St. Pölten University of Applied Sciences

/informatik & security

/fh/// st. pölten

Third-Party Risk Management

Wie sicher sind meine Lieferanten und Dienstleister?

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Thomas Bichler, BSc.
is201840

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer/Betreuerin: FH-Prof. Mag. Dr. Simon Tjoa
Mitwirkung: Simon Wilfing, MSc.

Frankenfels,
04.06.2022

(Unterschrift Autor/Autorin)

(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Frankenfels,
04.06.2022

(Unterschrift Autor/Autorin)

Zusammenfassung

Sowohl Outsourcing wie auch die Supply Chain führen dazu, dass Unternehmen eine Vielzahl an Beziehungen mit Dritten, sogenannten Third-Parties aufbauen. Durch die Digitalisierung und den steigenden Grad der Vernetzung zu diesen Dritten ergeben sich zusätzliche IT-Risiken für die Unternehmen. Das Ziel dieser Diplomarbeit ist es, zu beantworten, wie Unternehmen die IT-Sicherheit Ihrer Lieferanten und Dienstleister beurteilen können. Dazu wird die Forschungsfrage gestellt: „Wie können IT-Sicherheitsrisiken Dritter (Third-Parties), unter Berücksichtigung bekannter Methoden, Standards sowie aktueller Technologien, holistisch identifiziert und bewertet werden?“. Zur Beantwortung der Forschungsfrage wurde eine Literaturrecherche rund um die Thematik Third-Party Risk Management durchgeführt. Konkret wurden Methoden zur Identifikation und Beurteilung von Risiken, die sich durch Dritte ergeben, beleuchtet. Im ersten Schritt wurde der Stand der Wissenschaft erhoben. Danach wurden bekannte Third-Party Risk Management Frameworks untersucht. Als weiterer Schritt wurden Regularien hinsichtlich der Forderung eines Third-Party Risk Managements gesichtet. Darüber hinaus wurden Dienstleister, die die Aufgabe des Third-Party Risk Management für Unternehmen übernehmen, betrachtet und dazu der CEO eines österreichischen Anbieters befragt. Auf Basis der erhobenen Informationen wurde ein Modell zur Risikobewertung Dritter erarbeitet. Im Stand der Wissenschaft stellte sich heraus, dass der Thematik eine hohe Relevanz zugesprochen wird, diese gleichzeitig aber für Unternehmen besonders komplex und herausfordernd ist. So konnte festgestellt werden, dass sich noch kein standardisiertes Vorgehen durchgesetzt hat. Die Sichtung der Regularien zeigt jedoch klar, dass Third-Party Risk Management von den Unternehmen mehrfach gefordert wird. Darüber hinaus stellt die Arbeit fest, dass durch die Kombinationen unterschiedlicher Methoden wie Fragebögen, Risk-Scoring-Tools, Zertifizierungen oder Audits eine 360-Grad-Bewertung der Dritten erfolgen kann. Weiterführende Forschung könnte das erarbeitete Model im Praxiseinsatz validieren und erweitern.

Abstract

Both outsourcing and the supply chain lead companies to establish a large number of relationships with third parties. Digitalization and the increasing degree of networking with these third parties result in additional IT risks for companies. The aim of this thesis is to answer how companies can assess the IT security of their suppliers and service providers. For this purpose, the research question is posed: "How can IT security risks of third parties be identified and assessed holistically, taking into account known methods, standards as well as current technologies?". To answer the research question, a literature review around the topic of third-party risk management was conducted. Specifically, methods for identifying and assessing risks posed by third parties were examined. In a first step, the state of science was surveyed. Afterwards, known third-party risk management frameworks were inspected. As a further step, regulations were investigated regarding the requirement of third-party risk management. In addition, service providers who take over the task of third-party risk management for companies were reviewed and therefore the CEO of an Austrian provider was interviewed. Based on the information collected, a model for third-party risk assessment was developed. In the state of science, it turned out that the topic is attributed an enormous relevance, but at the same time it is enormously complex and challenging for companies. It was found that no standardized procedure has yet been established. However, the review of the regulations clearly shows that third-party risk management is demanded by the companies several times. Furthermore, the thesis states that a 360-degree assessment of third parties can be done by combining different methods such as questionnaires, risk scoring tools, certifications, or audits. Further research could validate and extend the elaborated model in practical use.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

