsame Prozess etabliert (Abbildung 6.8). In der ersten Aktivität geht es darum den Kontext des CISRM festzulegen. Das bedeutet für die Allianz die Teilnehmer für den Prozess auswählen und für die Organisationen, die Assets auszuwählen die im Scope des Prozesses sind. Anschließend müssen beide Entitäten ihren Risikoappetit und Risikotoleranz aufeinander abstimmen.

Allianz/GÉANT

Teilnehmer

Das bedeutet für die Allianz zunächst die Partner auszuwählen, welchem am gemeinsamen Prozess teilnehmen sollen. Dazu wählt die Allianz ein Reifegradmodell aus, um die Partner mit dem passenden ISM Reifegrad auszuwählen. In GÉANT wurde bereits zuvor die *Security Baseline for NRENs* als Standardmodell etabliert, dessen Einsatz bereits seit mehreren Jahren stark beworben wird [236, 227]. Somit liegt es nahe, dieses für die Allianz bereits angepasste Reifegradmodell auch für das CISRM zu verwenden. Darin wird die erste Stufe als Baseline-Level bezeichnet, welches die meisten NRENs erfüllen sollten[2]. Es liefert damit eine solide Zugangsvoraussetzung für die Teilnahme am kollaborativen Prozess, da es sicherstellt, dass die Partner zumindest die wichtigsten ISM Prozesse etabliert haben. Das Steering Comittee einigt sich auf diesen Reifegrad und fordert anschließend von allen NRENs eine Reifegradbewertung anhand der Baseline, um sich als Teilnehmer zu qualifizieren.

Werte festlegen

Im nächsten Schritt muss die Allianz für sie sinnvolle Werte für Risikoappetit und Toleranz definieren. Diese Aufgabe wird durch das vorher bestimmte Risiko Board übernommen. An dieser Stelle hätte die Allianz die Möglichkeit, besondere Anforderungen an das Risikoniveau basierend auf ihrer Branche oder Umgebung zu etablieren. GÉANT bewegt sich im Bereich R&E und ist damit in einer Vergleichsweise unkritischen Branche tätig und benötigt kein übermäßig strenges Vorgehen. Gleichzeitig wurde bisher keine besonders scheue Haltung (Risikoaversion) beobachtet, während GÉANT als nicht-gewinnorientiertes Projekt auch nicht die Möglichkeiten hat übermäßige Risiken einzugehen (Risikoaffinität), weshalb eher ein mittlerer Risikoappetit (Risikoneutral) angebracht ist. Aufgrund dieser Rahmenbedingen wird auch beim Festlegen der Risikotoleranz empfohlen, sich an den Standardwerten der ENISA Methode (Kapitel 7) zu orientieren. Die Toleranz der qualitativen Risikomethode wird damit auf *sehr hoch* gesetzt.

[2]GÉANT strebt an, dass 80% der NRENs zeitnah das Baseline-Level erreichen: „This level defines a GÉANT wide minimum of security and is expected to be met by most NRENs by default and implemented by all NRENs in the short term“ [156]. In der Realität wurde dieses Ziel jedoch noch nicht erreicht und die Allianz muss erst noch Zeit in die Erhöhung des Reifegrades investieren.

Organisationen/NRENs

Scope Aufseiten der NRENs beginnt die Aktivität mit dem Festlegen des Scopes des CISRM innerhalb der Organisation. Während es bei großen Unternehmen sicherlich sinnvoll ist zu betrachten, ob alle Assets im Scope des Prozesses sein sollten, gestaltet sich dies bei NRENs eher einfach. Letztlich handelt es sich bei den NREN um KMU im Bereich R&E ohne Nebentätigkeiten. Damit ist zu erwarten, dass alle Assets potenziell relevant für die Allianz sind. Trotzdem sollte die Allianz im Kontext der Scope-Definition das Mapping auf die Standard-Asset-Kategorien durchführen ((Kapitel 7)), um die Verknüpfungen zu etablieren und eventuell organisationsspezifische Assets zu identifizieren.

Werte Hier zeigt sich der Zusammenhang zwischen den festgelegten Werten für Risikoappetit und Toleranz der Allianz und der Partner. GÉANT besitzt einen mittleren Risikoappetit, damit ist es für die Zusammenarbeit besser, wenn die Allianz eine ähnliche Einstellung hat. Ein sehr unterschiedlicher Risikoappetit würde eine Einigung im Risiko Board erschweren, aber nicht verhindern. Strenger ist es bei der Risikotoleranz, welche eine maximale Grenze für die Organisation definiert. Hier kann jedes NREN zwar einen eigenen Wert festlegen, dieser darf *sehr hoch* (abgebildet auf die gemeinsame Methode) allerdings nicht überschreiten.

8.2.4 Den kollaborativen Prozess durchführen

Somit wurde der kollaborative Prozess etabliert und GÉANT kann mit dem CISRM beginnen. Die Partner führen den Prozess gemäß Abbildung 6.8 durch und berücksichtigen dabei die vereinheitlichten Bedrohungen und Assets. Risiken werden auf Basis der gemeinsamen Methodik bewertet, geteilt und behandelt.

Risiken einschätzen und Informationen teilen

Die NRENs führen im Vordergrund erst einmal ihren internen ISRM Prozess aus. In diesem Zusammenhang werden die IS Risiken weiterhin wie bisher identifiziert und bewertet. Bei der Einschätzung von Risiken kann ein gemeinsames Bedrohungsmodell helfen, da es die geteilten Risikoinformationen der Partner widerspiegelt und so eine infromationsbasierte Bewertung erlaubt. Allerdings stehen weder geteilte Informationen noch ein Bedrohungsmodell beim ersten Durchlauf zur Verfügung, da es erst Iterativ entwickelt wird. Somit sollte sich die Qualität der Risikoeinschätzung bei den NRENs verbessern, je länger der Prozess läuft.

Risiken bewerten Wurden die Risiken intern bewertet, folgt die erste Schnittstelle in den kollaborativen Prozess. Dazu müssen vom CISRM Beauftragten nun die Risiken des NREN ausgewählt werden, die relevant für die anderen Partner sein können. Dazu wird zuerst geprüft, ob die betroffenen Assets im zuvor festgelegten Scope des CISRM sind. Als Nächstes muss geprüft werden, ob die Bedrohungen relevant für die Allianz sind, was aus dem gemeinsamen Bedrohungsmodell hervorgehen sollte. Da GÉANT eine internationale Allianz ist, haben die NRENs keine geografische Nähe. Umgebungsbezogene Risiken sind sehr wahrscheinlich für jedes NREN unterschiedlich und die Partner würden nicht von den geteilten Informationen

profitieren. Auch hier ist zu erwarten, dass diese Informationen in den ersten Iterationen des Prozesses noch nicht klar definiert sind und sich mit dem Bedrohungsmodell der Allianz verbessern. Sind die Risiken relevant für die anderen NRENs, dann teilt der CISRM Beauftragte diese mit GÉANT.

Informationen teilen

Der Allianz Risiko Manager ist nun dafür verantwortlich, dass diese Informationen den anderen NRENs zur Verfügung gestellt werden. Wie der Austausch der Risikoinformationen etabliert wird, ist im Prozess nicht definiert. Es sind sowohl regelmäßige Treffen zwischen den CISRM Beauftragten, eine einfache E-Mail Kommunikation oder komplexe RM Plattformen denkbar. An dieser Stelle bietet sich bei GÉANT das bereits vorhandene Wiki-System an, auf das bereits alle Partnerorganisationen zugreifen können. Die CISRM Beauftragten können ihre Informationen einfach in einem durch den Allianz Risiko Manager moderierten Bereich miteinander teilen. Damit erübrigt sich die Notwendigkeit von Spezialsoftware für den Anfang. Je mehr Risikoinformationen die NRENs miteinander teilen, desto mehr profitiert jede einzelne Organisation wiederum davon.

Gemeinsame Risikobehandlung

Der nächste Schritt ist die Behandlung der Risiken, die grundsätzlich unabhängig von den geteilten Risikoinformationen ist. Bei der ersten Iteration muss eine Risikoakzeptanzschwelle festgelegt werden. Diese definiert, ab welcher Risikohöhe ein Risiko an die Allianz gemeldet werden muss. Im GÉANT Beispiel wird angenommen, dass die Allianz keine besonderen Anforderungen stellt und die ENISA Standardmethode nutzt. Das Risiko Board legt diese nun auf Basis der Methode auf *moderat* fest, d.h. *geringe* und *sehr geringe* Risiken werden nicht im Risiko Board diskutiert.

Relevanz

Die NRENs müssen nun anhand dieser Akzeptanzschwelle die Relevanz der Risiken für die gemeinsame Risikobehandlung prüfen. Dazu muss die interne Risikobewertung mithilfe der gewählten Methode auf die generische Bewertung der Allianz abgebildet werden. Dies erfolgt abhängig von der Bewertungsmethode des NREN als Abbildung auf die Werte der allgemeinen Methode. Ist der abgeleitete Wert *moderat* oder höher, dann muss das Risiko im nächsten Boardmeeting besprochen werden.

Behandlung

Dazu muss ein regelmäßiger Termin etabliert werden, zu dem sich das Risiko Board trifft, um über die Risikobehandlung zu entscheiden. Da es sich bei GÉANT um eine internationale Allianz handelt, macht ein Remote-Meeting Sinn, welches etwa einmal pro Quartal stattfinden kann. Alle von den NRENs als relevant identifizierten Risiken und deren Behandlungsmethode werden an das Board gemeldet. Es besteht nun die Möglichkeit, eine gemeinsame Risikobehandlung zu forcieren oder die Behandlungsoption des NREN zu diskutieren. Das Ergebnis ist ein verbindlicher Risikobehandlungsplan, dem alle NREN Vertreter zugestimmt haben.

Umsetzung

Falls sich das Risiko Board für eine gemeinsame Maßnahme entschieden hat, wird diese zur Projektsteuerung an den zuvor in der GÉANT Association eingesetzten Projektmanager übergeben. Dieser koordiniert die Maßnahme mit den verschiedenen Maßnahmen Ownern der NRENs. Abhängig von der gewählten Projektmanagementmethode wird die Maßnahme (z.B. eine gegenseitige Datensicherung) dann asynchron implementiert und die erfolgreiche Umsetzung anschließend zurückgemeldet. Durch Umsetzung einer solchen Maßnahme ändert sich nicht nur das Sicherheitsniveau einer Organisation, sondern der ganzen Allianz.

Überwachen und Bedrohungsmodell aktualisieren

Am Ende des Prozesses steht die Aktivität *Risiken und Maßnahmen überwachen*. Hier kommt wieder eine Stärke der Kollaboration zu tragen - die Fähigkeit, aus dem gemeinsamen Wissen zu lernen und die eigenen Maßnahmen zu bewerten. Der Risiko Manager von GÉANT nutzt die geteilten Risikoinformationen und Maßnahmen, um das Bedrohungsmodell der Allianz zu aktualisieren. In der Praxis kann GÉANT etwa auf die ENISA Threat Taxonomy [65] zurückgreifen und um Risikoinformationen ergänzen.
Für die NRENs ändert sich in dieser Phase nicht viel im Vergleich zum klassischen ISRM. Zuvor gemeinsam beschlossene und entwickelte Maßnahmen unterscheiden sich an dieser Stelle nicht von unabhängig implementierten Maßnahmen. Der NREN Maßnahmen Owner prüft weiterhin die bereits implementierten Maßnahmen und kontrollieren deren Wirksamkeit, während der Asset Owner die Bedrohungslage überwacht. Dabei können sie allerdings das Bedrohungsmodell der Allianz nun nutzen, welches ihnen Zugriff auf die bisherigen Einschätzungen der Partner verschafft. Mit diesen Informationen beginnt der iterative Prozess wieder von vorne, wodurch sich langfristig das Sicherheitsniveau der Allianz verbessert.

8.3 Zusammenfassung

In den Kapiteln 4, 5, 6 und 7 wurden die einzelnen Komponenten des CISRM Frameworks beschrieben. Jede einzelne davon stellt eine Erweiterung des klassischen ISRM dar, welche in sich bereits einen zusätzlichen Gewinn liefern. Der wahre Mehrwert entsteht jedoch, wenn diese zusammen genutzt werden, um einen kollaborativen Prozess zu etablieren. In diesem Kapitel wurde das Framework daher zusammenfassend dargestellt und evaluiert.
Dabei wurde überprüft, ob das Framework vollständig ist, die vorher festgelegten Anforderungen erfüllt und wie eine Anwendung in der Praxis aussehen könnte. Zusammengefasst wurden in diesem Abschnitt die folgenden Fragestellungen untersucht und diskutiert: Zusammenfassung

- Wie lassen sich die einzelnen Komponenten verknüpfen und als integriertes Framework verwenden (Abschnitt 8.1)?
- Ist das CISRM grundsätzlich geeignet für eine interorganisationale Zusammenarbeit und erfüllt das Framework aller zuvor definierten Anforderungen (Abschnitt 8.1)?
- Wie lässt sich das Framework in der Praxis anwendenden, um einen kollaborativen Prozess für das CISRM in einer Allianz zu etablieren (Abschnitt 8.2)?

Es hat sich gezeigt, dass sich die einzelnen Komponenten sinnvoll miteinander verknüpfen lassen, um ein vollständiges Framework für das CISRM zu erstellen. Der beschriebene Ansatz ist grundsätzlich geeignet ein interorganisationales ISRM innerhalb einer Partnerschaft zu etablieren und erfüllt alle zuvor definierten Anforderungen an ein solches CISRM Vorgehen. Anhand des GÉANT Projektes konnte skizziert werden, welche Schritte eine Allianz unternehmen muss, um den kollaborativen Prozess erfolgreich zu etablieren. Die Beschreibung hat sich dabei auf die organisatorische Perspektive konzentriert, einen Prozess innerhalb der Allianz aufzubauen. Der Einsatz technischer Lösungen innerhalb der Aktivitäten stand dabei nicht im Fokus dieser Arbeit, sie können den Prozess jedoch in der Praxis unterstützen. Lösung
Der größtenteils manuelle Prozess könnte durch den Einsatz von Spezialsoftware digitalisiert werden, etwa für den Austausch der Risikoinformationen oder eine gemeinsame RM Plattform. Es existieren bereits zahlreiche Werkzeuge für das ISRM, wobei die meisten kommerziellen Produkte auf die Nutzung innerhalb einer Organisation ausgerichtet sind. Doch auch die Möglichkeit für die Erstellung von organisationsübergreifenden Softwarelösungen wurden in früheren Forschungsarbeiten bereits ausgiebig erforscht. So stehen bereits seit Jahrzehnten Lösungen für integrierte Managementplattformen [237, 238], interorganisationale Architekturen [188], interorganisationales Dienstmanagement [239] und Implementierungen, etwa auf Basis mobiler Agenten [240], zur Verfügung. Diese Konzepte können auch im CISRM Anwendung finden, um eine interorganisationale Risikoplattform zu entwickeln. Tools
Trotz dieser Verbesserungspotentiale konnte durch die Beantwortung der gelisteten Fragestellungen gezeigt werden, dass das Framework geeignet ist, ein wirksames CISRM zu etablieren. Es liefert damit eine Möglichkeit, das bisher nur intern etablierte ISRM mit den Vorteilen einer strategischen Allianz zu verknüpfen, um das Sicherheitsniveau innerhalb der Partnerschaft zu erhöhen. Das CISRM Framework, seine Komponenten und deren Nutzung ist somit vollständig erörtert. Fazit

Kapitel 9

Zusammenfassung und Ausblick

Durch die jährlich ansteigende Zahl an Sicherheitsvorfällen gewinnt auch das Thema IS in Organisationen jeder Größe zunehmend an Bedeutung. Diese Bedrohungslage betrifft inzwischen alle Bereiche und Branchen weltweit, wodurch der Umgang mit Sicherheitsereignissen zu einem essenziellen Wettbewerbsfaktor geworden ist. Das ISM befasst sich mit dem zielgerichteten Aufbau von strukturierten Sicherheitsprozessen und unterstützt so die ganzheitliche Erhöhung des Sicherheitsniveaus von Organisationen. Internationale Standards und Industrie-Frameworks fordern dabei schon lange ein risikobasiertes Vorgehen, welches auch im Zentrum eines jeden ISMS steht. Das ISRM ist der Prozess der ein solches Vorgehen etabliert und die Risiken innerhalb einer Organisation identifiziert, einschätzt und behandelt.

Ein paralleler Trend zeigt die zunehmende Bedeutung von IORs, von der einfachen Lieferantenbeziehung bis hin zu strategischen Allianzen. In einer globalisierten Wirtschaft können wenige Organisationen noch alleine bestehen und vollkommen isoliert agieren. Die verschiedenen Formen der Kooperation liefern den Organisationen neue Möglichkeiten der Zielerreichung.

Durch die Existenz dieser Partnerschaften bietet sich auch im ISRM die Gelegenheit zur interorganisationalen Zusammenarbeit, welche bisher jedoch nicht untersucht wurde. Das klassische ISRM findet im Kontext eines ERM innerhalb einer einzelnen Organisation statt und stellt diese in den Mittelpunkt der Risikobetrachtung. Erweiterte Methoden wie das SCRM berücksichtigen die IORs einer Organisation, betrachtet diese jedoch nur als weiteren Risikofaktor. Kaum betrachtet wurde jedoch, wie die Teilnehmer einer Allianz sich gegenseitig unterstützen und eine gemeinsame Risikostrategie entwickeln können.

Diese Arbeit präsentierte einen Lösungsversuch, das CISRM, ein interorganisationales Vorgehen für das ISRM. Es adaptiert das existierende Prozessmodell und wendet es auf der Ebene einer Allianz an, um den Partnern die Zusammenarbeit zu ermöglichen. Der Ansatz zielt auf ein Teilen von Risikoinformationen und eine gemeinsame Risikobehandlung innerhalb der Allianz ab. Auf diese Weise soll das Sicherheitsniveau der Allianz als Ganzes und seiner Teilnehmer erhöht werden, indem die Vorteile einer existierenden interorganisationalen Kollaboration für das Management von Risiken verwendet wird.