Es ist fast schon zum Standard geworden, dass Unternehmen jene Tätigkeiten, die außerhalb der eigenen Kerntätigkeit liegen, an andere Unternehmen auslagern. So ist dies auch mit IT-Dienstleistungen häufig der Fall. Diese Auslagerung, meist „Outsourcing“ genannt, geht oftmals mit einer Vielzahl an Vorteilen wie Kostenreduktion, Konzentration auf das Kerngeschäft wie auch eine erhöhte Flexibilität und Qualitätssteigerung einher. Nicht zu vernachlässigen sind jedoch die Risiken, die sich durch Outsourcing beziehungsweise die Zusammenarbeit mit Dritten für die eigene Organisation ergeben [1]. Dass vor allem Sicherheitsrisiken damit einhergehen, zeigen die vielen Sicherheitsvorfälle und Datenpannen, die meist erhebliche Auswirkungen auf die betroffenen wie auch Partnerunternehmen hatten [2]. Laut einer Befragung durch das Ponemon Institute haben 51 % der Unternehmen bereits eine durch Dritte verursachte Datenschutzverletzung erlebt, die zum Missbrauch sensibler oder vertraulicher Informationen geführt hat [3]. Neben der bewussten Auslagerung von IT-Diensten führt auch die sogenannte Supply-Chain beziehungsweise Lieferkette zu einem steigenden Grad an Vernetzung und digitaler Integration. So sind Partnerunternehmen oftmals über die gesamte Lieferkette hin vernetzt, wodurch die operative Abwicklung von der Planung über die Überwachung bis hin zur Ausführung von Aufträgen effizienter gestaltet werden kann. Darüber hinaus haben diese Partner Ihre eigenen Partner, die wiederum andere Partner haben, woraus eine komplexe Vernetzung von Unternehmen entsteht [4]. Leider hängt genau diese Innovation und Vernetzung mit erheblichen Sicherheitsrisiken zusammen [5]. Denn wird nur eines der Unternehmen in der Kette kompromittiert, können die Folgen vielfältig und weitreichend sein. So reichen die Auswirkungen von Diebstahl sensibler Daten bis hin zur Unterbrechung des gesamten Geschäftsprozesses (zum Beispiel durch Ransomware oder Denial-of-Service) [6]. Der Security Threat Report 2019 von Symantec zeigt einen Anstieg der Angriffe auf die Supply Chain um 78 % im Jahr 2018 [7]. Ein prominentes Beispiel für eine Supply-Chain-Attacke liefert die sogenannte Operation ShadowHammer im Jahr 2018. Dabei wurde signierte Malware über die offizielle Downloadseite im „Asus Live Updater“ verteilt, die von bis zu einer Million Benutzer installiert wurde, bevor der Angriff entdeckt werden konnte [4].

Das Thema Third-Party Risk Management (TPRM) erlangt daher in vielen Unternehmen immer größer werdender Bedeutung, denn die Unternehmen sind meist von einer enormen Anzahl von Lieferanten, Partnern und anderen Dritten auf der ganzen Welt abhängig [8]. Dennoch zeigen Umfragen immer wieder, dass mehr als 50 % der Unternehmen keine Art von TPRM oder Cybersecurity-Due-Diligence für deren Lieferanten im Einsatz haben [3] [2]. Das TPRM beziehungsweise die Supply-Chain-Security sind keine gänzlich neuen Disziplinen, was durch die Existenz von Rahmenwerken, regulatorischen Richtlinien und Zertifizierungen rund um das Thema belegt wird [2]. Nichtsdestotrotz befindet sich die Forschung zum Thema Cybersicherheit in der Supply-Chain noch in den Kinderschuhen [9].

Vor diesem Hintergrund zielt diese Arbeit darauf ab, die Forschung im Bereich TPRM mit Bezug auf IT-Sicherheitsrisiken zu erweitern. Die Arbeit adressiert die Forschungsfrage: *Wie können IT-Sicherheitsrisiken Dritter (Third-Parties), unter Berücksichtigung bekannter Methoden, Standards sowie aktueller Technologien (* [10] [11] [12] [13]*), holistisch identifiziert und bewertet werden?* Für diese essenziellen TPRM-Phasen werden in der Literatur einige wenige Methoden aufgezeigt, die meist auch mit einer Vielzahl an Nachteilen behaftet sind [6]. Außerdem wird evaluiert, ob gesetzliche und regulatorische Vorschriften das Thema Third-Party Risk Management im Bereich der IT bereits berücksichtigen und welche Anforderungen sich daraus an eine österreichische Bank ergeben.

Die Arbeit teilt sich dazu in vier Teile. Im ersten Teil wird ein Überblick über das Thema TPRM geschaffen, wobei der Stand der Wissenschaft erhoben wird. TPRM im Blickwinkel regulatorischer und gesetzlicher Anforderungen wird im zweiten Teil behandelt. Der dritte Teil liefert einen Einblick in das Thema TPRM-as-a-Service; hierbei wird ein österreichischer Lösungsansatz näher betrachtet. Abschließend wird im vierten Teil auf das konkrete Vorgehen zur Risikobewertung von Dienstleistern und Lieferanten eingegangen und ein durch den Autor entwickelter Prozess vorgestellt.

2. Stand der Wissenschaft

Um einen Überblick über das Thema Third-Party Risk Management (TPRM) im IT-Umfeld zu erhalten, wurde im ersten Schritt eine Literaturrecherche durchgeführt. Im ersten Absatz wird die Methodik zur Literaturrecherche beschrieben. Darauffolgend werden im Literatureinblick die relevantesten Arbeiten durch eine Kurzfassung näher betrachtet. Jenen Arbeiten mit besonderer Relevanz wird eine ausführlichere Zusammenfassung gewidmet. Das letzte Kapitel der Literaturrecherche bildet den Literaturüberblick, wobei das Ergebnis tabellarisch aufbereitet wird. TPRM-Rahmenwerke, die durch internationale Gremien oder staatliche Organisationen geschaffen wurden, werden im eigenen Absatz 2.2 behandelt und gleichzeitig die für diese Arbeit wichtigsten Teile herausgefiltert. Den Abschluss dieses Kapitels bildet das Fazit, das den aktuellen Stand der Wissenschaft im TPRM-Bereich zusammenfast.

2.1. Literaturrecherche

Die Literaturrecherche teilt sich in zwei Suchvorgänge. Im ersten Teil wurde versucht, einen möglichst breiten Blickwinkel auf die Thematik zu werfen. Es galt, einen Überblick zu erhalten sowie möglichst viele Schlüsselwörter zu erheben. Darauf aufbauend wurde der zweite Teil durchgeführt, in dem systematisch nach geeigneter Literatur zur Beantwortung der Forschungsfrage gesucht wurde. Internationale Standards und staatliche Vorgehensweisen (ISO, NIST) wurden hierbei explizit ausgeklammert, da diese separat in 2.2 betrachtet werden.

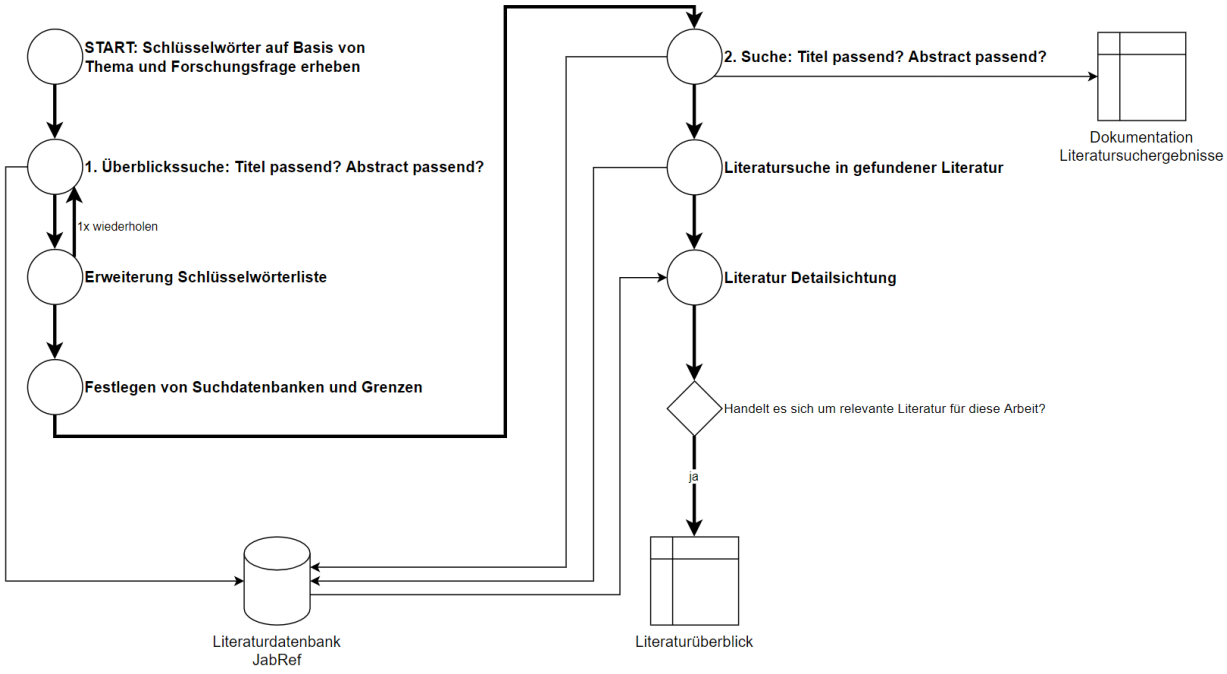

Abbildung 1: Ablauf der Literaturrecherche

2.1.1. Methodik

Zunächst wurde mit Schlüsselwörtern gesucht, welche sich direkt aus der Forschungsfrage und dem Titel ergeben. Diese wurden in dieser ersten offenen Suche unterschiedlich kombiniert.

Englisch	Deutsch
Third-party	Dritter
Third-party vendor	Drittanbieter
Risk	Risiko
Risk management	Risikomanagement
Risk assessment	Risikobewertung
Cybersecurity Cyber security Cyber	Cybersicherheit
IT security	IT-Sicherheit
Information security	Informationssicherheit

Tabelle 1: Schlüsselwörter für die initiale Suche

Dabei wurde vorrangig Google Scholar[1] verwendet, da hier direkt auf eine große Anzahl an wissenschaftlichen Datenbanken zurückgegriffen wird. Es wurden je Suche die ersten 50 Suchergebnisse auf Basis des Titels auf deren Relevanz für diese Arbeit überprüft. Relevante Arbeiten wurden gesichtet und in einer Literaturdatenbank[2] aufgenommen.

Auf Basis dieser ersten Recherche wurde die bestehende Schlüsselwörterliste erweitert.

Englisch	Deutsch
Third-party	Dritter
Third-party vendor **Third-party supplier** **Third-party provider**	Drittanbieter
Supplier	**Lieferant**
Supplier relationship	**Lieferantenbeziehung**
Risk	Risiko
Risk management	Risikomanagement
Assessment **Rating**	Bewertung **Beurteilung**
Cybersecurity Cyber security Cyber	Cybersicherheit
IT security	IT-Sicherheit
Information security	Informationssicherheit
Supply chain	**Lieferkette**
Supply chain management	**Lieferkettenmanagement**
IT outsourcing	**IT-Auslagerung**

Tabelle 2: Erweiterte Schlüsselwörterliste für initiale Suche

Durch diese erste Suche wurde eine Vielzahl an ähnlichen Bezeichnungen für Third-Party Risk Management entdeckt. In der Literatur tauchen für das Thema rund um die Steuerung der Risken von Dritten unterschiedliche Bezeichnungen auf. So wurden die folgenden Management-Bezeichnungen in Zusammenhang mit Third-Party Risk Management dokumentiert und sofern vorhanden mit einer Definition versehen:

[1] Google Scholar - https://scholar.google.de/
[2] JabRef

Third Party Risk Management (TPRM)
"Third-Party Risk Management (TPRM) ist der Prozess, mit dem Unternehmen die Interaktionen mit allen externen Parteien, insbesondere ihren Lieferanten, überwachen und verwalten." [14]

„Third-Party Risk Management ist die Gesamtheit der Risikomanagementpraktiken und -prozesse, die die Risiken, die mit Beziehungen zwischen Unternehmen und seinen Partnern verbunden sind, angemessen mindern." [15]