9.1 Ergebnisse dieser Arbeit

In dieser Arbeit wurde ein Framework erstellt, welches Organisationen beim Aufbau eines gemeinsamen CISRM unterstützt. Dieses definiert kein neues Vorgehen, sondern erweitert die vorhandenen Prozesse, sodass das existierende ERM nicht beeinträchtigt wird. Voraussetzung dafür ist, dass die Partner bereits ein wirksames ISRM etabliert haben. Das erstellte Prozessmodell verknüpft diese unabhängigen Prozesse miteinander, um einen kollaborativen Prozess zu schaffen.
Es handelt sicher daher um ein Meta-Framework, da es im Kern auf existierende IS und RM Frameworks aufsetzt. Dies liefert den Organisationen die notwendige Flexibilität, weiterhin einen internen Prozess zu etablieren, der optimal auf ihre Anforderungen zugeschnitten ist. Letztlich ist diese Freiheit der Kerngedanke des CISRM im Vergleich zum klassischen ISRM, da es auf Partnerschaften unabhängiger Organisationen abzielt. Es ist die Überzeugung des Autors, dass ein kollaboratives Vorgehen auf gegenseitigem Vertrauen basieren und diese Unabhängigkeit unterstützten muss, um langfristig erfolgreich zu sein.
Das Ergebnis der Arbeit sind vier Komponenten, die sich zu einem CISRM Framework verbinden lassen:

I. Anwendbarkeit des Frameworks
   Definiert ein Partnerschaftsmodell, welches zur Bewertung von IORs genutzt werden kann. Basierend darauf lässt sich beurteilen, ob die Allianz geeignet ist, um ein gemeinsames CISRM zu etablieren.

II. Einheitliche Terminologie
   Beschreibt eine generische Terminologie bestehend aus Kernbegriffen und Schlüsselkonzepten des ISRM. Diese etabliert ein vergleichbares Verständnis von Risiken und eine einheitliche Sprache innerhalb der Allianz.

III. Kollaborativer Prozess
   Enthält eine Liste von Aktivitäten mit zugehörigen Rollen & Verantwortlichkeiten und beschreibt deren Kommunikation im Prozessmodell. Allianzen können auf Basis dieser Vorlagen einen ähnlichen Prozess in ihrer Allianz etablieren.

IV. Unterstützende Ressourcen
   Liefert zusätzliche Hilfsmittel zum Aufbau des CISRM in der Allianz. Diese Ressourcen helfen bei der Definition der notwendigen Inputs für den kollaborativen Prozess.

Jede der Komponenten kann unabhängig voneinander genutzt werden und liefert in sich bereits einen Mehrwert für das ISRM. Gemeinsam bilden diese Komponenten jedoch ein Framework mit allen notwendigen Werkzeugen, um einen gemeinsamen Prozess innerhalb einer Allianz zu etablieren. Dass dies gelingen kann, wurde anhand eines Fallbeispiels skizziert, welches auf andere Allianzen übertragbar ist. Somit liefert das vorgestellte CISRM Framework einen ersten Ansatz für das kollaborative Management von Sicherheitsrisiken in strategischen Allianzen.

9.2 Limitierungen der Forschung

Bei der Konzeption des vorgestellten Frameworks wurden möglichst viele Erkenntnisse aus Forschung und Praxis zu existierenden Konzepten des ISRM berücksichtigt. Trotzdem wurden potenzielle Probleme identifiziert und daher ist sowohl das Vorgehensmodell zur Erstellung als auch das Framework selbst nicht ohne Limitierungen.

Nicht-empirische Forschung: Allen voran steht die Problematik, dass es sich beim CISRM selbst und dem dazu erstellten Framework lediglich um ein theoretisches Konzept handelt. Obwohl dies ursprünglich geplant war, hat keine Evaluation in der Praxis stattgefunden. Es hat sich gezeigt, dass das Etablieren interorganisationaler Initiativen sehr komplex und zeitintensiv ist, weshalb eine Umsetzung als Teil dieser Arbeit nicht möglich war. Insbesondere ist ein solches Unterfangen wie bei anderen organisationsweiten (IS) Initiativen nur möglich, wenn diese durch das Top-Management getrieben wird, was im Rahmen einer externen Forschungsarbeit kaum realistisch ist. Somit fällt es schwer zu bewerten, wie praxistauglich der kollaborative Prozess tatsächlich ist. Eventuell ergeben sich bei einem Praxistest neue Herausforderungen, die bisher nicht erkannt wurden. Die Einschränkung ist nicht spezifisch für diese Arbeit, sondern wie bereits von Karlsson et al. [24] festgestellt wurde, ein generelles Problem von (IS) Management Frameworks und aktueller Forschung im Themenbereich, welches es zu lösen gilt.

Austausch sensibler Daten: Das CISRM erfordert grundsätzlich die Bereitschaft zum Teilen vertraulicher und sensibler Informationen innerhalb der Allianz. Dabei handelt es sich um Risikoinformationen, die etwa Auskunft über frühere Sicherheitsvorfälle und existierende Schwachstellen enthalten, welche außerdem Einblick in die Sicherheitsstrategie der Organisation zulassen. Somit stellt sich die Frage, ob Organisationen überhaupt bereit sind, diese Informationen mit ihren Partnern zu teilen. Im Bereich R&E erfolgt Erfahrungsgemäß ein transparenter Umgang mit Sicherheitsvorfällen, wie etwa diverse Ransomware-Vorfälle gezeigt haben, aber andere Branchen sind dabei oftmals zurückhaltender. Zwar werden bei der Anwendbarkeit des Frameworks nur kollaborative Beziehungen berücksichtigt, da diese ein hohes Vertrauen und eine sehr enge Bindung zwischen den Partnern aufweisen. In der Realität ist das trotzdem kein Garant dafür, dass die Organisationen für einen solchen Schritt bereit sind. Dies betrifft insbesondere Wirtschaftsunternehmen, bei denen die Bereitschaft zum Teilen von sensiblen Firmendaten wahrscheinlich geringer ist als im Non-Profit-Sektor. Die Idee eines CISRM hängt damit von der Annahme ab, dass Organisationen tatsächlich zum Teilen dieser Informationen bereit sind.

Ableitung des Prozesses: Eine weitere Einschränkung ist, dass das Prozessmodell für den kollaborativen Prozess von den fünf ISRM Frameworks abgeleitet wurde, die am weitesten verbreitet sind. Der Grund dafür war, dass diese internationalen Standards und Industrie-Frameworks den Großteil der heute in Organisationen implementierten ISRM Prozesse abdecken. Eventuell gibt es trotzdem inkompatible Prozesse, die ein anderes Vorgehen, eine andere Methode oder eine andere Terminologie verwenden. Insbesondere nationale oder branchenspezifische Verfahren könnten somit Schwierigkeiten bei der Prozessintegration aufweisen. Somit ist das Konzept zwar zu den meisten Prozessen kompatibel, aber es ist eventuell nicht universal anwendbar.

9.3 Ausblick und offene Fragestellungen

Auf Basis der Ergebnisse und natürlich auch deren Limitierungen ergeben sich weitere Fragestellungen, welche in zukünftigen Forschungsarbeiten untersucht werden können.

Anwendung des Konzeptes in der Praxis: Aufbauend auf den Ergebnissen wäre es ein essenzieller nächster Schritt, dass Framework in der Praxis anzuwenden. Dazu müssen Organisationen bzw. Allianzen gefunden werden, die bereit sind, dass CISRM als Pilotprojekt zu implementieren. Nur so kann im Rahmen einer Machbarkeitsstudie geprüft werden, ob das Konzept in der Praxis tatsächlich umsetzbar und wirksam ist. Darauf aufbauend stellt sich die Frage, ob Allianzen die ein gemeinsames CISRM betreiben tatsächlich erfolgreicher sind, als solche die dies nicht tun. Dabei gilt es die einzelnen Organisationen zu betrachten und herauszufinden, wie sich das CISRM im direkten Vergleich zum ISRM auswirkt. Wie der Erfolg von Organisationen und Allianzen im Bezug zu deren Umgang mit Sicherheitsrisiken einer Vergleichsstudie bewertet werden kann, bleibt dabei eine offene Frage.

Grundlage für weitere ISM Prozesse: Bereits in Kapitel 4 wurde beschrieben, dass auch andere Bereiche des ISM für IORs geeignet sind. Während sich diese Arbeit auf das ISRM fokussiert hat, bietet sich die Möglichkeit der Anwendung des Konzeptes auf weitere ISM Prozesse. Die Architektur des CISRM Frameworks kann als Vorlage zur Erstellung weiterer kollaborativer Frameworks genutzt werden. Der Aufbau bestehend aus den vier Komponenten ist nicht spezifisch für das ISRM und kann grundsätzlich auch auf jeden anderen (IS) Prozess angewendet werden. Schmidt und Mizani [165] liefern dazu bereits einen Überblick über alle ISM Prozesse und wie diese von verschiedenen Kooperationsformen profitieren könnten. Im Zuge weiterer Forschungsarbeiten können diese Prozesse untersucht und ebenfalls für die interorganisationale Zusammenarbeit adaptiert werden.

Interorganisationales ISMS: Die Idee weiterer interorganisationaler ISM Prozesse lässt letztlich auch die Vision eines interorganisationalen ISMS zu. Langfristig könnten sich Organisationen dazu entscheiden, nicht nur einzelne Prozesse gemeinsam mit ihren Partnern zu etablieren, sondern ein komplettes ISMS innerhalb der Allianz aufzubauen. Aktuell sind jedoch die gängigen Normen nicht darauf ausgerichtet, dass Prozesse eines ISMS über die Grenzen eines (unabhängigen) Unternehmens hinausgehen. Bereits der in Kapitel 6 vorgestellte Prozess basiert auf einer freiwilligen Zusammenarbeit und Selbstverpflichtung der Partner, welcher somit nicht dem Verständnis eines durch das Top-Management gesteuerten Prozesses folgt. Es ergibt sich die Fragestellung, ob die Vorstellung eines Enterprise ISMS auf ein Allianz ISMS übertragbar wäre und wie sich ein solches Konzept mit gängigen Normen vereinbaren ließe.

Die interorganisationale Kollaboration bietet somit in Zukunft viele Möglichkeiten mit Potenzial zur Weiterentwicklung des ISM. Das CISRM liefert an dieser Stelle einen ersten Ansatz, um der zunehmenden Bedrohungslage für Informationen und Technologie in Partnerschaften gemeinsam zu begegnen. Ein Verschieben von Sicherheitsrisiken in den Verantwortungsbereich von strategischen Allianzen kann dazu beitragen, das Sicherheitsniveau von Organisationen langfristig zu erhöhen.

Anhang A

Modelle der einzelnen Aktivitäten des kollaborativen Prozesses

Dieser Anhang liefert eine grafische Darstellung jeder Aktivität des generischen Prozesses (Abschnitt 6.2). Diese Teilmodelle wurden anschließend zusammengefasst um den kollaborativen Prozesses (Abbildung 6.8) zu erstellen.