Vendor Risk Management (VRM)
„Beim Lieferantenrisikomanagement geht es darum, sicherzustellen, dass die Inanspruchnahme von Dienstleistern und IT-Lieferanten kein inakzeptables Potenzial für Geschäftsunterbrechungen oder negative Auswirkungen auf die Unternehmensleistung birgt." [16]

Supplier Risk Management (SRM)
„Supplier Risk Management ist definiert als der Prozess der Vorhersage und Vorbereitung auf Ereignisse, die sich negativ oder positiv auf die Lieferkette auswirken können." [17]

Supply Chain Risk Management (SCRM) / Supply Chain Management (SCM)
„Unter Supply Chain Risk Management versteht man den Prozess der Identifizierung, Bewertung und Abschwächung der Risiken in der Lieferkette eines Unternehmens." [18]
„Das Supply Chain Management umfasst die Planung und das Management aller Aktivitäten, die mit der Beschaffung, der Umwandlung und dem gesamten Logistikmanagement verbunden sind. Wichtig ist, dass es auch die Koordinierung und Zusammenarbeit mit den Vertriebspartnern umfasst, bei denen es sich um Lieferanten, Zwischenhändler, Drittdienstleister und Kunden handeln kann." [19]

Neben den oben genannten generischen Management-Bezeichnungen sind in der Literatur für IT-Sicherheit unterschiedlich zusammengesetzte Bezeichnungen zu finden:

- Third-Party Information Security Risk Management (TPISRM)
- Cyber Third-Party Risk Management (C-TPRM)
- Cyber Supply Chain Risk Management (C-SCRM)
- IT Vendor Risk Management (IT-VRM)

Systematische Literatursuche
Die Anzahl an unterschiedlichen Schlüsselwörtern und Bezeichnungen zeigte bereits im ersten Teil die Schwierigkeit der Literatursuche in diesem Themenbereich. Daher wird im zweiten Teil versucht, möglichst systematisch relevante Literatur zu identifizieren.
Im ersten Schritt wurden Suchbegriffe aus dem Teil eins abgeleitet und festgelegt, wie zum Beispiel „Third Party Risk Management". Im nächsten Schritt wurden geeignete Literatur-Datenbanken erhoben, zu welchen auch ein notwendiger Zugriff existiert – meist über den Bibliotheken-Zugang der Fachhochschule St. Pölten. Danach wurden Grenzen für die Literatursuche definiert, so werden nur die ersten 50 und somit relevantesten Suchergebnisse je Datenbank überprüft. Für die Sortierung dieser ersten 50 Ergebnisse werden die Standardeinstellungen der jeweiligen wissenschaftlichen Datenbank verwendet. Die Literaturdurchsicht erfolgte manuell, wobei zunächst Titel und Abstract betrachtet wurden.

Für die Umsetzung wurde eine Dokumentationstabelle angelegt, in der die Suchbegriffe und Sucherkenntnisse festgehalten wurden. Jede Suche wurde neben Google Scholar auch für ACM Digital Library[3], IEEE Xplore[4] und Springer Digital Library[5] verwendet. Anschließend wurden jeweils die ersten 50

[3] ACM Digital Library - https://dl.acm.org/
[4] IEEE Xplore - https://ieeexplore.ieee.org/
[5] Springer Digital Library - https://link.springer.com/

Treffer begutachtet, um die Relevanz für diese Arbeit und Forschungsfrage festzustellen. Sofern relevante Literatur identifiziert wurde, wurde diese in der Tabelle dokumentiert und die entsprechende Quellenangabe im Literatur-Manager aufgenommen.

Durch diese strukturierte Suche konnten weitere 27 relevante Beiträge erfasst werden. In Summe konnte durch die initiale Literaturrecherche, gemeinsam mit der strukturierten Suche, eine Literaturbasis von 37 Einträgen geschaffen werden.

Suche	Google Scholar		ACM Digital Library		IEEE Xplore		Springer Digital Library	
	Suchergebnisse	Bemerkung	*Suchergebnisse*	Bemerkung	Suchergebnisse	Bemerkung	*Suchergebnisse*	Bemerkung
"Third Party Risk Management"	*541*	7 rB	*1*	0 rB	1	1 rB	*13*	0 rB
"Vendor Risk Management"	*229*	3 rB 1 rvB	*0*	0 rB	1	0 rB	*3*	0 rB
"Supplier Risk Management"	*864*	0 rB	*2*	0 rB	1	0 rB	*21*	0 rB
"Supply Chain Risk Management" AND cyber	*3080*	6 rB	*13*	0 rB	8	0 rB	*266*	0 rB
"Third-Party Information Security Risk Management"	*1*	1 rvB	*0*	0 rB	0	0 rB	*0*	0 rB
"Cyber Third-Party Risk Management"	*8*	1 rvB	*0*	0 rB	0	0 rB	*0*	0 rB
"Cyber Supply Chain Risk Management"	*314*	2 rB 3 rvB	*1*	0 rB	0	0 rB	*13*	0 rB
"IT Vendor Risk Management"	*6*	0 rB	*0*	0 rB	1	0 rB	*1*	0 rB
third-party risk cyber	*85900*	1 rvB	*329398*	0 rB	53	0 rB	*9895*	0 rB
third-party risk "IT security"	*19100*	1 rB 1rvB	*316384*	0 rB	2	0 rB	*1845*	2 rvB
third-party risk rating	*224000*	0 rB	*415897*	0 rB	46	0 rB	*157742*	0 rB
vendor risk cyber	*52100*	1 rvB	*130957*	0 rB	14	0 rB	*1211*	1 rB
vendor risk "IT security"	*13400*	0 rB	*108275*	0 rB	4	0 rB	*300*	0 rB
supplier risk assessment cyber	*40200*	1 rvB	*260021*	1 rB	2	0 rB	*4429*	0 rB
vendor risk assessment cyber	*37100*	1 rvB	*224830*	0 rB	2	0 rB	*2933*	0 rB
risk "IT outsourcing"	*23800*	1 rB	*85856*	0 rB	55	2 rB	*1665*	0 rB
cyber "IT outsourcing"	*2330*	1 rB 1rvB	*32343*	0 rB	1	0 rB	*86*	0 rB
supply chain risk cyber	*76000*	1 rB 5 rvB	*222785*	0 rB	77	0 rB	*7731*	1 rvB
supply chain risk "IT security"	*13600*	1 rB	*205341*	0 rB	2	0 rB	*1059*	0 rB
Deutsch:								
Drittanbieter Risiken Cyber	*491*	0 rB	*32142*	0 rB	0	0 rB	*114*	0 rB
Drittanbieter Risiken "IT Sicherheit"	*435*	0 rB	*18*	0 rB	0	0 rB	*87*	0 rB
Drittanbieter Risiken Bewertung	*2700*	0 rB	*58*	0 rB	0	0 rB	*382*	0 rB
Lieferant Risiko "IT Sicherheit"	*2130*	0 rB	*18*	0 rB	0	0 rB	*298*	0 rB
Lieferant Risiko Beurteilung	*24000*	0 rB	*21*	0 rB	0	0 rB	*5944*	0 rB
Risiko "IT-Auslagerung"	*67*	0 rB	*1930*	0 rB	0	0 rB	*24*	0 rB
Cyber "IT-Auslagerung"	*6*	0 rB	*33969*	0 rB	0	0 rB	*5*	0 rB
Lieferkette Risiko Cyber	*1050*	0 rB	*32141*	0 rB	0	0 rB	*208*	0 rB
Lieferkette Risiko "IT Sicherheit"	*611*	0 rB	*19*	0 rB	0	0 rB	*190*	0 rB
rB ... relevant Beiträge								
rvB ... relevante aber bereits vorhandene Beiträge								
Suche abgeschlossen: 04.01.2022								

Abbildung 2: Dokumentation der strukturierten Literatursuche

Literatur in den recherchierten Beiträgen

Im nächsten Schritt wurden die Literaturverzeichnisse aus den bereits erfassten Beiträgen gesichtet, um dadurch mögliche Standardwerke oder neue Literatur zu erfassen.

Durch diese Überprüfung konnten zwei Arbeiten entdeckt werden, die einen ausführlichen Literaturüberblick zur Thematik Cyberrisiken in der Supply Chain aufstellen [9] [20]. Außerdem konnten noch einige weitere Arbeiten erfasst werden, wobei sich ein großer Teil bereits in der Datenbank befunden hat.

Fazit Methodik

In Summe wurden durch die oben beschriebenen Schritte der Literaturrecherche 44 Werke identifiziert. Davon wurden 27 Werke nach der Detailsichtung als relevant eingestuft und damit auch in den Literaturüberblick in **Fehler! Verweisquelle konnte nicht gefunden werden.** aufgenommen.

Grundsätzlich finden sich viele Arbeiten in den verwandten Bereichen Third-Party Risk-, Supply Chain Risk- oder auch IT-Outsourcing-Risk-Management. Es gibt jedoch nur sehr begrenzt Literatur, die sich mit der Identifizierung und Bewertung von IT-Sicherheitsrisiken in diesem Bereich auseinandersetzt. Dass der Bereich rund um das Thema Cyber-Third-Party-Risk-Management (C-TPRM) generell noch eher wenig erforscht ist, bestätigen auch andere Arbeiten [5] [21].

Durch die ausführliche Literaturrecherche konnten auch Bereiche ausfindig gemacht werden, die durch die initiale Suche unentdeckt blieben. So konnten relevante Arbeiten aus dem Bereich der Cyberversicherungen entdeckt werden. Diese Arbeiten liefern auch für diese Arbeit spannende Einblicke, denn vor allem auch Versicherer mit Cyberversicherungen im Portfolio müssen zur Erstellung der Polizze sowie Tarifeinstufung das Cyberrisiko der Versicherten bewerten [22].

In einer Vielzahl von Arbeiten wird für plakative Statistiken auf die Studien des Ponemon Institute verwiesen [22] [23] [24]. Eine prominente Ponemon Aussage aus dem Jahr 2021 lautet, dass bereits 51 % der Unternehmen eine durch Dritte verursachte Datenschutzverletzung erlebt haben, die zum Missbrauch sensibler oder vertraulicher Informationen geführt hat [3].

2.1.2. Literatureinblick

Im folgenden Literatureinblick werden die relevantesten wissenschaftlichen Arbeiten rund um TPRM kurz vorgestellt sowie deren gewonnene Erkenntnisse reflektiert. Als relevant werden diejenigen Arbeiten eingestuft, die entweder auf die Identifikation oder die Beurteilung der TP-Risiken näher eingehen. Diese sind in der Tabelle 3 in den Spalten „Methoden: Identifikation von TP-Risiken“ und „Methoden: Beurteilung von TP-Risiken“ mit einem „ja“ versehen. Darüber hinaus werden noch diejenigen Arbeiten beschrieben, die das TPRM im IT-Umfeld mit wesentlichen Fakten untermauern. Dazu zählen durchgeführte Studien oder Arbeiten, in denen die TPRM-Literatur näher beleuchtet wird.