Abbildung A.1: Übersicht der im Prozessmodell genutzten BPMN 2.0 Elemente

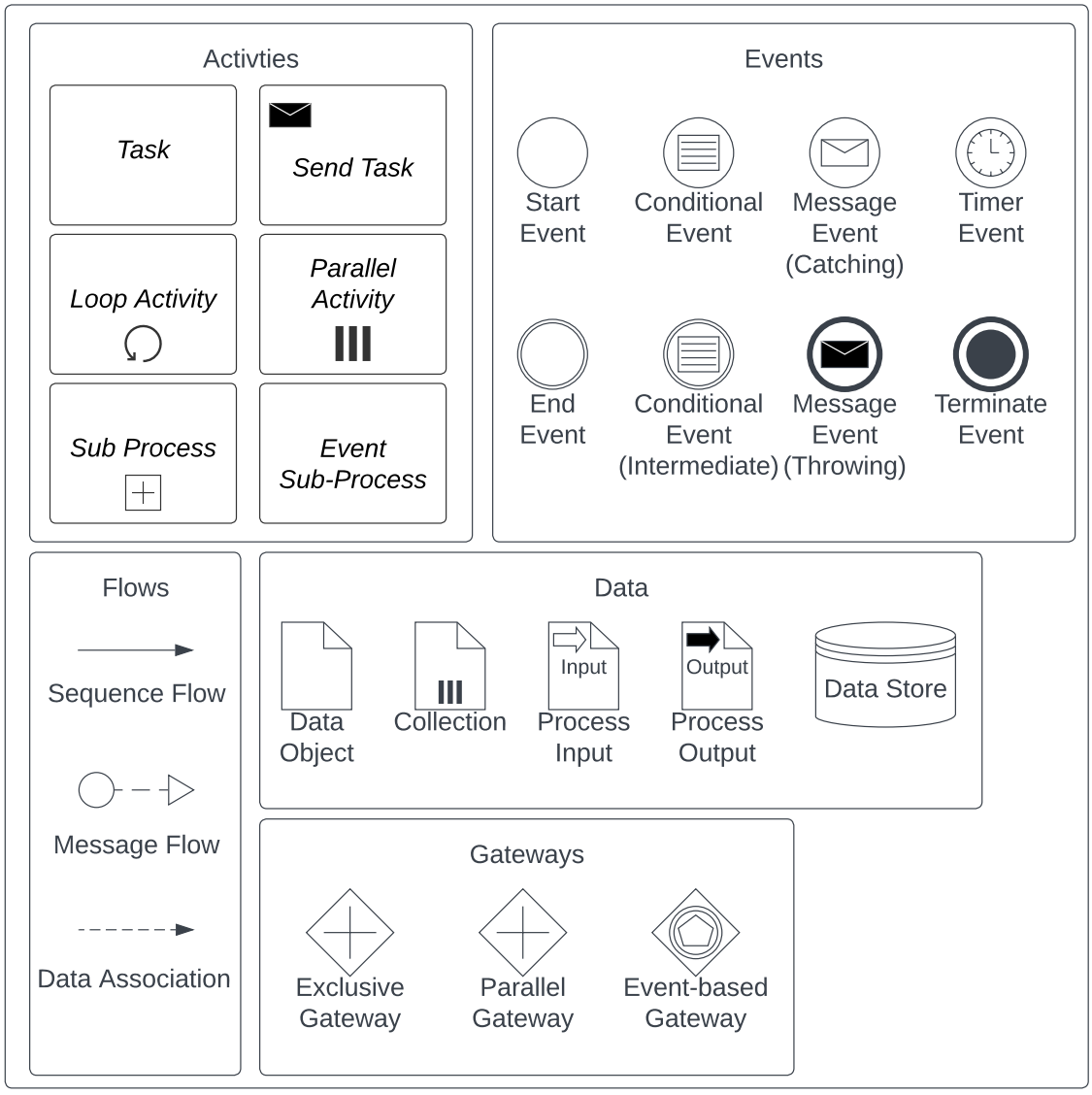


Abbildung A.2: Aktivität 1: Kontext festlegen im CISRM

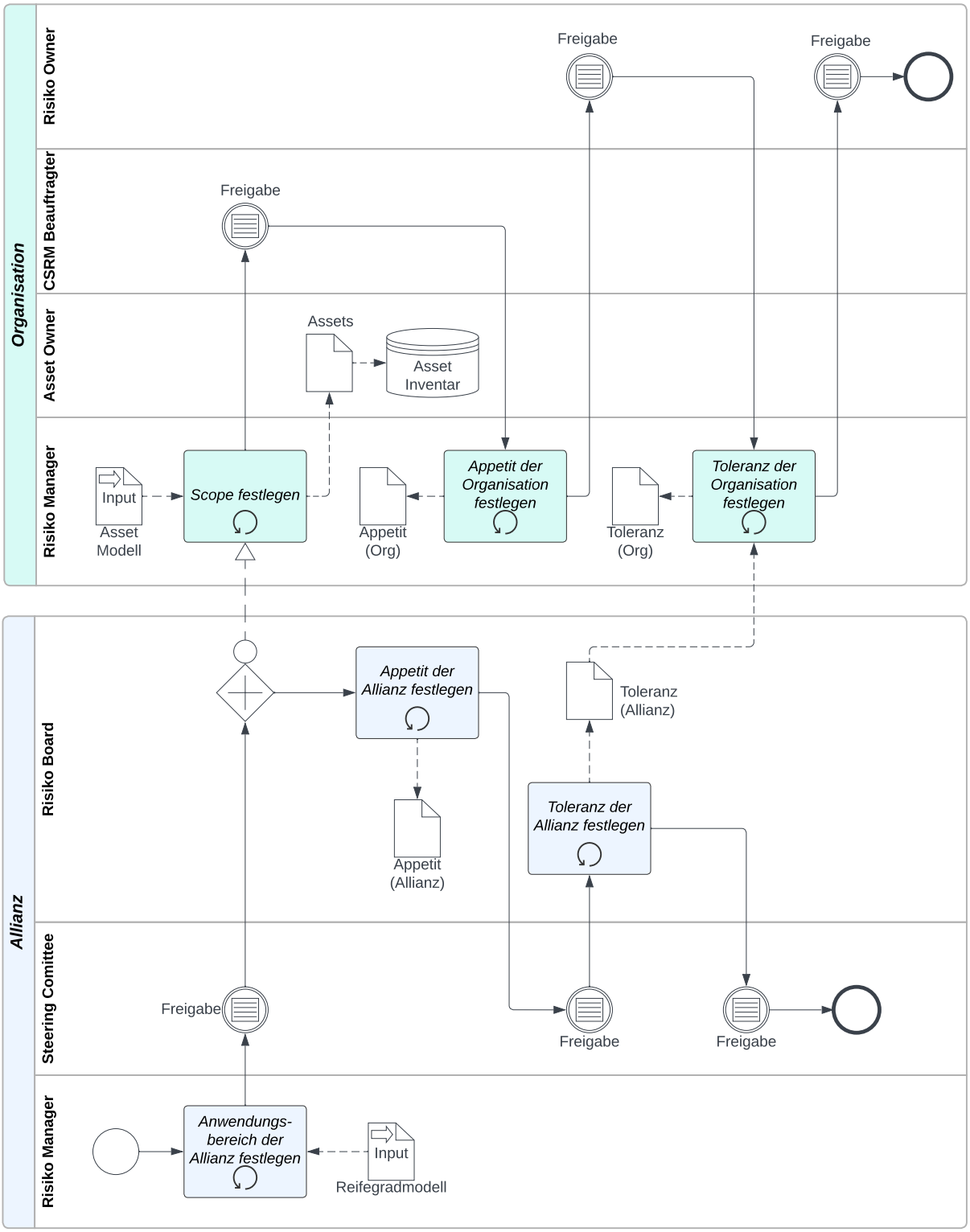


Abbildung A.3: Aktivität 2: Risiken einschätzen im CISRM

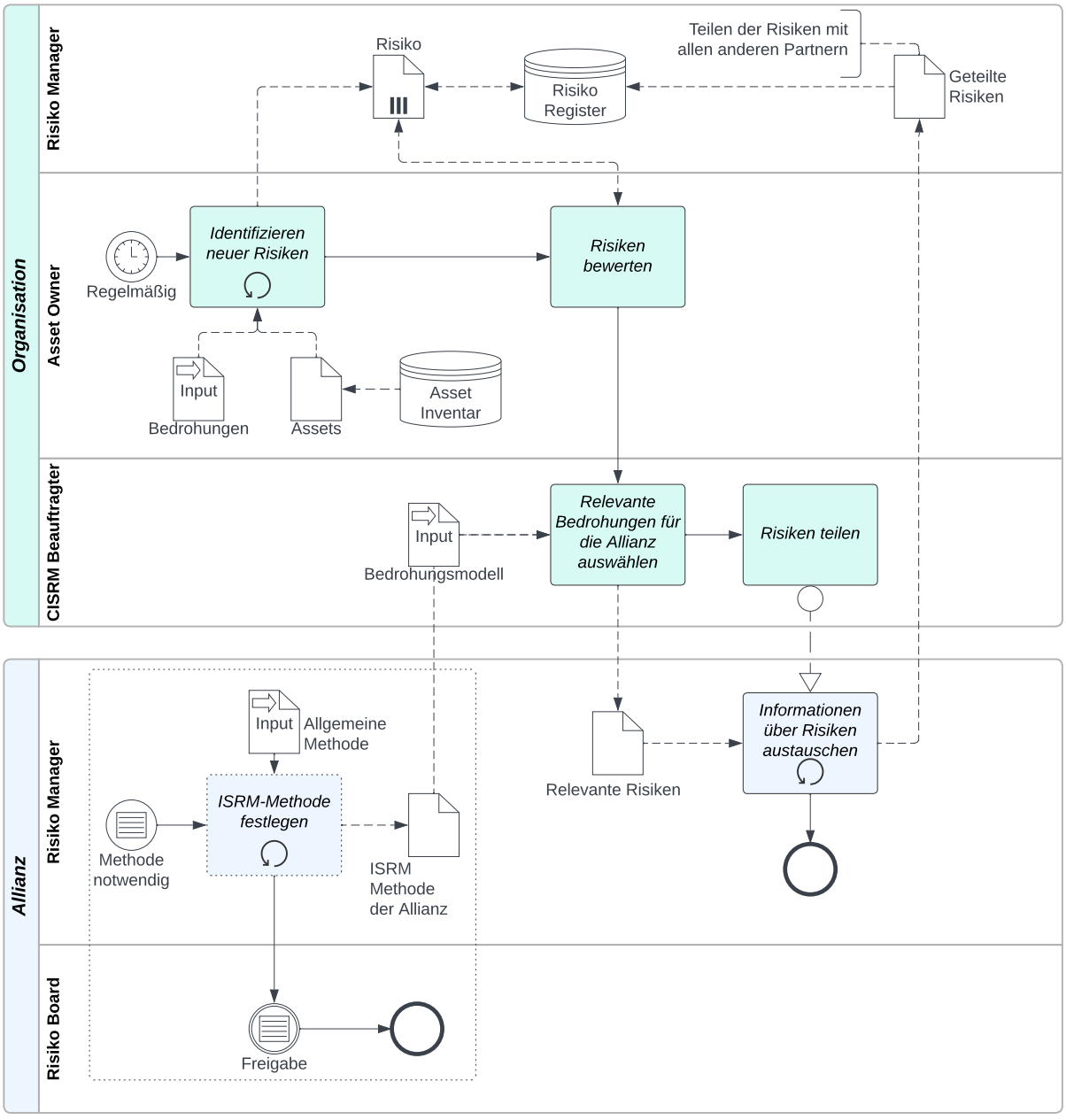


Abbildung A.4: Aktivität 3: Risiken behandeln im CISRM

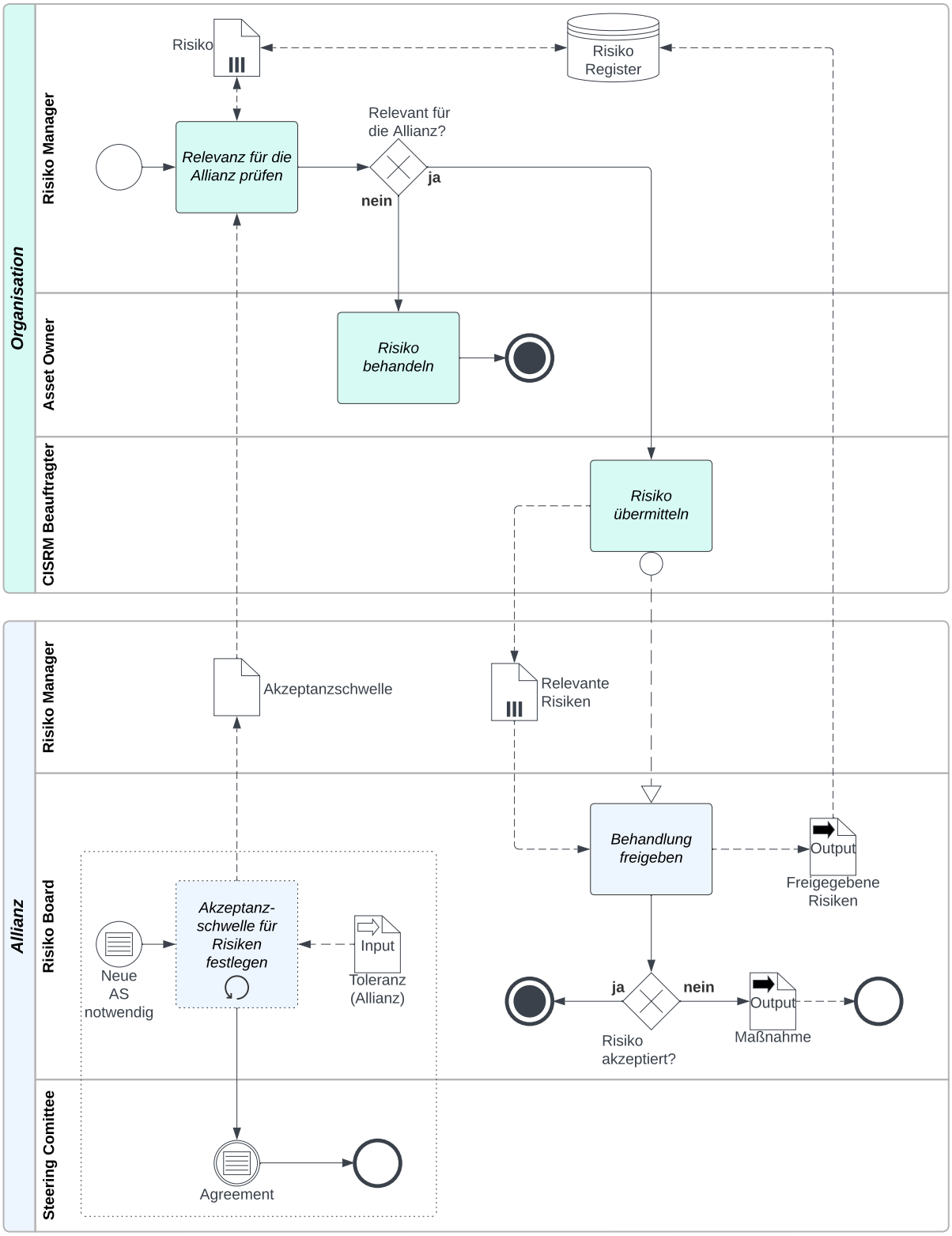


Abbildung A.5: Aktivität 4: Behandlung umsetzen im CISRM

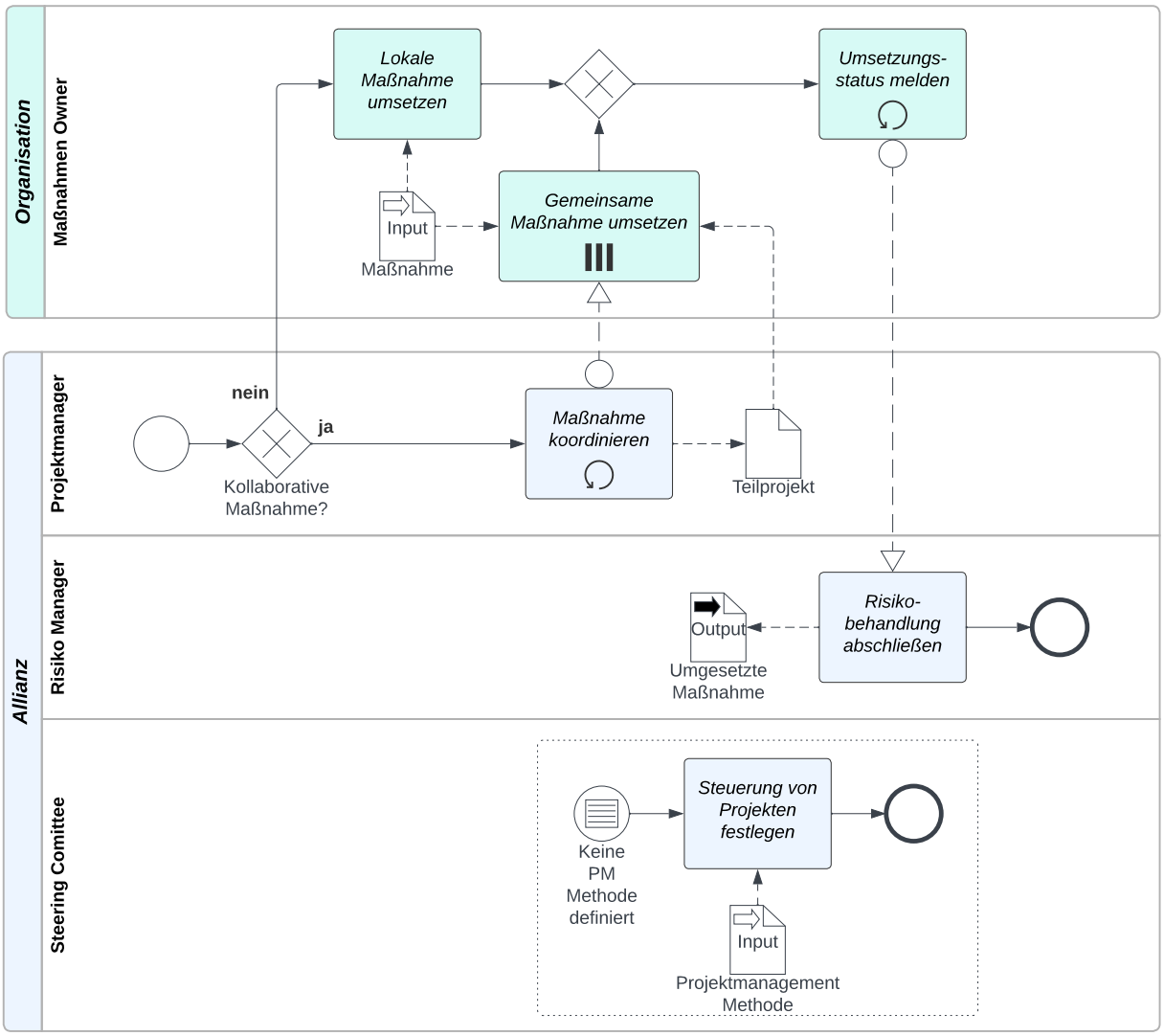


Abbildung A.6: Aktivität 5: Risiken und Maßnahmen überwachen im CISRM

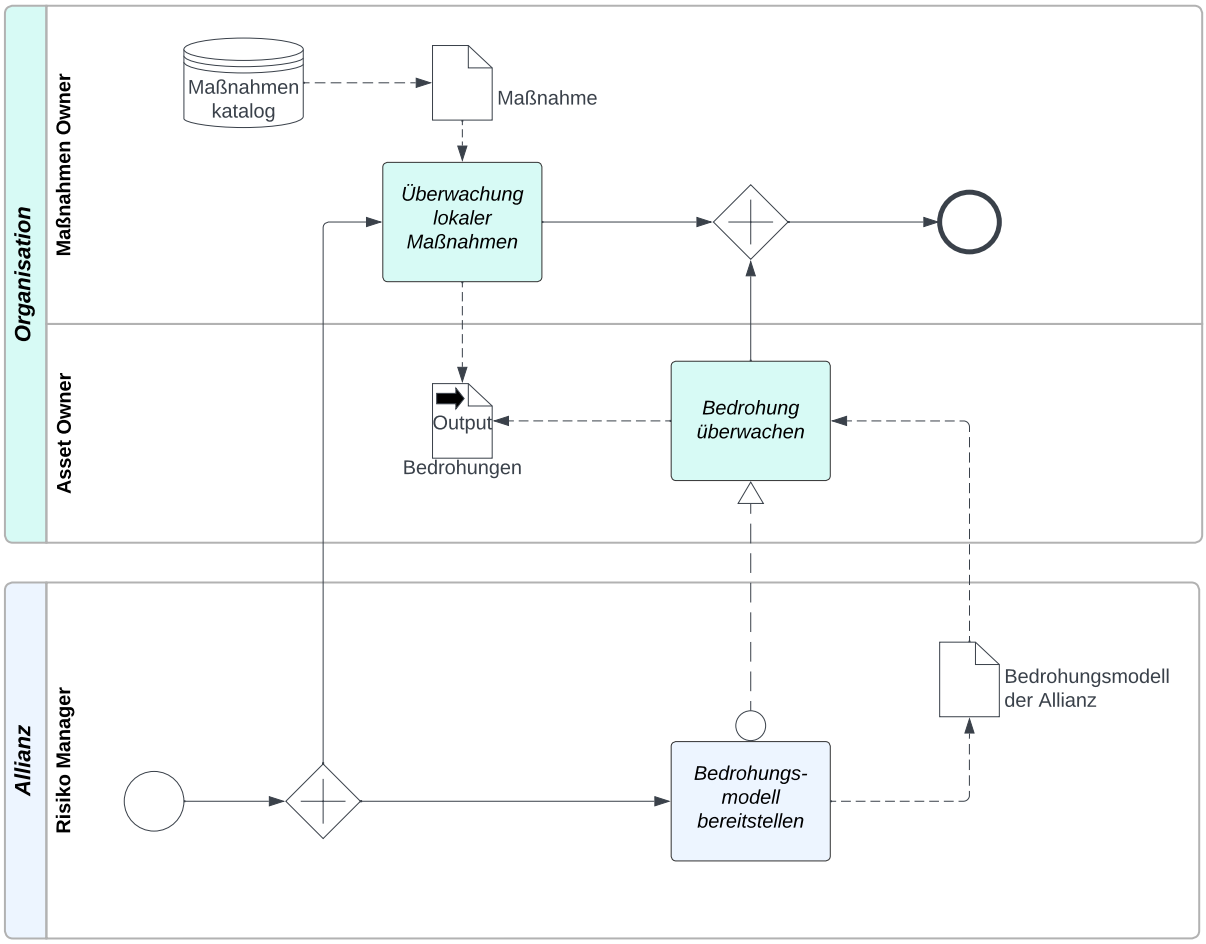
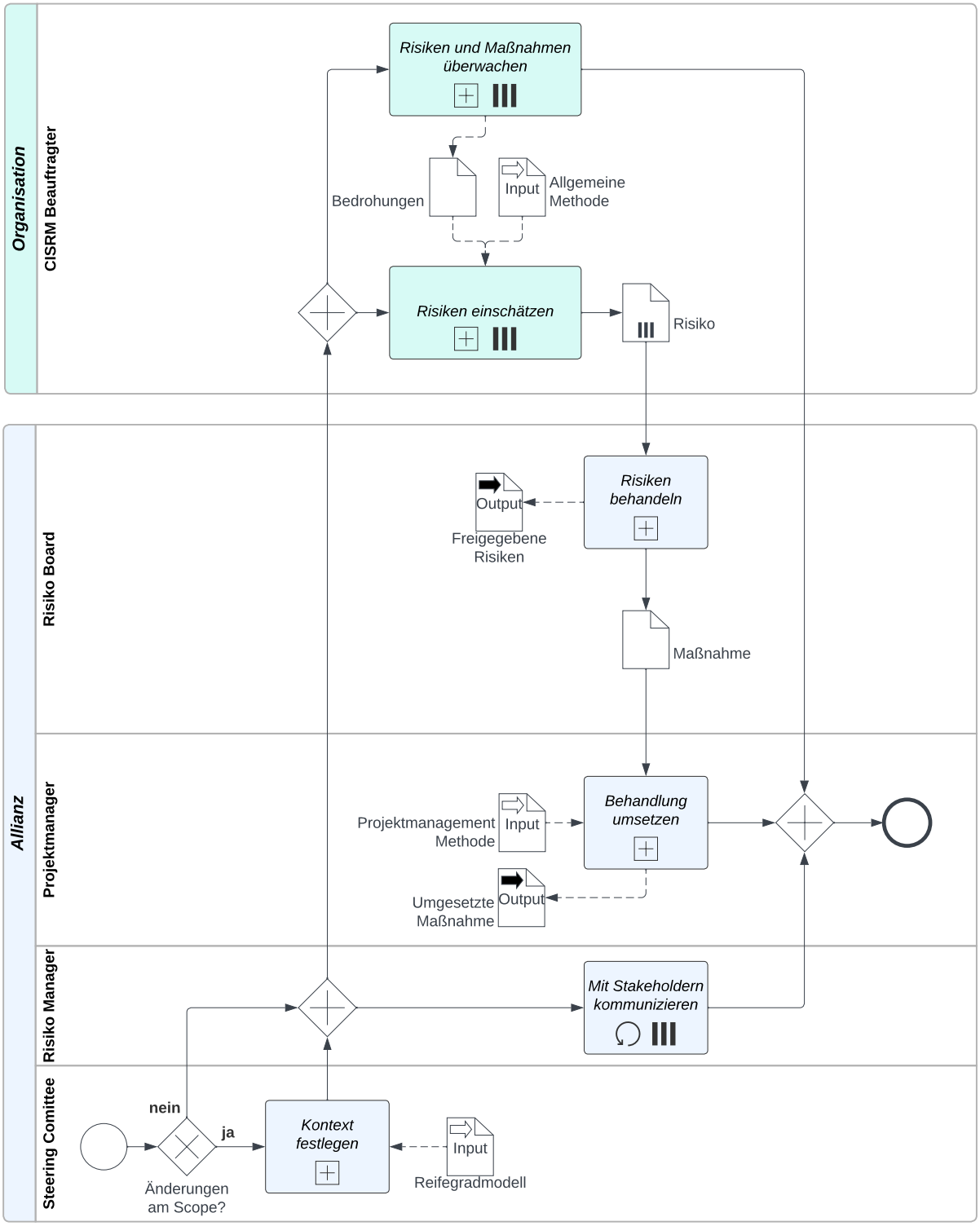


Abbildung A.7: CISRM Aktivitäten mit Sub-Prozessen aus Sicht der Allianz



Anhang B

Ergänzende Darstellungen zu den geteilten Ressourcen

Die in diesem Anhang mitgelieferten Darstellungen sollen lediglich einen vertiefenden Einblick in bestimmte Aspekte der geteilten Ressourcen (Kapitel 7) liefern, welche jedoch nicht für die Arbeit selbst und das Framework notwendig sind.

Tabelle B.1: Auswirkungen von Sicherheitsbedrohungen auf Schutzziele [233]

Auswirkung der Bedrohung	**Schutzziele**
Zerstörung von Informationen und/oder anderen Ressourcen	A
Verfälschung oder Veränderung von Informationen	I
Diebstahl oder Verlust von Informationen und/oder anderen Ressourcen	C, A
Offenlegung von Informationen	C
Unterbrechung von Services	A

Abbildung B.1: Architektur der GÉANT Security Baseline [227]

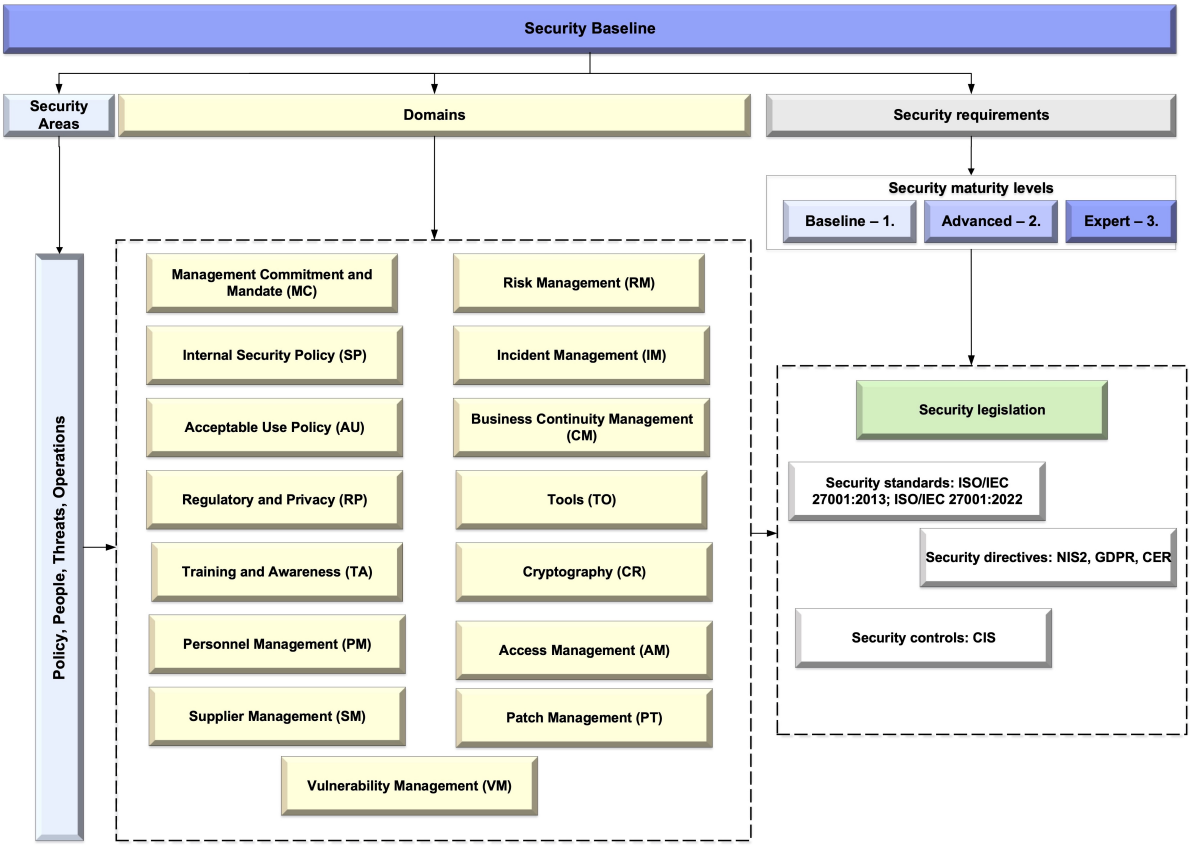


Tabelle B.2: Zuweisung von Variablen zu den Ausprägungen der Dimensionen der Bedrohungsklassifikation [233]

Dimension (D_n)	d_n	**Ausprägung**	**Variable** deutsch	engl.
Quelle	d_1	extern	ex	ex
(D_1)	d_1	intern	in	in
Auslöser	d_2	Mensch	me	hu
(D_2)	d_2	Umwelt	uw	en
	d_2	Technik	te	te
Böswilligkeit	d_3	böswillig	bw	ma
(D_3)	d_3	nicht böswillig	nb	nm
Absicht	d_4	versehentlich	vs	ac
(D_4)	d_4	beabsichtigt	be	it
Auswirkung	d_5	Zerstörung von Informationen [...]	ze	de
(D_5)	d_5	Verfälschung/Veränderung von Informatio-	ve	mo
	d_5	nen	di	th
	d_5	Diebstahl/Verlust von Informationen [...]	of	di
	d_5	Offenlegung von Informationen	un	ir
		Unterbrechung von Services		

Tabelle B.3: Zuordnung von dimensionsspezifischen Variablen zu Wahrscheinlichkeitswerten für die Berechnung einer Eintrittswahrscheinlichkeit der Bedrohung [233]

Dimension D_n	$p(d_n)$	**Wahrscheinlichkeitsvariable** **deutsch**	**englisch**
D_1: Quelle	$p(d_1)$	p_{quelle}	p_{source}
D_2: Auslöser	$p(d_2)$	$p_{ausloeser}$	p_{agent}
D_3: Böswilligkeit	$p(d_3)$	$p_{boeswilligkeit}$	p_{malice}
D_4: Absicht	$p(d_4)$	$p_{absicht}$	$p_{intention}$
D_5: Auswirkung	$p(d_5)$	$p_{auswirkung}$	p_{impact}
Bedrohung insgesamt (d_1, d_2, d_3, d_4, d_5)	$p((d_1, d_2, d_3, d_4, d_5))$	$p_{bedrohung}$	p_{threat}

Tabelle B.4: Anwendungsbeispiel zum Mapping von Bedrohungen [233]

$(d_1, d_2, d_3, d_4, d_5)$		**Nummer der ENISA-Bedrohung** *(Threat number)*
deutsch	englisch	
(ex, me, bw, vs, ze)	(ex, hu, ma, ac, de)	41
(ex, me, bw, vs, ve)	(ex, hu, ma, ac, mo)	35, 144, 154, 169
(ex, me, bw, vs, di)	(ex, hu, ma, ac, th)	35, 37, 154, 169
(ex, me, bw, vs, of)	(ex, hu, ma, ac, di)	154, 169
(ex, me, bw, vs, un)	(ex, hu, ma, ac, ir)	154, 169, 175
(ex, me, bw, be, ze)	(ex, hu, ma, it, de)	5, 14, 15, 46, 50, 87, 123, 136, 175, 176
(ex, me, bw, be, ve)	(ex, hu, ma, it, mo)	2, 89, 94, 96, 98, 107, 123, 131, 136, 144, 152, 153, 154, 169, 175, 176, 181, 183
(ex, me, bw, be, di)	(ex, hu, ma, it, th)	6, 87, 89, 98, 107, 123, 126, 136, 152, 153, 154, 160, 162, 169, 175, 176, 183
(ex, me, bw, be, of)	(ex, hu, ma, it, di)	2, 11, 12, 13, 87, 88, 89, 95, 96, 98, 107, 123, 126, 136, 152, 153, 154, 160, 162, 169, 175, 176, 181, 183
(ex, me, bw, be, un)	(ex, hu, ma, it, ir)	4, 78, 79, 87, 103, 107, 123, 136, 154, 160, 163, 165, 169, 175, 176, 179
(ex, me, nb, vs, ze)	(ex, hu, nm, ac, de)	23, 30, 31, 41, 46, 50, 87, 123, 136, 174
(ex, me, nb, vs, ve)	(ex, hu, nm, ac, mo)	28, 29, 30, 31, 35, 89, 107, 123, 136, 144, 153, 154, 174, 181
(ex, me, nb, vs, di)	(ex, hu, nm, ac, th)	23, 30, 31, 35, 37, 87, 89, 107, 123, 126, 136, 153, 154, 160, 162, 174
(ex, me, nb, vs, of)	(ex, hu, nm, ac, di)	17, 30, 31, 87, 88, 89, 123, 126, 136, 153, 154, 160, 162, 165, 174, 179, 181
(ex, me, nb, vs, un)	(ex, hu, nm, ac, ir)	30, 31, 33, 72, 78, 80, 87, 103, 123, 136, 154, 160, 163, 165, 174, 179
(ex, me, nb, be, ze)	(ex, hu, nm, it, de)	46, 50, 174
(ex, me, nb, be, ve)	(ex, hu, nm, it, mo)	154, 174, 183
(ex, me, nb, be, di)	(ex, hu, nm, it, th)	6, 154, 174
(ex, me, nb, be, of)	(ex, hu, nm, it, di)	11, 107, 154, 174, 183
(ex, me, nb, be, un)	(ex, hu, nm, it, ir)	72, 78, 79, 103, 107, 154, 174, 184
(ex, uw, nb, vs, ze)	(ex, en, nm, ac, de)	45, 46, 47, 48, 49, 50, 51, 52, 55, 57
(ex, uw, nb, vs, ve)	(ex, en, nm, ac, mo)	35
(ex, uw, nb, vs, di)	(ex, en, nm, ac, th)	35
(ex, uw, nb, vs, of)	(ex, en, nm, ac, di)	
(ex, uw, nb, vs, un)	(ex, en, nm, ac, ir)	45, 48, 49, 52, 55, 56, 57
(ex, te, nb, vs, ze)	(ex, te, nm, ac, de)	46, 50, 51, 69, 73, 93
(ex, te, nb, vs, ve)	(ex, te, nm, ac, mo)	35, 59, 73, 93
(ex, te, nb, vs, di)	(ex, te, nm, ac, th)	34, 35, 37, 59, 64, 73, 75
(ex, te, nb, vs, of)	(ex, te, nm, ac, di)	59, 73, 126
(ex, te, nb, vs, un)	(ex, te, nm, ac, ir)	59, 64, 72, 73, 75, 80, 81, 82, 179
(in, me, bw, vs, ze)	(in, hu, ma, ac, de)	41
(in, me, bw, vs, ve)	(in, hu, ma, ac, mo)	35, 144, 154, 169
(in, me, bw, vs, di)	(in, hu, ma, ac, th)	35, 37, 154, 169
(in, me, bw, vs, of)	(in, hu, ma, ac, di)	100, 154, 165, 169
(in, me, bw, vs, un)	(in, hu, ma, ac, ir)	100, 103, 154, 165, 169, 175
(in, me, bw, be, ze)	(in, hu, ma, it, de)	5, 14, 15, 46, 50, 87, 123, 136, 175, 176, 178
(in, me, bw, be, ve)	(in, hu, ma, it, mo)	2, 89, 94, 96, 98, 107, 123, 131, 136, 144, 152, 153, 154, 169, 175, 176, 178, 181, 183
(in, me, bw, be, di)	(in, hu, ma, it, th)	6, 87, 89, 98, 107, 123, 126, 136, 152, 153, 154, 160, 162, 169, 175, 176, 178, 183
(in, me, bw, be, of)	(in, hu, ma, it, di)	2, 11, 12, 13, 87, 88, 89, 95, 96, 98, 100, 107, 123, 126, 136, 152, 153, 154, 160, 162, 169, 175, 176, 178, 181, 183
(in, me, bw, be, un)	(in, hu, ma, it, ir)	4, 78, 79, 87, 100, 107, 123, 136, 154, 160, 163, 165, 169, 175, 176, 179
(in, me, nb, vs, ze)	(in, hu, nm, ac, de)	23, 30, 41, 46, 50, 87, 123, 136, 174, 178
(in, me, nb, vs, ve)	(in, hu, nm, ac, mo)	28, 29, 30, 35, 89, 107, 153, 154, 174, 178, 181
(in, me, nb, vs, di)	(in, hu, nm, ac, th)	23, 30, 35, 37, 87, 89, 107, 126, 153, 154, 160, 162, 174
(in, me, nb, vs, of)	(in, hu, nm, ac, di)	17, 30, 87, 88, 89, 100, 107, 123, 126, 136, 153, 154, 160, 162, 165, 174, 178, 181
(in, me, nb, vs, un)	(in, hu, nm, ac, ir)	30, 33, 78, 80, 87, 100, 103, 107, 123, 136, 154, 160, 163, 174, 179
(in, me, nb, be, ze)	(in, hu, nm, it, de)	46, 174, 178
(in, me, nb, be, ve)	(in, hu, nm, it, mo)	123, 136, 154, 174, 178, 183
(in, me, nb, be, di)	(in, hu, nm, it, th)	6, 123, 136, 154, 174
(in, me, nb, be, of)	(in, hu, nm, it, di)	11, 154, 174, 178, 179, 183
(in, me, nb, be, un)	(in, hu, nm, it, ir)	78, 79, 103, 154, 174
(in, uw, nb, vs, ze)	(in, en, nm, ac, de)	47, 49, 52
(in, uw, nb, vs, ve)	(in, en, nm, ac, mo)	35, 144
(in, uw, nb, vs, di)	(in, en, nm, ac, th)	35
(in, uw, nb, vs, of)	(in, en, nm, ac, di)	
(in, uw, nb, vs, un)	(in, en, nm, ac, ir)	49, 52
(in, te, nb, vs, ze)	(in, te, nm, ac, de)	46, 50, 69, 73, 93
(in, te, nb, vs, ve)	(in, te, nm, ac, mo)	35, 59, 73, 93
(in, te, nb, vs, di)	(in, te, nm, ac, th)	35, 37, 59, 64, 73, 75
(in, te, nb, vs, of)	(in, te, nm, ac, di)	59, 73, 126
(in, te, nb, vs, un)	(in, te, nm, ac, ir)	59, 64, 69, 73, 75, 80, 82, 93, 179

Farbe nach d_{2m} (Auslöser)
- Mensch
- Umwelt
- Technik

Tabelle B.5 zeigt vier in der ENISA Toolbox betrachtete ISRM Methoden (ITSRM2, MONARC, EBIOS, MAGERIT). Dies stellt einen Ausschnitt aus dem (dynamischen) *Risk Comparison Calculator* dar. Dieser erlaubt es, die Einstufung gemäß der einzelnen Methoden direkt auf einen allgemeinen Toolbox-Wert abzubilden. So ergibt sich aus einem *Medium* bei *ITSRM2* ein *Moderate* und ein *High* bei *MONARC* wird zu *Very High*. Dadurch sind die Ergebnisse leicht vergleichbar und können zwischen den einzelnen Methoden ausgetauscht werden.

Tabelle B.5: Mapping mehrerer ISRM Methoden in der ENISA EU RM Toolbox [235]

ITSRM2	MONARC	EBIOS	MAGERIT
Impact Level			
1	4	5	5
Probability/Likelihood Level			
5	4	5	5
Risk Level			
5	16	25	25
Medium	High	Very High	Very High
ENISA ToolBox			
Moderate	Very High	Very High	Very High

Anhang C

Veröffentlichungen im Rahmen des Promotionsvorhabens

Nachfolgend sind alle wissenschaftlichen Publikationen in chronologischer Reihenfolge aufgelistet, welche im Verlauf des Promotionsvorhabens entstanden sind. Dabei wurden Teile dieser Dissertation bereits in einzelnen Veröffentlichungen vorveröffentlicht.

An Identity Provider as a Service platform for the eduGAIN research and education community

Michael Schmidt und Jule Anna Ziegler. „An Identity Provider as a Service platform for the eduGAIN research and education community“. In: *IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. Mai 2019, S. 739–740

Beitrag Schmidt und Ziegler [241] beschreiben in ihrer Veröffentlichung das Konzept für eine Identity Provider as a Service Plattform, welches im Rahmen des GÉANT Projektes (GN4-2 Joint Research Activity 3) entwickelt wurde.
Michael Schmidt war im Projekt an der Entwicklung der vorgestellten Prototypen beteiligt, erstellte die Architekturübersicht und die Beschreibung der Plattform. Jule Ziegler, ebenfalls im gleichen Projekt, unterstützte beim Review und der inhaltlichen Verbesserung des Artikels.