Aubert [25] veröffentlichte bereits 1998 eine Arbeit mit dem Titel „Assessing the Risk of IT Outsourcing“. Er weist dabei auf die Relevanz des Risikomanagements bei IT-Outsourcing-Projekten hin. In der Arbeit konzentriert er sich auf die notwendigen Aktivitäten zur Risikobewertung. Diese beschreibt er wie folgt in drei Schritten: Identifizierung der potenziellen unerwünschten Folgen des IT-Outsourcings, Identifizierung der Risikofaktoren und Verknüpfung dieser mit unerwünschten Ergebnissen. Die aufgestellten Folgen durch IT-Outsourcing beinhalten zeitgemäß noch keine Cyberattacken verursacht durch Dritte, stattdessen wird auf mögliche versteckte Kosten, Rechtsstreitigkeiten oder den Verlust von internen Kompetenzen hingewiesen.

Dhillon et al. [26] befragten in Form einer Delphi-Studie sowohl Kunden als auch Lieferanten, um die wesentlichen Bedenken hinsichtlich der Informationssicherheit beim IT-Outsourcing zu identifizieren. Es wurden dabei US-Firmen mit bestehenden Outsourcing-Verträgen mit indischen Unternehmen befragt. Durch die Umfrage auf beiden Seiten konnte sowohl eine Priorisierung der Lieferanten- wie auch der Kundenbedenken erstellt werden. Die größte Sorge auf Kundenseite besteht darin, ob der Outsourcing-Anbieter angemessene Sicherheitskontrollen anwendet, um die Datenvertraulichkeit, -integrität und -verfügbarkeit sicherstellen zu können. Darauffolgend ist die Sorge, ob der Partner die eigenen Sicherheitsrichtlinien, -standards und -prozesse einhalten kann. An dritter Stelle liegt die Angst, dass der Outsourcing-Partner die geschützten Informationen und das Wissen des Kunden missbrauchen könnte. Basierend auf dieser Analyse konnten drei notwendige Kernkompetenzen des Lieferanten aufgestellt werden: die allgemeine technologische Kompetenz des Lieferanten, die Einhaltung von Richtlinien und Vorschriften sowie die vorhandenen Kontrollen für den Informationsschutz.

Gonzales [27] beschäftige sich in seiner Arbeit mit den Gründen, warum Unternehmen IT-Themen auslagern. Dazu wurden die 5000 größten spanischen Unternehmen mit einem Fragebogen kontaktiert.

Basierend auf 398 gültigen Rückmeldungen konnte eruiert werden, warum Unternehmen sich dafür entscheiden, IT-Aktivitäten auszulagern. Der entscheidendste Punkt ist der Fokus auf strategisch relevante Themen beziehungsweise werden im Umkehrschluss strategisch weniger relevante IT-Aktivitäten ausgelagert. Die weiteren Punkte sind die Erhöhung der Flexibilität in der IT-Abteilung und eine erwartete verbesserte Qualität der ausgelagerten Dienste. Außerdem wurden auch hier die Outsourcing-Risiken der Studienteilnehmer erfragt. Laut spanischen Unternehmen sind die die Top-Risiken: eine mögliche unzureichende Qualifikation des Personals des Dienstleisters, eine übermäßige Abhängigkeit vom Dienstleister, die Nichteinhaltung des Vertrags und der Wissensverlust auf Grund der Auslagerung.

Wie relevant und real Informationssicherheitsrisiken durch Dritte sind, beschreibt Malatesta [24] durch die Aufarbeitung von Vorfällen und Statistiken in diesem Bereich. So lässt sich auch die Datenpanne der Fima Target – zweitgrößter Discounteinzelhandel nach Walmart in Amerika – im Jahr 2013 auf einen Lieferanten zurückführen. Durch ein kleines Partnerunternehmen für Heizungs- und Klimatechnik konnten Angreifer bei Target einsteigen und rund 110 Millionen Kundendatensätze stehlen. Nach Angaben von Target belaufen sich die Kosten für den Umgang mit der Datenpanne auf insgesamt 200 Millionen US-Dollar. Laut Malatesta ist es nicht das Problem, dass Unternehmen ihre Lieferanten überhaupt nicht überprüfen, sondern dass in diesem Bereich schlichtweg zu wenig getan wird. So haben bereits 2015 95% der Banken in New York angegeben, zumindest ihre risikoreichen Lieferanten einer spezifischen Risikobewertung für Informationssicherheit zu unterziehen. Der Fokus liegt dabei meist auf Bewertungen, bei denen verpflichtende Auflagen, wie etwa die Benachrichtigung in Falle einer Datenpanne, fehlen. Auch in einem *Forbes* Artikel mit dem Titel „Cybersecurity Domino Effect“ wird die Relevanz beschrieben: „Wir können uns nicht mehr nur um die Netzwerksicherheit unseres eigenen Unternehmens kümmern, weil so viele Netzwerke miteinander verbunden und voneinander abhängig sind. Eine Sicherheitslücke in einem Netzwerk kann sich leicht auf jedes Unternehmen in einer Lieferkette auswirken. Tatsächlich sind wir vielleicht nur so sicher wie der am wenigsten sichere Partner, mit dem wir verbunden sind.“ [28]

Pompon [29] liefert in seinem Buch „IT Security Risk Control Management“ einen sehr praxisnahen Leitfaden zur Risikobewertung von Dritten und dadurch einen wichtigen Input für diese Arbeit. Die wesentliche Herausforderung bei der Bewertung ist laut Pompon der fehlende direkte Zugriff auf die dafür notwendigen Informationen des Dritten. Die Tiefe der Bewertung sollte von den möglichen Auswirkungen eines Sicherheitsversagens beim Lieferanten abhängig gemacht werden. So gilt es, Dritte mit direktem Zugriff auf eigene Systeme einer gründlichen und ausführlichen Analyse zu unterziehen. Derartige Analysen sind bereits bei Vertragsabschluss beziehungsweise der Anbindung zu durchlaufen und danach auch periodisch zu wiederholen. Die häufigste Form der Risikobewertung ist die Gap-Analyse der vorhandenen Maßnahmen, oftmals in Form eines „Self-Assessments“. Um möglichst effizient zu sein, sollte die Analyse an den entsprechenden Fall angepasst werden, folglich ist es wenig sinnvoll, den Dienstleister für Aktenvernichtung auf Softwareentwicklungssicherheit zu überprüfen. Eine weitere Möglichkeit ist die Sichtung bestehender unabhängiger Audit-Reports des Lieferanten. Basierend auf der Analyse kann das Unternehmen die Zusammenarbeit mit dem Lieferanten stoppen (Risikovermeidung), so weitermachen wie zuvor (Risikoakzeptanz) oder das Risiko steuern und zusätzliche Maßnahmen einsetzen.