Abstract Im Bereich R&E existieren nationale Identitätsföderationen, welche Bildungs- und Forschungseinrichtungen miteinander verbindet. Diese Föderationen sind wiederum durch die globale eduGAIN Interföderation miteinander verbunden. Technisch wird dies realisiert, indem sogenannte Identity Provider (IdP) und Service Provider (SP) auf Basis der Security Assertion Markup Language (SAML) miteinander kommunizieren. Mit wachsenden Netzwerken, sich entwickelnden Technologien und höheren Sicherheitsstandards, die in R&E eingeführt werden, wird die Aufgabe, IdPs zu erstellen und zu verwalten, immer komplexer. Die üblicherweise verwendeten Softwarelösungen für den Einsatz eines IdP, z.B.

Shibboleth und SimpleSAMLphp, erfordern beide praktische Erfahrung mit SAML und spezifische Kenntnisse der Produkte. Darüber hinaus müssen im Rahmen der globalen Zusammenarbeit immer mehr Konfigurationsoptionen implementiert werden, z.B. Standards und Richtlinien, die in der Gemeinschaft eingeführt werden, oder neue Identitätsattribute. Die Komplexität hat einen Punkt erreicht, an dem es für Organisationen sehr anspruchsvoll ist, die technischen Herausforderungen zu bewältigen, sodass sie nicht in der Lage sind, der R&E Community beizutreten. Um dieses Problem zu lösen, wurde eine IdP as a Service Plattform entwickelt, die vor allem kleine und mittlere Organisationen bei der Erstellung eines IdP und dem Beitritt zu einer nationalen Identitätsföderation unterstützt.

IT Service Management Frameworks Compared - Simplifying Service Portfolio Management

Michael Schmidt, Michael Brenner und Thomas Schaaf. „IT Service Management Frameworks Compared - Simplifying Service Portfolio Management“. In: *IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. 2019, S. 421–427

Beitrag Schmidt et al. [211] präsentieren in dieser Veröffentlichung ein Vorgehen zum inhaltlichen Vergleich von IT Service Management Frameworks erstellen so einen leichtgewichtigen Service Portfolio Management Prozess. Das Projekt basiert auf den Vorarbeiten von Schmidt [242], welche im Rahmen der Masterarbeit entwickelt wurden.
Michael Schmidt war als Hauptautor federführend für die Ausarbeitung des Artikels verantwortlich. Michael Brenner betreute bereits die dem Artikel zugrunde liegenden Masterarbeit, unterstützte das Review und die inhaltliche Verbesserung des Artikels. Thomas Schaaf war ebenfalls Betreuer der Masterarbeit, war allerdings nicht aktiv an der Ausarbeitung des Artikels beteiligt.

Abstract Der Zweck des IT Serviceportfoliomanagements (SPM) besteht darin, das Serviceangebot einer Organisation mit ihrer IT-Strategie in Einklang zu bringen. Es ist ein integraler Bestandteil jedes Service Management Systems (SMS) und in unterschiedlichen Formen von so gut wie jedem IT Service Management (ITSM) Framework gefordert, wurde aber bisher weniger formal erforscht als stärker betriebsorientierte und strukturierte Prozesse wie das Incident Management. ITSM Frameworks enthalten oft recht umfangreiche Anleitungen zu bestimmten Prozessen wie SPM, was eine effiziente Umsetzung insbesondere für kleine und mittlere Unternehmen erschweren kann. Darüber hinaus ist es bei der Auswahl der für die eigene Organisation anzuwendenden Empfehlungen aufgrund der fehlenden Formalisierung alles andere als einfach, die Gemeinsamkeiten und Unterschiede der verschiedenen Rahmenwerke zu erkennen. Die vorliegende Publikation stellt einen modellbasierten Ansatz vor, um ITSM Frameworks zu vergleichen, zwischen den wesentlichen und weniger wesentlichen Elementen ihrer Prozessführung zu unterscheiden und wendet diesen Ansatz exemplarisch auf die Anleitungen zum SPM von ITIL, ISO/IEC 20000, MOF und FitSM an.

Improving Identity and Authentication Assurance in Research & Education Federations

Jule Anna Ziegler, Michael Schmidt und Mikael Linden. „Improving Identity and Authentication Assurance in Research & Education Federations“. In: *International Workshop on Security and Trust Management*. 2019

Beitrag Ziegler et al. [243] präsentieren das REFEDS Assurance Framework, ein Identitäts- und Authentisierungsframework für den Bereich R&E. Dieses wurde im Rahmen des GÉANT Projektes (GN4-2 Joint Research Activity 3) gemeinsam mit der REFEDS Assurance Working Group entwickelt.
Mikael Linden war als Leiter der REFEDS Assurance Working Group hauptverantwortlich für die inhaltliche Ausgestaltung des *REFEDS Assurance Frameworks*, welches in dem Artikel beschrieben wird. Er war selbst nicht aktiv an der Erstellung des Artikels beteiligt. Sowohl Jule Ziegler als auch Michael Schmidt waren ebenfalls Mitglieder der Arbeitsgruppe und haben die Finalisierung des Frameworks unterstützt. Zusätzlich waren sie die Editoren des zugehörigen *REFEDS Single Factor Authentication Profile*. Beide waren gleichermaßen an der Ausarbeitung des Artikels auf Basis der Ergebnisse aus der Assurance Working Group beteiligt.

Abstract In diesem Papier stellen wir einen leichtgewichtigen Rahmen für die Identitäts- und Authentifizierungssicherheit vor, der auf die Bedürfnisse des Sektors R&E zugeschnitten ist. Es wurde eine umfassende Anforderungsanalyse durchgeführt, deren Ergebnisse mit bestehenden Frameworks wie NIST 800-63-3, IGTF und Kantara verglichen wurden. Aufgrund der besonderen Anforderungen in einer föderierten Umgebung, die sich über mehrere Länder erstreckt, scheint keines der bestehenden Rahmenwerke in dieser Umgebung zu skalieren. In diesem Kontext verhindern Bedingungen wie die Unabhängigkeit der Organisationen, die unterschiedlichen Organisationskulturen und technischen Möglichkeiten die Definition strenger Sicherheitsanforderungen, wie sie in den meisten Richtlinien gefordert werden. Das hier vorgestellte REFEDS Assurance Framework (RAF) definiert eine Reihe von Identitäts- und Authentifizierungskriterien, die auch zwei Sicherheitsprofile enthalten, die zwischen risikoarmen und risikoreichen Forschungsanwendungen unterscheiden. Der vorgestellte Ansatz berücksichtigt relevante Kriterien aus bestehenden Rahmenwerken und wurde im Rahmen einer öffentlichen Umfrage und eines technischen Pilotprojekts bewertet. Die Evaluierung hat gezeigt, dass die Konfiguration und das Testen mit der Shibboleth- und SimpleSAMLphp-Software erfolgreich verlaufen ist, aber auch, dass die Mitglieder der R&E-Gemeinschaft positiv darauf reagiert haben.

Managementsysteme ohne spezialisierte Tools etablieren

Michael Schmidt, Stefan Metzger und Miran Mizani. „Managementsysteme ohne spezialisierte Tools etablieren. Ein leichtgewichtiger Ansatz zur Dokumentation im Service- und Informationssicherheitsmanagement“. In: *29. DFN-Konferenz „Sicherheit in vernetzten Systemen"*. Feb. 2022

Michael Schmidt, Stefan Metzger und Miran Mizani. „Aufbau eines Managementsystems - Tools vs. Prozesse“. In: *DFN Mitteilungen* (Juni 2022)

Beitrag Schmidt et al. [244, 245] beschreiben einen leichtgewichtigen Ansatz zum Aufbau eines ISO konformen Managementsystems, welches größtenteils auf eine leichtgewichtige Dokumentation auf Basis eines Wiki-Systems setzt. Das Vorgehen wurde während der Arbeit am Leibniz Rechenzentrum entwickelt, wo das System so für das integrierte Managementsystem eingesetzt wird.
Michael Schmidt war für die Ausarbeitung des Artikels verantwortlich, insbesondere für die Aspekte zum Service Management am LRZ. Stefan Metzger hat mit den Informationen aus der Norm unterstützt und deren Dokumentationsvorgaben beschrieben. Miran Mizani lieferte die Expertise zu Dokumentenlenkung, Kennzahlensystemen und der Aufgabenplanung.
Die Autoren haben gemeinsam eine überarbeitete Version des Beitrags für die DFN-Mitteilungen erstellt.

Abstract Zur verbesserten Planung, Steuerung und Überwachung strategischer Initiativen und operativer Abläufe haben sich Managementsysteme, wie sie etwa von der International Organization for Standardization definiert werden, in vielen Organisationen etabliert. Ein wichtiger Aspekt eines solchen Systems ist der Umgang mit Dokumentation, nicht nur im Sinne des Dokumentenmanagements (DCM), sondern auch im Kontext des Betriebs. Viele Organisationen bieten hierzu Spezialsoftware an, die einen oder auch mehrere Teilbereiche eines Managementsystems unterstützen, etwa das Risikomanagement. Solche Softwareprodukte erleichtern zwar die Implementierung und sind mit einigen Komfortfunktionen ausgestattet, sind jedoch oftmals kostenintensiv und bringen zusätzliche Komplexität mit sich. Gerade die hohen Kosten können besonders für kleine und mittlere (nicht gewinnorientierte) Organisationen ein Problem darstellen. In diesem Bericht wird ein Konzept zum Aufbau eines leichtgewichtigen Ansatzes zur Dokumentation vorgestellt, welches in einem wissenschaftlichen Rechenzentrum auf Basis einer verbreiteten Wiki-Lösung implementiert wurde. Der hier beschriebene Ansatz soll Organisationen helfen, die für ein Managementsystem notwendigen Abläufe trotz begrenzter Ressourcen und ohne den Einsatz von Spezialsoftware zu etablieren.

Information security risk management terminology and key concepts

Michael Schmidt. „Information security risk management terminology and key concepts“. In: *Risk Management* 25.1 (16. Dez. 2023), S. 1–23. DOI: 10.1057/s41283-022-00108-8

Beitrag Schmidt [193] präsentiert eine generische ISRM Terminologie bestehend aus Schlüsselkonzepten und Kernbegriffen, welche aus den meistgenutzten Industriestandards und Frameworks extrahiert wurden. Der Artikel stellt eine Vorabveröffentlichung der Inhalte und Ergebnisse aus Kapitel 5 dieser Arbeit dar. Dabei wurden diese in einer komprimierten Version zusammengefasst und insbesondere die erstelle Terminologie vorgestellt. Als Einzelveröffentlichung fehlt jedoch der größere Kontext als Teil des übergreifenden CISRM, welcher erst als Teil dieser Dissertation deutlich wird.
Michael Schmidt war hauptverantwortlich für die Ausarbeitung des Artikels und seiner Inhalte.

Abstract Sprache ist die Grundlage jeder Kommunikation, wobei das verwendete Vokabular einen entscheidenden Einfluss auf die Fähigkeit der Kommunikationspartner hat, sich gegenseitig klar zu verstehen. Im Bereich des ISRM wird die verwendete Terminologie häufig von Industriestandards und Rahmenwerken vorgegeben. Es gibt jedoch keine allgemein akzeptierte Terminologie, was die Zusammenarbeit für Experten und Forscher gleichermaßen erschwert. Diese Publikation vergleicht die Terminologien, die von häufig verwendeten Rahmenwerken wie ISO und NIST im Bereich des ISRM definiert werden. Es werden die Begriffe und inhärenten Konzepte der jeweiligen Terminologie untersucht, der Risikobegriff verglichen und ein Konzeptdiagramm auf der Grundlage der wichtigsten Schlüsselkonzepte erstellt. Das Ergebnis ermöglicht ein gemeinsames Verständnis des ISRM über Frameworks und organisatorische Grenzen hinweg und ermöglicht so weitere Forschung, Diskussion sowie inner- und interorganisationale Kommunikation.

Transition zur neuen ISO/IEC 27001 - Erfahrungen zum neuen Anhang A

Miran Mizani, Michael Schmidt, Daniel Weber, Stefan Metzger und Helmut Reiser. „Transition zur neuen ISO/IEC 27001. Erfahrungen zum neuen Anhang A“. In: *30. DFN-Konferenz „Sicherheit in vernetzten Systemen"*. Feb. 2023

Beitrag Mizani et al. [246] untersuchen die geänderten Anforderungen an ein ISMS, die sich aus der Neuauflage der Standards ISO/IEC 27001 und 27002 ergeben. Die Praxisbeispiele und Vorschläge zu den Maßnahmen ergeben sich dabei aus den bisherigen Erfahrungen zum Betrieb eines ISMS am Leibniz Rechenzentrum.
Miran Mizani beschrieb die neue Norm und deren strukturelle Änderungen. Er lieferte außerdem die Erfahrungen zur physischen Zutrittsüberwachung und der Überwachung von

Aktivitäten. Michael Schmidt analysierte die Überarbeitung des *Anhang A* und die neuen sowie geänderten Controls. Er lieferte die Erfahrungen zur Informationssicherheit für die Nutzung von Clouddiensten. Daniel Weber war verantwortlich für den Abschnitt Threat Intelligence und lieferte Erfahrungen vom HITS-IS. Stefan Metzger und Helmut Reiser unterstützten mit ihrer allgemeinen Expertise zum ISM, übernahmen das Review und die inhaltliche Verbesserung des Artikels.

Abstract Aufgrund der stetig zunehmenden (Cyber-)Bedrohungen für Hochschulen, deren Infrastruktur und schützenswerten Informationen wird das Management der Informationssicherheit auch im Bereich Forschung und Lehre zunehmend bedeutsamer. Die internationalen Standards der Reihe ISO/IEC 27000 haben sich in der Wirtschaft bereits weitläufig etabliert und auch bei Hochschulen und Hochschulrechenzentren stoßen sie auf große Beliebtheit. Aus diesem Grund ist die 2022 veröffentlichte Neuauflage des Standards auch im Hochschulbereich von großer Bedeutung. Dieser Artikel untersucht die Neuerungen des Standards und gibt einen Überblick über die notwendigen Änderungen. Weiterhin werden der Transitionsprozess und ausgewählte Controls und deren Umsetzung am Beispiel eines Hochschulrechenzentrums erläutert. Es zeigt sich, dass die Transition auf die neue Version relativ einfach möglich ist und die vereinfachte Strukturierung der neuen Version vor allem Neueinsteigern einen schnelleren Zugang ermöglicht.

Leveraging Taxonomical Engineering for Security Baseline Compliance in International Regulatory Frameworks

Šarūnas Grigaliūnas, Michael Schmidt, Rasa Brūzgienė, Panayiota Smyrli und Vladislav Bidikov. „Leveraging Taxonomical Engineering for Security Baseline Compliance in International Regulatory Frameworks“. In: *Future Internet* 15.10 (2023). DOI: 10.3390/fi15100330

Beitrag Grigaliūnas et al. [227] beschreiben in ihrem Artikel wie die *Security Baseline for NRENs* zur Verbesserung des Sicherheitsniveaus von R&E Organisationen genutzt werden kann. Weiterhin identifizieren Schnittstellen zu anderen Standards und vergleichen deren Anforderungen untereinander. Die Security Baseline wurde im Rahmen des GÉANT Projektes (GN4-3 Work Package 8 Task 2) entwickelt und später weiterentwickelt (GN5-1 Work Package 8 Task 1).
Šarunas Grigaliunas und Rasa Bruzgiene waren gemeinsam für die Ableitung der Taxonomie und die automatisierte Auswertung des Mappings verantwortlich. Michael Schmidt war Editor der Security Baseline und erstellte das initiale Mapping zu anderen Standards. Er liefert die zugehörige Expertise zu den Sicherheitsanforderungen und war für die fachlichen Hintergründe der Baseline im Artikel zuständig. Panayiota Smyrli war für die Literaturrecherche verantwortlich. Vladislav Bidikov war für das Review und die inhaltliche Verbesserung des Artikels verantwortlich.

Abstract Die Zunahme (erfolgreicher) Angriffe auf die IS von Forschungs- und Bildungseinrichtungen hat gezeigt, dass diese einen zusätzlichen Schutz vor solchen Angriffen benötigen. Um dieses Problem anzugehen, hat eine Allianz von europäischen NRENs ein gemeinsames IS Framework geschaffen. In diesem Artikel wird die *Security Baseline for NRENs* vorgestellt, ein Sicherheitsreifegradmodell für R&E Organisationen. Es wurde auf Basis von allgemeinen best practices im ISM abgeleitet und auf die Bedürfnisse von NRENs, Universitäten und anderen Forschungseinrichtungen zugeschnitten. Auf der Grundlage der Taxonomie wird ein Mapping zwischen den Anforderungen der Baseline und anderen Frameworks und Regularien erstellt. Dies zeigt eine Korrelation zwischen den meisten Regelungen, die R&E Organisationen betreffen und eine Überschneidung zwischen high-level Anforderungen, die bei der Implementierung mehrerer Standards genutzt werden können. Das Ergebnis ermöglicht es Organisationen, einen systematischen Vergleich zwischen verschiedenen Sicherheitsstandards und deren Anforderungen durchzuführen, fehlende Aspekte in ihrer Strategie zu identifizieren und einen Plan zur Verbesserung ihres Sicherheitsprogramms zu definieren.

Opportunities of Interorganizational Collaboration in Information Security Management

Michael Schmidt und Miran Mizani. „Opportunities of Interorganizational Collaboration in Information Security Management“. In: *International Journal of Information Security* (2024). Eingereicht

Beitrag Schmidt und Mizani [165] analysieren die Anwendbarkeit von ISM Prozessen im interorganisationalem Kontext. Die Veröffentlichung ist zu großen Teilen auf Grundlage der Ergebnisse in dieser Dissertation entstanden. Insbesondere werden dabei die Ergebnisse aus Kapitel 4 aufgegriffen und zusammengefasst. Während der Fokus in der vorliegenden Arbeit auf Beziehungen zur Etablierung eines ISRM liegt, werden im Artikel auch andere Prozesse betrachtet. Dabei wird das hier vorgestellte Partnerschaftsmodell genutzt, um die IOR Tauglichkeit weiterer ISM Prozesse zu prüfen.
Michael Schmidt entwickelte die Idee des Artikels aufgrund seiner vorangegangen Forschung im Bereich der IORs in dieser Dissertation. Er lieferte die theoretischen Grundlagen von Beziehungen bis hin zum vorgestellten Partnerschaftsmodell. Miran Mizani forschte im Bereich IS und untersuchte dabei die existierende Literatur zu ISM Prozessen. Er analysierte die Prozessliste der ISO/IEC 27022 und ihre Aktivitäten auf die Anwendbarkeit in den beschriebenen Formen der Zusammenarbeit. Beide Autoren haben gemeinsam das Mapping der ISM Prozesse auf das Partnerschaftsmodell erarbeitet und so die für die interorganisationale Zusammenarbeit geeigneten Prozesse identifiziert.