Tondel et al. [22] befragten Versicherungsunternehmen mit Cyberversicherungen im Produktportfolio. Als Grundlage für das Angebot von Versicherungspolizzen und die Tarifberechnung müssen Cyberversicherer das Risiko von potenziellen Kundenunternehmen einschätzen. Auch sie verfügen über nur begrenzte historische Daten und Vorfälle, die zu einer Auszahlung geführt haben. Die Studie wurde 2015 im nordischen Versicherungsmarkt durchgeführt. Es wurde dabei festgestellt, dass die Versicherer sehr ähnliche Ansätze und auch Herausforderungen haben, um das Risiko der Kunden einzuschätzen. Die primären Herausforderungen lauten wie folgt: fehlende standardisierte Metriken zur Messung des Cyberrisikos, fehlender Zugriff auf die für die Einschätzung notwendigen Daten sowie die effiziente Risikoeinschätzung und die sich ständig ändernde Risikosituation. Das konkrete Vorgehen zur

Risikobewertung der Cyberversicherer wird durch die Studie nicht offenlegt. Jedoch dürfte die ISO/IEC 27001 [30] eine wesentliche Rolle spielen.

Colicchia et al. [5] untersuchten, welche Ansätze die Unternehmen zur Steuerung der Cyberrisiken in der Supply Chain verfolgen. Es wurden dazu in einer qualitativen Fallstudie fünf multinationale Unternehmen mit Hauptsitz oder Standort in UK befragt. Darüber hinaus wurde eine strukturierte Literaturanalyse durchgeführt, um den aktuellen Stand der Forschung im Bereich Cyber-Supply-Chain-Risk-Management (CSCRM) zu erheben. Es wird dabei festgehalten, dass, obwohl die Bedeutung der Thematik in der Literatur des Supply Chain Managements anerkannt ist, sie noch nicht umfassend erforscht wurde (2018). Außerdem wird festgestellt, dass es noch keinen holistischen und kohärenten Ansatz zur Steuerung der IT-Sicherheitsrisiken in der Supply Chain gibt. Die durchgeführte fallübergreifende Analyse zeigt, dass die Unternehmen der Stichprobe keinen einheitlichen CSCRM-Ansatz verfolgen, sondern eine Mischung aus reaktiven und proaktiven Ansätzen zu erkennen ist. Die dafür eingesetzten Instrumente sind Risikoabschätzungen, Szenarioanalysen, Krisenpläne beziehungsweise Business-Continuity-Pläne. Überdies wird durch die Studie ersichtlich, dass sich die Unternehmen sehr darauf konzentrieren, sich selbst abzuschirmen, und weniger einen generellen Schutz vor Cyber- und Informationsrisiken für die gesamte Supply Chain anstreben.

Auch Ghadge et al. [9] publizieren eine Studie zur Untersuchung des Cyber-Risk-Managements in der Supply Chain (2019). Durch eine systematische Literaturanalyse wurden Arbeiten zwischen 1990 und 2017 mit Hilfe von Data-Mining-Techniken überprüft. Bei den meisten Forschungsarbeiten kommen qualitative Forschungsmethoden zum Einsatz. Dies wiederum ist im akademischen Bereich ein Indikator für eine Unreife des Fachgebiets und einen fehlenden Konsens. Etwa die Hälfte aller Arbeiten stammen aus den USA oder UK. Dies erklärt man sich vor allem mit den staatlichen Bemühungen rund um das Thema Cybersicherheit. So haben die USA und UK bereits lange vor 2010 eine Nationale-Cybersicherheitsstrategie präsentiert, europäische Länder hingegen erst ab 2011.

Papastergiou et al. [31] präsentieren in der Arbeit eine faktengestützte Supply-Chain-Risk-Assessment-Methode, die durch ein Forschungsprojekt der EU mit mehr als 3 Millionen Euro unterstützt wurde. Die erarbeitete Methode namens MITIGATE zielt darauf ab, Cyberrisiken eines jeden Supply-Chain-Services abzuschätzen und vorherzusagen. Die Ziele des Projekts sind: Identifizierung und Messung aller Cyber-Bedrohungen innerhalb der Supply Chain, Bewertung der individuellen, kumulativen und sich ausbreitenden Schwachstellen, Vorhersage aller möglichen Angriffs-/Bedrohungspfade und -muster innerhalb des Systems, Bewertung der möglichen Auswirkungen, Ableitung und Priorisierung der entsprechenden Cyber-Risiken und Formulierung einer geeigneten Strategie zur Schadensbegrenzung. Die daraus erarbeitete Methode besteht aus sechs Phasen mit jeweils mehreren Unterphasen. Die Hauptphasen lauten wie folgt: Festlegen der Grenzen, Cyber-Bedrohungs-Analyse, Schwachstellenanalyse, Auswirkungsanalyse, Risikoabschätzung und Risikobehandlung.