Abstract In der heutigen globalisierten und vernetzten Welt ist die Bildung von Partnerschaften für die meisten Organisationen unerlässlich für den Erfolg. Die Partner in einer solchen IOR können sich gegenseitig bei der Herstellung ihrer Produkte unterstützen, gemeinsame Dienstleistungen anbieten, Ressourcen austauschen oder gemeinsam an Innovationsprojekten arbeiten. Neben gemeinsamen Geschäftszielen bieten diese IORs auch die Möglichkeit, ein gemeinsames Sicherheitsmanagement zu betreiben, ein Aspekt, der bisher wenig Beachtung fand. Funktionen des ISM wie Vorfall-, Schwachstellen- oder Risikomanagement sind nur einige Beispiele, die von einer Zusammenarbeit profitieren könnten. In dieser Publikation wird untersucht, welche der allgemein bekannten ISM-Funktionen, die auf Standards wie ISO und NIST basieren, für einen interorganisatorischen Ansatz infrage kommen. Es wird ein Partnerschaftsmodell vorgestellt, das drei Arten von IORs definiert: die Lieferantenbeziehung, die Kooperative Beziehung oder die Kollaborative Beziehung. Darauf aufbauend werden die IOR Anforderungen für jede ISM-Funktion analysiert, da jeder Typ unterschiedlich geeignet ist, ein gemeinsames ISM zu etablieren. Als Ergebnis wird eine Übersicht über alle bekannten ISM-Funktionen präsentiert, die zeigt, ob sie von einer gemeinsamen Ausführung profitieren und welcher Beziehungstyp dafür erforderlich ist.

Abkürzungen

ALE Annual Loss Exposure

ARO Annual Rate of Occurrence

BIA Business Impact Analysis

BPMN Business Process Model and Notation

BSI Bundesamt für Sicherheit in der Informationstechnik

CRM Collaborative Risk Management

CIA Confidentiality, Integrity, Availability

CISRM Collaborative Information Security Risk Management

CISO Chief Information Technology Officer

CSF Critical Success Factor

CVSS Common Vulnerability Scoring System

DC Definition Count

DFN Deutsches Forschungsnetz

ENISA European Union Agency for Cybersecurity

ERM Enterprise Risk Management

FAIR Factor Analysis of Information Risk

FoC Forms of Cooperation

KMU Kleine und mittlere Unternehmen

KRI Key Risk Indicator

IOR Interorganisational Relationship

IS Information Security

ITIL Information Technology Infrastructure Library

ISM Information Security Management

ISMS Information Security Management System

ISO International Organization for Standardization

ISRA Information Security Risk Assessment

ISRM Information Security Risk Management

LoR Level of Risk

LRAM Livermore Risk Analysis Methodology

MoR Management of Risk

NREN National Research and Education Network

R&E Research & Education

RA Risiko der Allianz

RO Risiko der Organisation

RM Risk Management

RMF Risk Management Framework

ROI Return On Investment

ROSI Return On Security Investment

SLE Single Loss Exposure

SR Supplier Risk

SCR Supply Chain Risk

SCRM Supply Chain Risk Management

SLA Service Level Agreement

UML Unified Modeling Language

Definitionen

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] Griselda Sinanaj und Jan Muntermann. „Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis“. In: *Bled eConference Proceedings*. Bd. 29. 2013.

[2] Griselda Sinanaj, Jan Muntermann und Timo Cziesla. „How Data Breaches Ruin Firm Reputation on Social Media! - Insights from a Sentiment-based Event Study“. In: *Proceedings der 12. internationalen Tagung Wirtschaftsinformatik (WI 2015)*. 2015, S. 902–916.

[3] David Stout. „AOL Engineer Sold 92 Million Names to Spammer, U.S. Says“. In: *The New York Times* (23. Juni 2004). URL: https://www.nytimes.com/2004/06/23/technology/aol-engineer-sold-92-million-names-to-spammer-us-says.html?smid=url-share.

[4] Nicole Perlroth, Amie Tsang und Adam Satariano. „Marriott Hacking Exposes Data of Up to 500 Million Guests“. In: *The New York Times* (30. Nov. 2018). URL: https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html?smid=url-share.

[5] AJ Dellinger. „Personal Data Of 533 Million Facebook Users Leaks Online“. In: *Forbes* (3. Apr. 2021). URL: https://www.forbes.com/sites/ajdellinger/2021/04/03/personal-date-of-533-million-facebook-users-leaks-online/.

[6] David McCandless und Tom Evans. *World's Biggest Data Breaches & Hacks*. URL: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (besucht am 13. 11. 2021).

[7] Deutscher Bundestag. *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*. 17. Juli 2015. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf.

[8] Deutscher Bundestag. *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*. 18. Mai 2021. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf.

[9] Europäische Kommission. *Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG*. 27. Apr. 2016. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679.

[10] Europäische Kommission. *Directive on Security of Network and Information Systems (NIS directive)*. 6. Juli 2016. URL: http://data.europa.eu/eli/dir/2016/1148/oj.

[11] Europäische Kommission. *Directive on measures for a high common level of cybersecurity across the Union*. 14. Dez. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555.

[12] ISO/IEC JTC 1/SC 27. *ISO/IEC 27001:2013. Information security management systems - Requirements*. Version 2. International Organization for Standardization, Okt. 2013. URL: https://www.iso.org/standard/27001.

[13] Bundesamt für Sicherheit in der Informationstechnik. *BSI-Standard 200-1. Information Security Management Systems (ISMS)*. 15. Nov. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html.

[14] Bundesamt für Sicherheit in der Informationstechnik. *Die Lage der IT-Sicherheit in Deutschland*. URL: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html (besucht am 08. 01. 2024).

[15] Ponemon Institute. *Cost of a Data Breach Report*. IBM Security, 2020. URL: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

[16] Vassiliki Gogou und Marnix Dekker. *Telecom Services Security Incidents 2019*. European Network and Information Security Agency, 23. Juli 2020. DOI: 10.2824/491113.

[17] Vassiliki Gogou und Marnix Dekker. *Trust Services Security Incidents 2019*. European Network and Information Security Agency, 10. Juli 2020. DOI: 10.2824/047833.

[18] Larry Clinton und Stacey Barrack. *Management von Cyber-Risiken. Handbuch für Unternehmensvorstände und Aufsichtsräte*. Internet Security Alliance, 4. Okt. 2018.

[19] Evan E. Anderson und Joobin Choobineh. „Enterprise information security strategies“. In: *Computers & Security* 27.1 (2008), S. 22–29. ISSN: 0167-4048. DOI: 10.1016/j.cose.2008.03.002.

[20] Ebru Yildirim. „The Importance of Information Security Awareness for the Success of Business Enterprises“. In: *Advances in Human Factors in Cybersecurity*. Springer International Publishing, Jan. 2016, S. 211–222. ISBN: 978-3-319-41931-2. DOI: 10.1007/978-3-319-41932-9_17.

[21] David Brooks. „Security risk management: A psychometric map of expert knowledge structure“. In: *Risk Management* 13 (Feb. 2011), S. 17–41. DOI: 10.2307/41289355.

[22] Enrico Baraldi, Espen Gressetvold und Debbie Harrison. „Resource interaction in inter-organizational networks: Foundations, comparison, and a research agenda“. In: *Journal of Business Research* 65.2 (2012). Resource Interaction in Inter-Organizational Networks, S. 266–276. ISSN: 0148-2963. DOI: 10.1016/j.jbusres.2011.05.030.

[23] Håkan Håkansson und Alexandra Waluszewski. *Managing Technological Development*. Taylor & Francis, 22. Sep. 2003. ISBN: 978-0-203-21753-5. DOI: 10.4324/9780203217535.

[24] Fredrik Karlsson, Ella Kolkowska und Frans Prenkert. „Inter-organisational information security: A systematic literature review“. In: *Information and Computer Security* 24 (Nov. 2016), S. 418–451. DOI: 10.1108/ICS-11-2016-091.

[25] G. Lo Nigro et al. „How risk considerations can affect inter-organization relationship decisions“. In: *ICPR-19: 19th International Conference on Production Research*. International Foundation for Production Research, 2007. ISBN: 978-956-310-751-7.

[26] Norbert Jastroch et al. „Inter-Organizational Collaboration: Product, Knowledge and Risk“. In: *Journal of Systemics, Cybernetics and Informatics*. Bd. 9. 5. Okt. 2011, S. 30–35.

[27] Leslie Willcocks und Chong Ju Choi. „Co-operative Partnership and 'Total' IT Outsourcing: From Contractual Obligation to Strategic Alliance“. In: *European Management Journal* 13 (1995), S. 76–78. ISSN: 0263-2373.

[28] Emanuel Gomes, Bradley R. Barnes und Tehmina Mahmood. „A 22 year review of strategic alliance research in the leading management journals“. In: *International Business Review* 25.1, Part A (2016), S. 15–27. DOI: 10.1016/j.ibusrev.2014.03.005.

[29] Derek Friday et al. „Collaborative risk management: A systematic literature review“. In: *International Journal of Physical Distribution & Logistics Management* 48 (Jan. 2018). DOI: 10.1108/IJPDLM-01-2017-0035.

[30] Gang Li et al. „Joint supply chain risk management: An agency and collaboration perspective“. In: *International Journal of Production Economics* 164 (2015), S. 83–94. DOI: 10.1016/j.ijpe.2015.02.021.

[31] Uta Jüttner, Helen Peck und Martin Christopher. „Supply Chain Risk Management: Outlining an Agenda for Future Research“. In: *International Journal of Logistics : Research & Applications* 6 (Dez. 2003), S. 197–210. DOI: 10.1080/13675560310001627016.

[32] Dr Abhijeet Ghadge, Samir Dani und Roy Kalawsky. „Supply Chain Risk Management: Present and Future Scope“. In: *The International Journal of Logistics Management* 23 (Okt. 2012), S. 313–339. DOI: 10.1108/09574091211289200.

[33] Ozlem Bak. „Supply chain risk management research agenda: From a literature review to a call for future research directions“. In: *Business Process Management Journal* 24 (Feb. 2018). DOI: 10.1108/BPMJ-02-2017-0021.

[34] Subhashish Samaddar und Savitha S. Kadiyala. „An analysis of interorganizational resource sharing decisions in collaborative knowledge creation“. In: *European Journal of Operational Research* 170.1 (2006), S. 192–210. DOI: 10.1016/j.ejor.2004.06.024.

[35] ISO/TC 262. *ISO 31000. Risk Management - Guidelines*. International Organization for Standardization, Feb. 2018. URL: https://www.iso.org/standard/65694.html.

[36] William Ho et al. „Supply Chain Risk Management: A Literature Review“. In: *International Journal of Production Research* 53 (Apr. 2015). DOI: 10.1080/00207543.2015.1030467.

[37] Costas Lambrinoudakis et al. *Compendium of Risk Management Frameworks with Potential Interoperability. Supplement to the Interoperable EU Risk Management Framework Report*. European Network and Information Security Agency, Jan. 2022. DOI: 10.2824/75906.

[38] Costas Lambrinoudakis et al. *Interoperable EU Risk Management Framework. Methodology for and assessment of interoperability among risk management frameworks and methodologies*. European Network and Information Security Agency, 13. Jan. 2022. DOI: 10.2824/07253.

[39] Neil Robinson und Emma Disley. *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. Techn. Ber. European Network and Information Security Agency, Sep. 2010. DOI: 10.2824/549292.

[40] Felix Antonio Barrio Juárez et al. *Information Sharing and Analysis Center (ISACs). Cooperative models*. Techn. Ber. European Network and Information Security Agency, Feb. 2018. DOI: 10.2824/549292.

[41] Florian Skopik, Giuseppe Settanni und Roman Fiedler. „A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing“. In: *Computers & Security* 60 (2016), S. 154–176. ISSN: 0167-4048. DOI: 10.1016/j.cose.2016.04.003.

[42] ISO/IEC JTC 1/S27. *ISO/IEC 27010:2015. Security techniques - Information security management for inter-sector and inter-organizational communications*. Version 2. International Organization for Standardization, Nov. 2015. URL: https://www.iso.org/standard/68427.html.

[43] Panagiotis Trimintzios und Razvan Gavrila. *National-level Risk Assessments. An Analysis Report*. European Network and Information Security Agency, 19. Nov. 2013. DOI: 10.2824/2633.

[44] Chris Johnson et al. *Guide to Cyber Threat Information Sharing*. NIST SP 800-150. National Institute of Standards and Technology, Okt. 2016. DOI: 10.6028/NIST.SP.800-150.

[45] Giuseppe Settanni et al. „A collaborative cyber incident management system for European interconnected critical infrastructures“. In: *Journal of Information Security and Applications* 34 (2017), S. 166–182. ISSN: 2214-2126. DOI: 10.1016/j.jisa.2016.05.005.

[46] ISO/TC 262. *ISO/IEC 31073. Risk management — Vocabulary*. Version 1. International Organization for Standardization, Feb. 2022. URL: https://www.iso.org/standard/79637.html.

[47] Stephen D'Arcy und John C. Brogan. „Enterprise Risk Management“. In: *Journal of Risk Management of Korea* 12 (30. Mai 2001).

[48] Bundesamt für Sicherheit in der Informationstechnik. *Leitfaden zur Basis-Absicherung nach IT-Grundschutz*. 20. Okt. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.html.

[49] ISO/IEC JTC 1/SC 27. *ISO/IEC 27000:2018. Information security management systems - Overview and vocabulary*. Version 5. International Organization for Standardization, Feb. 2018. URL: https://www.iso.org/standard/73906.html.

[50] ISO/TC 251. *ISO 55000. Asset management — Overview, principles and terminology*. Version 1. International Organization for Standardization, Jan. 2014. URL: https://www.iso.org/standard/55088.html.

[51] Mario Sajko, Kornelije Rabuzin und Miroslav Bača. „How to calculate information value for effective security risk assessment“. In: *Journal of Information and Organizational Sciences* 30 (Dez. 2006).

[52] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutz-Kompendium*. 2. Aufl. Bundesanzeiger Verlag GmbH, 2019. ISBN: 978-3-8462-0906-6.

[53] Kevin Stine et al. *Guide for Mapping Types of Information and Information Systems to Security Categories*. NIST SP 800-60r1. National Institute of Standards and Technology, Aug. 2008. DOI: 10.6028/NIST.SP.800-60v1r1.

[54] ISO/TC 292. *ISO 22300. Security and resilience — Vocabulary*. Version 3. International Organization for Standardization, Feb. 2021. URL: https://www.iso.org/standard/77008.html.

[55] National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems*. 199. Feb. 2004.

[56] Bundesamt für Sicherheit in der Informationstechnik. *BSI-Standard 200-2. IT-Grundschutz-Methodik*. 15. Nov. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html.

[57] Yacov Haimes. „On the Complex Definition of Risk: A Systems-Based Approach“. In: *Risk analysis : an official publication of the Society for Risk Analysis* 29 (Nov. 2009), S. 1647–54. DOI: 10.1111/j.1539-6924.2009.01310.x.

[58] Terje Aven. „On Some Recent Definitions and Analysis Frameworks for Risk Vulnerability, and Resilience“. In: *Risk Analysis* 31.4 (2011), S. 515–522. DOI: 10.1111/j.1539-6924.2010.01528.x.

[59] Nayot Poolsappasit. „Towards an efficient vulnerability analysis methodology for better security risk management“. Diss. Fort Collins: Colorado State University, Department of Computer Science, 2010.

[60] Forum of Incident Response und Security Teams. *Common Vulnerability Scoring System*. URL: https://www.first.org/cvss/ (besucht am 24. 04. 2022).

[61] Golnaz Elahi, Eric Yu und Nicola Zannone. „Security Risk Management by Qualitative Vulnerability Analysis“. In: *2011 Third International Workshop on Security Measurements and Metrics*. 2011, S. 1–10. DOI: 10.1109/Metrisec.2011.12.

[62] Douglas J. Landoll. *The Security Risk Assessment Handbook. A Complete Guide for Performing Security Risk Assessments*. 3. Aufl. Boca Raton: CRC Press, 28. Sep. 2021. ISBN: 978-1-003-09044-1. DOI: 10.1201/9781003090441.

[63] Mouna Jouini, Latifa Ben Arfa Rabai und Anis Ben Aissa. „Classification of Security Threats in Information Systems“. In: *Procedia Computer Science* 32 (2014), S. 489–496. ISSN: 1877-0509. DOI: 10.1016/j.procs.2014.05.452.

[64] Savita Kumari Sheoran und Partibha Yadav. „An Innovative Model for Security Threats Classification in Information System“. In: *International Journal of Approximate Reasoning* 5 (2017), S. 2291–2294.

[65] European Network and Information Security Agency. *Threat Taxonomy*. Sep. 2016. URL: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.

[66] The MITRE Corporation. *MITRE ATT&CK*. URL: https://attack.mitre.org/ (besucht am 01. 02. 2024).

[67] ISO/TMBG. *ISO Guide 73:2009. Risk management — Vocabulary*. International Organization for Standardization, Nov. 2009. URL: https://www.iso.org/standard/44651.html.

[68] Terje Aven. „On how to define, understand and describe risk“. In: *Reliability Engineering & System Safety* 95.6 (2010), S. 623–631. ISSN: 0951-8320. DOI: 10.1016/j.ress.2010.01.011.

[69] Terje Aven. „On the new ISO guide on risk management terminology“. In: *Reliability Engineering & System Safety* 96.7 (2011), S. 719–726. ISSN: 0951-8320. DOI: 10.1016/j.ress.2010.12.020.

[70] Terje Aven und Ortwin Renn. „On risk defined as an event where the outcome is uncertain“. In: *Journal of Risk Research* 12 (Jan. 2009), S. 1–11. DOI: 10.1080/13669870802488883.

[71] National Bureau of Standards. *Guideline for Automatic Data Processing Risk Analysis*. 65. 1. Aug. 1979. DOI: 10.6028/NBS.FIPS.65.

[72] Sergio B. Guarro. „Principles and procedures of the LRAM approach to information systems risk analysis and management“. In: *Computers & Security* 6.6 (1987), S. 493–504. ISSN: 0167-4048. DOI: 10.1016/0167-4048(87)90030-7.

[73] Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar und Mohamed Cheriet. „Taxonomy of information security risk assessment (ISRA)“. In: *Computers & Security* 57 (2016), S. 14–30. ISSN: 0167-4048. DOI: 10.1016/j.cose.2015.11.001.

[74] Bob Blakley, Ellen McDermott und Dan Geer. „Information Security is Information Risk Management“. In: *Proceedings of the 2001 Workshop on New Security Paradigms*. NSPW '01. Association for Computing Machinery, 10. Sep. 2001, S. 97–104. ISBN: 1-58113-457-6. DOI: 10.1145/508171.508187.

[75] Lawrence D. Bodin, Lawrence A. Gordon und Martin P. Loeb. „Information Security and Risk Management“. In: *Communications of the ACM* 51.4 (1. Apr. 2008), S. 64–68. ISSN: 00010782. DOI: 10.1145/1330311.1330325. URL: http://portal.acm.org/citation.cfm?doid=1330311.1330325.

[76] Farhad Foroughi. „Information Asset Valuation Method for Information Technology Security Risk Assessment“. In: *Lecture Notes in Engineering and Computer Science* 2170 (Juli 2008).

[77] European Network and Information Security Agency. *Introduction to Return on Security Investment. Helping CERTs assessing the cost of (lack of) security*. 12. Dez. 2012. URL: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment.

[78] Wes Sonnenreich, Jason Albanese und Bruce Stout. „Return On Security Investment (ROSI): A Practical Quantitative Model“. In: *Journal of Research and Practice in Information Technology* 38 (Jan. 2006).

[79] Philip Bromiley et al. „Enterprise Risk Management: Review, Critique, and Research Directions“. In: *Long Range Planning* 48.4 (Apr. 2015), S. 265–276. ISSN: 0024-6301. DOI: 10.1016/j.lrp.2014.07.005.

[80] Basie Solms und Rossouw Solms. „Cyber security and information security - what goes where?“ In: *Information and Computer Security* 26 (Jan. 2018). DOI: 10.1108/ICS-04-2017-0025.

[81] Ebru Yeniman Yildirim. „The Importance of Risk Management in Information Security“. In: *International Journal of Advances in Electronics and Computer Science* 4 (Jan. 2017).

[82] Gaute Wangen, Christoffer Hallstensen und Einar Snekkenes. „A Framework for Estimating Information Security Risk Assessment Method Completeness: Core Unified Risk Framework, CURF“. In: *International Journal of Information Security* 17.6 (1. Nov. 2018), S. 681–699. DOI: 10.1007/s10207-017-0382-0.

[83] Amulya Gurtu und Jestin Johny. „Supply Chain Risk Management: Literature Review“. In: *Risks* 9 (Jan. 2021), S. 16. DOI: 10.3390/risks9010016.

[84] Terje Aven. „Risk assessment and risk management: Review of recent advances on their foundation“. In: *European Journal of Operational Research* 253.1 (16. Aug. 2016), S. 1–13. ISSN: 0377-2217. DOI: 10.1016/j.ejor.2015.12.023.

[85] Piyush Singhal, G. Agarwal und M.L. Mittal. „Supply chain risk management: Review, classification and future research directions“. In: *International Journal of Business Science & Applied Management* 6 (Jan. 2011).

[86] Stephan Wagner und Christoph Bode. „Dominant Risks and Risk Management Practices in Supply Chains“. In: *Supply Chain Risk: A Handbook of Assessment, Management, and Performance*. Hrsg. von George A. Zsidisin und Bob Ritchie. Springer US, 2009, S. 271–290. ISBN: 978-0-387-79934-6. DOI: 10.1007/978-0-387-79934-6_17.

[87] Simon Véronneau und Jacques Roy. „Security at the source: securing today's critical supply chain networks“. In: *Journal of Transportation Security* 7.4 (1. Dez. 2014), S. 359–371. DOI: 10.1007/s12198-014-0149-z.

[88] Panos Kouvelis und Jian Li. „Flexible Backup Supply and the Management of Lead-Time Uncertainty“. In: *Production and Operations Management* 17.2 (2008), S. 184–199. DOI: 10.3401/poms.1080.0015.

[89] Yossi Sheffi. „Supply chain management under the threat of international terrorism“. In: *The International Journal of logistics management* 12.2 (2001), S. 1–11.

[90] Dr Abhijeet Ghadge et al. „Managing cyber risk in supply chains: A review and research agenda“. In: *Supply Chain Management* (Juli 2019), S. 1–36. DOI: 10.1108/SCM-10-2018-0357.

[91] Jon M. Boyens et al. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. NIST SP 800-161. National Institute of Standards and Technology, Apr. 2015. DOI: 10.6028/NIST.SP.800-161.

[92] National Institute of Standards and Technology. *Minimum Security Requirements for Federal Information and Information Systems*. 200. März 2006. DOI: 10.6028/NIST.FIPS.200.

[93] Kirstin Scholten und Sanne Schilder. „The role of collaboration in supply chain resilience“. In: *Supply Chain Management: An International Journal* 20 (Juni 2015), S. 471–484. DOI: 10.1108/SCM-11-2014-0386.

[94] Jon Boyens et al. *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*. National Institute of Standards and Technology, Feb. 2021. DOI: 10.6028/NIST.IR.8276.

[95] Mass Lund, Bjørnar Solhaug und Ketil Stølen. *Model-Driven Risk Analysis. The CORAS Approach*. Springer, 2011. ISBN: 978-3-642-12322-1. DOI: 10.1007/978-3-642-12323-8.

[96] Zeki Yazar. *A Qualitative Risk Analysis and Management Tool - CRAMM*. SANS, 11. Apr. 2002. URL: https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83.

[97] ISO/IEC JTC 1/SC 27. *ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls*. Version 3. International Organization for Standardization, März 2022. URL: https://www.iso.org/standard/75652.html.

[98] ISO/IEC JTC 1/SC 27. *ISO/IEC 27005:2018. Security techniques - Information security risk management*. International Organization for Standardization, Juli 2018. URL: https://www.iso.org/standard/75281.html.

[99] ISO/TC 262. *ISO/IEC 31010. Risk Management - Risk Assessment Techniques*. Version 2. International Organization for Standardization, Juni 2019. URL: https://www.iso.org/standard/72140.html.

[100] ISO/TC 262. *IWA 31. Risk Management - Guidelines on using ISO 31000 in management systems*. International Organization for Standardization, Juli 2020. URL: https://www.iso.org/standard/75812.html.

[101] Bundesamt für Sicherheit in der Informationstechnik. *BSI-Standard 200-3. Risk Analysis based on IT-Grundschutz*. 15. Nov. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html.

[102] Bundesamt für Sicherheit in der Informationstechnik. *BSI-Standard 200-4. Business Continuity Management*. 14. Juni 2023. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf.

[103] Joint Task Force. *Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy*. NIST SP 800-37r2. National Institute of Standards and Technology, Dez. 2018. DOI: 10.6028/NIST.SP.800-37r2.

[104] Joint Task Force Transformation Initiative. *Managing Information Security Risk. Organization, Mission, and Information System View*. NIST SP 800-39. National Institute of Standards and Technology, März 2011. DOI: 10.6028/NIST.SP.800-39.

[105] Joint Task Force Transformation Initiative. *Guide for Conducting Risk Assessments*. NIST SP 800-30r1. National Institute of Standards and Technology, Sep. 2012. DOI: 10.6028/NIST.SP.800-30r1.

[106] Joint Task Force Transformation Initiative. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST SP 800-53r4. National Institute of Standards and Technology, Apr. 2013. DOI: 10.6028/NIST.SP.800-53r4.

[107] Marianne Swanson et al. *Contingency Planning Guide for Federal Information Systems*. NIST SP 800-34r1. National Institute of Standards and Technology, Mai 2010. DOI: 10.6028/NIST.SP.800-34r1.

[108] National Institute of Standards and Technology. *NIST Risk Management Framework*. 1. Nov. 2021. URL: https://csrc.nist.gov/Projects/risk-management (besucht am 20. 11. 2021).

[109] Information Systems Audit and Control Association. *COBIT 5*. COBIT 5. 2012. ISBN: 978-1-60420-237-3.

[110] Information Systems Audit and Control Association. *COBIT 5 for Information Security*. COBIT 5. 2012. ISBN: 978-1-60420-255-7.

[111] Information Systems Audit and Control Association. *COBIT 5 for Risk*. COBIT 5. Rolling Meadows, IL., 2013. ISBN: 978-1-60420-457-5.

[112] Information Systems Audit and Control Association. *COBIT 2019 Framework. Governance and Management Objectives*. COBIT 2019. 2018. ISBN: 978-1-60420-764-4.

[113] Information Systems Audit and Control Association. *COBIT 2019 Framework. Introduction and Methodology*. COBIT 2019. 2018. ISBN: 978-1-60420-763-7.

[114] Information Systems Audit and Control Association. *COBIT Focus Area: Information Security. Using COBIT 2019*. COBIT 2019. 1. Okt. 2020. ISBN: 978-1-60420-828-3.

[115] Information Systems Audit and Control Association. *COBIT Focus Area: Information and Technology Risk. Using COBIT 2019*. COBIT 2019. 1. Okt. 2020. ISBN: 978-1-60420-828-3.

[116] Committee of Sponsoring Organizations of the Treadway Commission. *COSO Enterprise Risk Management. Integrating with Strategy and Performance*. Juli 2017.

[117] Information Systems Audit and Control Association. *Risk IT Framework*. Rolling Meadows, IL, 2009. ISBN: 978-1-60420-111-6.

[118] Information Systems Audit and Control Association. *Risk IT Practitioner Guide*. 2009. ISBN: 978-1-60420-116-1.

[119] Information Systems Audit and Control Association. *Risk IT Framework*. 2. Aufl. 2020. ISBN: 978-1-60420-820-7.

[120] Jack Freund und Jack Jones. *Measuring and Managing Information Risk. A FAIR Approach*. Butterworth-Heinemann, 22. Aug. 2014. ISBN: 978-0-12-420231-3.

[121] The Open Group. *Risk Analysis (O-RA)*. Open Group Technical Standard. Okt. 2013. ISBN: 1937218416. URL: https://publications.opengroup.org/c13g.

[122] The Open Group. *Risk Taxonomy (O-RT)*. 2. Aufl. Open Group Technical Standard. Okt. 2013. ISBN: 1937218423. URL: https://publications.opengroup.org/c13k.

[123] Christopher Alberts und Audrey Dorofee. *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley Professional, 2002. ISBN: 0-321-11886-3.

[124] The Open Group. *FAIR - ISO/IEC 27005 Cookbook*. 1. Nov. 2010. ISBN: 1-931624-87-9. URL: https://publications.opengroup.org/c103.

[125] The Open Group. *The Open FAIR - NIST Cybersecurity Framework Cookbook*. 13. Okt. 2016. ISBN: 1-937218-80-5. URL: https://publications.opengroup.org/g167.

[126] Axelos. *Management of Risk: Creating and Protecting Value*. 4. Aufl. PeopleCert, 1. Jan. 2022. ISBN: 978-0-11-331274-0.

[127] Axelos. *Management of Risk: Guidance for Practitioners*. 3. Aufl. The Stationery Office, 9. Dez. 2010. ISBN: 978-0-11-331274-0.

[128] European Network and Information Security Agency. *ENISA RM/RA Framework*. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management (besucht am 19. 08. 2022).

[129] ENISA Technical Department. *Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment Methods and Tools*. European Network and Information Security Agency, 1. Juni 2006. URL: https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools.

[130] Daniele Catteddu und Giles Hogben. *Cloud Computing. Benefits, Risks and Recommendations for Information Security*. European Network and Information Security Agency, 20. Nov. 2009. URL: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

[131] Cédric Lévy-Bencheton et al. *Threat Landscape and Good Practice Guide for Internet Infrastructure*. European Network and Information Security Agency, 15. Jan. 2015. DOI: 10.2824/34387.

[132] Claudia Colicchia, Alessandro Creazza und David Menachof. „Managing cyber and information risks in supply chains: insights from an exploratory analysis“. In: *Supply Chain Management: An International Journal* 24 (Dez. 2018). DOI: 10.1108/SCM-09-2017-0289.

[133] Mu-Chen Chen, Taho Yang und Hsin-Chia Li. „Evaluating the supply chain performance of IT-based inter-enterprise collaboration“. In: *Information & Management* 44 (Sep. 2007), S. 524–534. DOI: 10.1016/j.im.2007.02.005.

[134] Alessandro Creazza et al. „Who cares? Supply chain managers perceptions regarding cyber supply chain risk management in the digital transformation era“. In: *Supply Chain Management: An International Journal* (Mai 2021). DOI: 10.1108/SCM-02-2020-0073.

[135] Ernest R. Alexander. „Interorganizational Coordination: Theory and Practice“. In: *Journal of Planning Literature* 7 (1. Mai 1993), S. 328–343. DOI: 10.1177/088541229300700403.

[136] Steve Cropper et al. „Introducing Inter-organizational Relations“. In: *The Oxford Handbook of Inter-Organizational Relations* (Jan. 2009). DOI: 10.1093/oxfordhb/9780199282944.003.0001.

[137] Dudenredaktion. *Joint Venture*. Duden online. 13. Apr. 2023. URL: https://www.duden.de/node/73483/revision/1298905.

[138] Johann Engelhard und Jörn Altmann. *Joint Venture*. Gabler Wirtschaftslexikon. Springer Gabler Verlag. 19. Feb. 2018. URL: https://wirtschaftslexikon.gabler.de/definition/joint-venture-37135/version-260578.

[139] SHARE NOW GmbH. *History of SHARE NOW car-sharing*. URL: https://www.share-now.com/de/en/history/ (besucht am 16. 05. 2023).

[140] Mercedes-Benz Group AG. *Mercedes-Benz and Google Join Forces*. URL: https://group.mercedes-benz.com/company/news/mercedes-benz-and-google.html (besucht am 16. 05. 2023).

[141] Dudenredaktion. *Föderation*. Duden online. 27. Apr. 2018. URL: https://www.duden.de/node/49320/revision/49356.

[142] Dudenredaktion. *Konsortium*. Duden online. 14. Apr. 2023. URL: https://www.duden.de/node/82130/revision/1412156.

[143] Münchner Verkehrs- und Tarifverbund GmbH. *Der MVV-Verbundgedanke. 1 Netz. 1 Fahrplan. 1 Ticket.* URL: https://www.mvv-muenchen.de/mvv-und-service/der-mvv/der-verbundgedanke/index.html (besucht am 16. 05. 2023).

[144] Dudenredaktion. *Konzern*. Duden online. 27. Apr. 2018. URL: https://www.duden.de/node/82629/revision/82665.

[145] GÉANT Association. *GÉANT Website. GÉANT Projects*. URL: https://geant.org/projects/ (besucht am 10. 08. 2023).

[146] DFN-Verein e.V. *DFN Website. Der Verein*. URL: https://www.dfn.de/dfn-verein/ (besucht am 12. 01. 2024).

[147] Europäische Kommission. *Research and innovation. Horizon 2020*. Funding programme. URL: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en (besucht am 17. 09. 2023).

[148] Europäische Kommission. *Research and innovation. Horizon Europe*. Funding programme. URL: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en (besucht am 17. 09. 2023).

[149] GÉANT Association. *GÉANT Association Website. About GÉANT*. URL: https://about.geant.org/ (besucht am 25. 08. 2023).

[150] GÉANT Association. *eduGAIN Website*. URL: https://edugain.org/ (besucht am 18. 09. 2023).

[151] GÉANT Association. *eduroam Website*. URL: https://eduroam.org/ (besucht am 18. 09. 2023).

[152] Sarunas Grigaliunas et al. *Deliverable D8.1 Summary of Security Training and Awareness Campaign Materials. An Investigation and Gap Analysis of Current Security Training and Awareness Resources*. GÉANT Association, 9. Juni 2020. URL: https://geant.org/projects/gn4-3-deliverables/.

[153] Klaus Möller et al. *Deliverable D8.5 Security Training Materials for NRENs and Constituents*. GÉANT Association, 22. Dez. 2021. URL: https://geant.org/projects/gn4-3-deliverables/.

[154] Bart Bosma et al. *Deliverable D8.9 Best Practices for Security Operations in Research and Education*. GÉANT Association, 30. Juni 2022. URL: https://geant.org/projects/gn4-3-deliverables/.

[155] David Heed et al. *Deliverable D8.6 Vulnerability Assessment as a Service Pilot Project*. GÉANT Association, 16. Aug. 2022. URL: https://geant.org/projects/gn4-3-deliverables/.

[156] Nicole Harris et al. *Deliverable D8.2 Security Baseline for NRENs*. GÉANT Association, 7. März 2020. URL: https://geant.org/projects/gn4-3-deliverables/.

[157] Anastas Mishev et al. *Deliverable D8.12 GÉANT Community Requirements for Business Continuity Planning*. GÉANT Association, 7. Mai 2021. URL: https://geant.org/projects/gn4-3-deliverables/.

[158] Charlie van Genuchten et al. *Deliverable D8.13 GÉANT Community Requirements for Crisis Management*. GÉANT Association, 2. Juni 2021. URL: https://geant.org/projects/gn4-3-deliverables/.

[159] Christine Bullen und John Rockart. „A primer on critical success factors“. In: *Sloan Working Papers*. 1981.

[160] Sylvie K. Chetty und Heather I.M. Wilson. „Collaborating with competitors to acquire resources“. In: *International Business Review* 12.1 (2003), S. 61–81. DOI: 10.1016/S0969-5931(02)00088-4.

[161] Claudia Loebbecke, Paul C. van Fenema und Philip Powell. „Managing inter-organizational knowledge sharing“. In: *The Journal of Strategic Information Systems* 25.1 (2016), S. 4–14. ISSN: 0963-8687. DOI: 10.1016/j.jsis.2015.12.002.

[162] Ying-Hueih Chen, Tzu-Pei Lin und David C. Yen. „How to facilitate inter-organizational knowledge sharing: The impact of trust“. In: *Information & Management* 51.5 (2014), S. 568–578. DOI: 10.1016/j.im.2014.03.007.

[163] Cynthia Hardy, Nelson Phillips und Thomas B. Lawrence. „Resources, Knowledge and Influence: The Organizational Effects of Interorganizational Collaboration“. In: *Journal of Management Studies* 40.2 (2003), S. 321–347. DOI: 10.1111/1467-6486.00342.

[164] Gregory B. White. „The Community Cyber Security Maturity Model“. In: *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. 2007, S. 99–99. DOI: 10.1109/HICSS.2007.522.

[165] Michael Schmidt und Miran Mizani. „Opportunities of Interorganizational Collaboration in Information Security Management“. In: *International Journal of Information Security* (2024). Eingereicht.

[166] Reinhard Bachmann und Arjen van Witteloostuijn. „Analyzing Inter-Organizational Relationships In The Context Of Their National Business Systems. A Conceptual Framework for Comparative Research“. In: *European Societies* 11 (Feb. 2009), S. 49–76. DOI: 10.1080/14616690801941084.

[167] Thomas Ritter und Hans Gemuenden. „Interorganizational relationships and networks: An overview“. In: *Journal of Business Research* 56 (Feb. 2003), S. 691–697. DOI: 10.1016/S0148-2963(01)00254-5.

[168] Niki Panteli und Siva Sockalingam. „Trust and conflict within virtual inter-organizational alliances: a framework for facilitating knowledge sharing“. In: *Decision Support Systems* 39.4 (2005), S. 599–617. ISSN: 0167-9236. DOI: 10.1016/j.dss.2004.03.003.

[169] Eiren Tuusjärvi und Kristian Möller. „Multiplicity of norms in inter-company cooperation“. In: *Journal of Business & Industrial Marketing* 24 (Aug. 2009), S. 519–528. DOI: 10.1108/08858620910986758.

[170] Paul D Cousins. „A conceptual model for managing long-term inter-organisational relationships“. In: *European Journal of Purchasing & Supply Management* 8.2 (2002), S. 71–82. DOI: 10.1016/S0969-7012(01)00006-5.

[171] Ravi Singh Achrol. „Changes in the theory of interorganizational relations in marketing: Toward a network paradigm“. In: *Journal of the Academy of Marketing Science* 25 (Dez. 1997), S. 56–71. DOI: 10.1007/BF02894509.

[172] M. Bensaou. „Interorganizational Cooperation: The Role of Information Technology An Empirical Comparison of U.S. and Japanese Supplier Relations“. In: *Information Systems Research* 8.2 (1997), S. 107–124.

[173] Ivan Pouwels und Ferry Koster. „Inter-organizational cooperation and organizational innovativeness. A comparative study“. In: *International Journal of Innovation Science* 9 (Feb. 2017). DOI: 10.1108/IJIS-01-2017-0003.

[174] Dries Faems und Bart Looy. „The role of inter-organizational collaboration within innovation strategies: towards a portfolio approach“. In: *Katholieke Universiteit Leuven, Open Access publications from Katholieke Universiteit Leuven* (Jan. 2003).

[175] Joris Knoben und Leon Oerlemans. „Proximity and Inter-Organizational Collaboration: A Literature Review“. In: *International Journal of Management Reviews* 8 (Juni 2006), S. 71–89. DOI: 10.1111/j.1468-2370.2006.00121.x.

[176] Barbara Gray. „Conditions Facilitating Interorganizational Collaboration“. In: *Human Relations* 38.10 (1985), S. 911–936. DOI: 10.1177/001872678503801001.

[177] Aric Rindfleisch. „Organizational Trust and Interfirm Cooperation: An Examination of Horizontal Versus Vertical Alliances“. In: *Marketing Letters* 11 (2000), S. 81–95.

[178] Howard E. Aldrich. *Organizations and Environments*. Prentice-Hall, 1979. ISBN: 978-0-13-641431-5.

[179] Walter Powell. „Neither Market Nor Hierarchy: Network Forms of Organization“. In: *Research in Organizational Behaviour* 12 (1990), S. 295–336.

[180] Maryam R. Nezami et al. „Collaboration and Data Sharing in Inter-Organizational Infrastructure Construction Projects“. In: *Sustainability* 14.24 (2022). DOI: 10.3390/su142416835.

[181] Mari Sako. *Price, Quality and Trust: Inter-firm Relations in Britain and Japan*. Cambridge Studies in Management. Cambridge University Press, 1992. DOI: 10.1017/CBO9780511520723.

[182] Roy Lewicki und Barbara Bunker. „Developing and Maintaining Trust in Working Relations“. In: *Trust in organizations: Frontiers of theory and research*. SAGE Publications, Jan. 1996, S. 114–139. ISBN: 978-0-8039-5740-4. DOI: 10.4135/9781452243610.n7.

[183] Robert Morgan und Shelby Hunt. „The Commitment-Trust Theory of Relationship Marketing“. In: *the journal of marketing* 58 (Apr. 1994), S. 20–38. DOI: 10.2307/1252308.

[184] Joseph Raelin. „A Mandated Basis of Interorganizational Relations: The Legal-Political Network“. In: *Human Relations* 33 (1980), S. 57–68. DOI: 10.1177/001872678003300104.

[185] William Edwards Deming. *Out of the Crisis: Quality, Productivity and Competitive Position*. Cambridge University Press, 1986.

[186] Dudenredaktion. *Organisation*. Duden online. 13. Apr. 2023. URL: https://www.duden.de/node/106413/revision/1242985.

[187] Matthias Hamm. „Eine Methode zur Spezifikation der IT-Service-Managementprozesse Verketteter Dienste“. Diss. München: Ludwig-Maximilians-Universität, Juni 2009. DOI: 10.5282/edoc.10264.

[188] Gabriela-Patricia Marcu. „Architekturkonzepte für interorganisationales Fehlermanagement“. Diss. München: Ludwig-Maximilians-Universität, 2011. DOI: 10.5282/edoc.13106.

[189] Jürgen Weber und Gerhard Schewe. *Profitcenter*. Gabler Wirtschaftslexikon. Springer Gabler Verlag. 14. Feb. 2018. URL: https://wirtschaftslexikon.gabler.de/definition/profitcenter-44391/version-267702.

[190] Axelos. *ITIL 4: Create, Deliver and Support*. ITIL 4 Managing Professional. The Stationery Office, 31. Jan. 2020. ISBN: 978-0-11-331632-8.

[191] Joseph Raelin. „Policy output model of interorganizational relations“. In: *Organization Studies* 3 (Jan. 1982), S. 243–267. DOI: 10.2139/ssrn.3929032.

[192] ISO/IEC JTC 1/SC 27. *ISO/IEC TS 27022:2021. Guidance on information security management system processes*. Version 1. International Organization for Standardization, März 2021. URL: https://www.iso.org/standard/61004.html.

[193] Michael Schmidt. „Information security risk management terminology and key concepts“. In: *Risk Management* 25.1 (16. Dez. 2023), S. 1–23. DOI: 10.1057/s41283-022-00108-8.

[194] Stephen N. Luko und Mark E. Johnson. „Statistical Standards and ISO, Part 2 - Terminology“. In: *Quality Engineering* 24.2 (2012), S. 346–353. DOI: 10.1080/08982112.2012.654437.

[195] Alain Rey. *Essays on Terminology*. John Benjamins, 16. März 1995. ISBN: 978-90-272-8358-0. DOI: 10.1075/btl.9.

[196] Hendrik J. Kockaert und Frieda Steurs. *Handbook of Terminology*. Bd. 1. John Benjamins, 13. März 2015. ISBN: 978-90-272-5777-2. DOI: 10.1075/hot.1.

[197] ISO/TC 37/SC 1. *ISO 1087:2019. Terminology work and terminology science — Vocabulary*. Version 2. International Organization for Standardization, Sep. 2019. URL: https://www.iso.org/standard/62330.html.

[198] ISO/TC 37/SC 1. *ISO 860:2007. Terminology work — Harmonization of concepts and terms*. Version 3. International Organization for Standardization, Nov. 2007. URL: https://www.iso.org/standard/40130.html.

[199] David Brooks. *Key concepts in security risk management: A psychometric concept map to approach to understanding*. Saarbrücken: VDM Verlag, 2009.

[200] Standards Australia. *AS/NZS 4360:2004. Risk management*. 31. Aug. 2004.

[201] Stephen N. Luko. „Risk Management Terminology“. In: *Quality Engineering* 25.3 (2013), S. 292–297. DOI: 10.1080/08982112.2013.786336.

[202] American National Standards Institute. *ANSI/ASSE Z690.1. Vocabulary for Risk Management*. 2011.

[203] Stephen N. Luko. „Risk Management Principles and Guidelines“. In: *Quality Engineering* 25.4 (2013), S. 451–454. DOI: 10.1080/08982112.2013.814508.

[204] Stephen N. Luko. „Risk Assessment Techniques“. In: *Quality Engineering* 26.3 (2014), S. 379–382. DOI: 10.1080/08982112.2014.875769.

[205] Michele Boulanger, Mark E. Johnson und Stephen N. Luko. „Statistical Standards and ISO, Part 1“. In: *Quality Engineering* 24.1 (2012), S. 94–101. DOI: 10.1080/08982112.2012.623956.

[206] Terje Aven et al. *Society for Risk Analysis Glossary*. SRA. Aug. 2018. URL: https://www.sra.org/risk-analysis-introduction/risk-analysis-glossary/.

[207] Committee on National Security Systems. *CNSS Glossary*. 4009. 6. Apr. 2015. URL: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf.

[208] Michael Dallas. *Management of Risk: Guidance for Practitioners and the international standard on risk management, ISO 31000:2009*. The British Standards Institution, Apr. 2013.

[209] European Union Agency for Cybersecurity. *Risk Management Glossary*. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary (besucht am 08. 01. 2021).

[210] Information Systems Audit and Control Association. *Glossary*. 2020. URL: www.isaca.org/resources/glossary (besucht am 17. 07. 2020).

[211] Michael Schmidt, Michael Brenner und Thomas Schaaf. „IT Service Management Frameworks Compared - Simplifying Service Portfolio Management“. In: *IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. 2019, S. 421–427.

[212] ISO/IEC JTC 1/S27. *ISO/IEC 27032:2012. Guidelines for cybersecurity*. International Organization for Standardization, Juli 2012. URL: https://www.iso.org/standard/44375.html.

[213] Alireza Shameli-Sendi et al. „FEMRA: Fuzzy Expert Model for Risk Assessment“. In: *2010 Fifth International Conference on Internet Monitoring and Protection*. 2010, S. 48–53. DOI: 10.1109/ICIMP.2010.15.

[214] Frank Hyneman Knight. *Risk, uncertainty and profit*. New York: Kelley, 1921.

[215] Mike Brownsword und Rossi Setchi. „A Formalised Approach to the Management of Risk: Process Formalisation“. In: *International Journal of Knowledge and Systems Science* 2 (Juli 2011), S. 63–80. DOI: 10.4018/jkss.2011070105.

[216] TM Forum. *Information Framework (SID)*. Open Digital Framework (Frameworx). 20. Aug. 2019. URL: https://www.tmforum.org/resources/reference/gb922-information-framework-r19-0/.

[217] Simon von Danwitz. „Managing inter-firm projects: A systematic review and directions for future research“. In: *International Journal of Project Management* 36.3 (2018), S. 525–541. ISSN: 0263-7863. DOI: 10.1016/j.ijproman.2017.11.004.

[218] Dean A. Baker. *Multi-company Project Management. Maximizing Business Results Through Strategic Collaboration*. J. Ross Publishing, 15. Okt. 2009. ISBN: 978-1-60427-035-8.

[219] Lee Colquitt, Robert Hoyt und Ryan Lee. „Integrated Risk Management and the Role of the Risk Manager“. In: *Risk Management and Insurance Review* 2 (1999), S. 43–61. DOI: 10.1111/j.1540-6296.1999.tb00003.x.

[220] Mark Beasley, Richard Clune und Dana Hermanson. „Enterprise Risk Management: An Empirical Analysis of Factors Associated With the Extent of Implementation“. In: *Journal of Accounting and Public Policy* 24 (Nov. 2005), S. 521–531. DOI: 10.1016/j.jaccpubpol.2005.10.001.

[221] Object Management Group. *Business Process Model and Notation (BPMN)*. Version 2. 3. Jan. 2011. URL: http://www.omg.org/spec/BPMN/2.0.

[222] Alison Olechowski et al. „The professionalization of risk management: What role can the ISO 31000 risk management principles play?“ In: *International Journal of Project Management* 34.8 (Nov. 2016), S. 1568–1578. ISSN: 0263-7863. DOI: 10.1016/j.ijproman.2016.08.002.

[223] Knut Haufe. „Maturity based approach for ISMS governance“. Diss. Madrid: Universidad Carlos III de Madrid, 2017.

[224] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. 16. Apr. 2018. DOI: 10.6028/NIST.CSWP.04162018.

[225] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. *Cybersecurity Capability Maturity Model (C2M2)*. Version 2.1. Juni 2022. URL: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[226] ISO/IEC JTC 1/SC 7. *ISO/IEC 33004:2015. Process assessment - Requirements for process reference, process assessment and maturity models*. Version 1. International Organization for Standardization, Apr. 2017. URL: https://www.iso.org/standard/14256.html.

[227] Šarūnas Grigaliūnas et al. „Leveraging Taxonomical Engineering for Security Baseline Compliance in International Regulatory Frameworks“. In: *Future Internet* 15.10 (2023). DOI: 10.3390/fi15100330.

[228] ISO/IEC JTC 1/SC 27. *ISO/IEC 27001:2022. Information security management systems - Requirements*. Version 3. International Organization for Standardization, Okt. 2022. URL: https://www.iso.org/standard/27001.

[229] Martina De Gramatica et al. „The Role of Catalogues of Threats and Security Controls in Security Risk Assessment: An Empirical Study with ATM Professionals“. In: *Requirements Engineering: Foundation for Software Quality*. Hrsg. von Samuel A. Fricker und Kurt Schneider. Lecture Notes in Computer Science. 14. März 2015. ISBN: 978-3-319-16100-6. DOI: 10.1007/978-3-319-16101-3.

[230] Katsiaryna Labunets, Federica Paci und Fabio Massacci. „Which security catalogue is better for novices?“ In: *2015 IEEE Fifth International Workshop on Empirical Requirements Engineering (EmpiRE)*. 2015, S. 25–32. DOI: 10.1109/EmpiRE.2015.7431304.

[231] Bundesamt für Sicherheit in der Informationstechnik. *Elementare Gefährdungen*. 7. Dez. 2020. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Elementare_Gefaehrdungen.html.

[232] Ifigeneia Lella et al. *ENISA Threat Landscape 2021*. European Network and Information Security Agency, 27. Okt. 2021. DOI: 10.2824/324797.

[233] Nina Franze. „Bedrohungsmodellierung im Kontext Informationssicherheit“. Bachelorarbeit. München: Ludwig-Maximilians-Universität, 15. Juni 2021.

[234] ISO/IEC JTC 1. *ISO 7498-2:1989. Terminology work and terminology science — Vocabulary*. Version 1. International Organization for Standardization, Feb. 1989. URL: https://www.iso.org/standard/14256.html.

[235] Costas Papadatos et al. *Interoperable EU Risk Management Toolbox*. European Network and Information Security Agency, 21. Feb. 2023. DOI: 10.2824/68948.

[236] GÉANT Association. *GÉANT Security. Security Baseline*. A Security Maturity Model for NRENs. URL: https://security.geant.org/baseline/ (besucht am 14. 01. 2024).

[237] Heinz-Gerd Hegering, Sebastian Abeck und Bernhard Neumair. *Integriertes Management vernetzter Systeme: Konzepte, Architekturen und deren betrieblicher Einsatz*. Heidelberg: dpunkt.verlag, 1999. ISBN: 978-3-932588-16-7.

[238] Wolfgang Hommel. „Integriertes Management von Security-Frameworks“. Diss. München: Ludwig-Maximilians-Universität, 2012. DOI: 10.5282/ubm/epub.12963.

[239] Michael Nerb. „Customer Service Management als Basis für interorganisationales Dienstmanagement“. Diss. München: Ludwig-Maximilians-Universität, 2001.

[240] Helmut Reiser. „Sicherheitsarchitektur für ein Managementsystem auf der Basis mobiler Agenten“. Diss. München: Ludwig-Maximilians-Universität, 2001.

[241] Michael Schmidt und Jule Anna Ziegler. „An Identity Provider as a Service platform for the eduGAIN research and education community“. In: *IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. Mai 2019, S. 739–740.

[242] Michael Schmidt. „Ein Fachkonzept für ein leichtgewichtiges Serviceportfolio-, Servicekatalog- und Service-Level-Management“. Masterarbeit. München: Ludwig-Maximilians-Universität, 1. Aug. 2016.

[243] Jule Anna Ziegler, Michael Schmidt und Mikael Linden. „Improving Identity and Authentication Assurance in Research & Education Federations“. In: *International Workshop on Security and Trust Management*. 2019.

[244] Michael Schmidt, Stefan Metzger und Miran Mizani. „Managementsysteme ohne spezialisierte Tools etablieren. Ein leichtgewichtiger Ansatz zur Dokumentation im Service- und Informationssicherheitsmanagement“. In: *29. DFN-Konferenz „Sicherheit in vernetzten Systemen"*. Feb. 2022.

[245] Michael Schmidt, Stefan Metzger und Miran Mizani. „Aufbau eines Managementsystems - Tools vs. Prozesse“. In: *DFN Mitteilungen* (Juni 2022).

[246] Miran Mizani et al. „Transition zur neuen ISO/IEC 27001. Erfahrungen zum neuen Anhang A“. In: *30. DFN-Konferenz „Sicherheit in vernetzten Systemen"*. Feb. 2023.