In der Arbeit von Polemi et al. [32] wird der sogenannte Medusa-Ansatz zur Risikobewertung in der Supply-Chain beschrieben. Es handelt sich dabei um einen Vorläufer der soeben beschriebenen MITIGATE-Methode. Das beschriebene Vorgehen ist im Ablauf ähnlich, wobei versucht wird, den Anforderungen des ISO 28001 Standards nachzukommen. In diesem wird ein generisches Managementsystem für die Supply-Chain-Sicherheit beschrieben.

Boyens et al. [4] behaupten in Ihrer Publikation, dass eine Lieferantenbewertung, die vor Vertragsabschluss durchgeführt wird, nur eine Momentaufnahme ist, die zum Abschluss bereits wieder veraltet ist. Bei der Arbeit handelt es sich um eine Fallstudie des National Institute of Standards and Technology (NIST). Darin wird angemerkt, dass fortgeschrittene Unternehmen auf Programme setzen, die den gesamten Lebenszyklus der Lieferantenbeziehung abdecken und eine Vielzahl an Risiken überwachen. Unternehmen setzen hierbei eine Vielzahl an Lieferantenbewertungen und -überwachungen

ein. Unter anderem kommen Self-Assessments, Lieferantenzertifizierungen, Dritt-Bewertungen, offizielle Zertifizierungen und vor Ort Besuche zum Einsatz. Dabei wird auch auf „Shared Assessments“ verwiesen, um eine Flut von Bewertungsfragebögen auf Lieferantenseite zu vermeiden. Die Lieferanten können hierbei die Antworten für andere Kunden wiederverwenden, wodurch ein effizienterer Prozess geschaffen wird. Darüber hinaus gibt es mehrere Risk-Rating-Plattformen, die für einen zusätzlichen Blickwinkel auf den Lieferanten verwendet werden können.

Keskin et al. [14] untersuchen in ihrer Studie die bestehenden Methoden für Cyber-Third-Party-Risk-Management (C-TPRM) erarbeitet durch unterschiedliche Privatunternehmen. Es handelt sich dabei um nicht-invasive Risikobewertungsplattformen, die durch öffentlich verfügbare Informationen versuchen, das Cyberrisiko von Unternehmen einzuschätzen. Für die Studie wurde eine US-Hochschule von vier verschiedenen Unternehmen, die einen derartigen Risk-Rating-Dienst anbieten, bewertet und die Ergebnisse verglichen. Bei den verwendeten Produkten handelt es sich um FICO, BitSight, RiskRecon und ComplyScore. Als grundlegende Erkenntnis wird festgestellt, dass es erhebliche Unterschiede beim Bewertungsergebnis durch die unterschiedlichen Produkte gibt. So liegt der Bewertungsscore der als Beispiel verwendeten US-Hochschule je Produkt in besten Fall bei 80 %, in schlechtesten Fall bei 57 %. Diese Abweichungen deuten darauf hin, dass unterschiedliche Bewertungsmethoden sowie proprietäre Datensätze verwendet werden.

Viega [6] macht in seiner Publikation auf die Nachteile und Schwächen von Fragenbögen beziehungsweise Self-Assessments aufmerksam. Die damit erzeugte Selbsteinschätzung stimmt laut Viega oftmals nicht mit der Realität überein, wodurch für Lieferanten und Dritte eine falsche Risikoeinstufung erfolgt. Viega geht sogar so weit, zu behaupten, dass es Dritte gibt, welche im Self-Assessment bewusst lügen.

Im Kurzartikel von Sotnikov [33] werden mögliche Methoden zur Beurteilung Dritter dargelegt, ohne jedoch Detailumsetzungen zu nennen. Die aufgestellten Methoden beziehen sich auf eine Risikobeurteilung angelehnt an bekannte Industriestandards, die Durchführung einer Due-Diligence und das ständige Überwachen aller Dritten. Außerdem stellt Sotnikov fest, dass jene Dritte, die sensible Daten verarbeiten, mit konkreten und risikobasierten Anforderungen konfrontiert und diese auch vertraglich festgehalten werden sollten.

2.1.3. Ausgewählte wissenschaftliche Arbeiten

Folgend finden sich jene wissenschaftlichen Arbeiten, die nicht in die Kategorisierung des Literatureinblicks von 2.1.2 fallen. Denn die Arbeiten beziehen sich nur indirekt auf die Identifikation und Bewertung von Third-Party Risiken (TP-Risiken). Gerade deshalb liefern die Arbeiten wichtige TPRM-Erkenntnisse, wodurch sie eine hohe Relevanz darstellen und somit auch in diesem eigenen Abschnitt zusammengefasst werden.

Der Wissenschaftler Michel Benaroch setzt sich in seiner Arbeit [34] mit Cybersicherheits-Risiken in Zusammenhang mit IT-Outsourcing auseinander. Michel Benaroch wurde von Information-System-Journals (MISQ[6], ISR[7], JMIS[8] und JAIS[9]) in der Zeit von 1999-2011 als einer der Top-100-Forscher weltweit eingestuft. In dieser im Jahr 2020 veröffentlichten Publikation stellte er fest, dass das marktbasierte Vertrauen bei der Entscheidung über die Auswahl eines IT-Outsourcing-Partners eine führende Rolle spielt. Beim marktbasierten Vertrauen handelt es sich um Cybersicherheitszertifizierungen und deren direkten Einfluss auf den Markt. So steigert eine Zertifizierung das Vertrauen in einen Partner, was sich wiederum für diesen positiv auf seine Marktpräsenz auswirkt. Im Gegenzug werden Unternehmen, die eine

[6] MISQ - Management Information Systems Quarterly
[7] ISR - Information Systems Research
[8] JMIS - Journal of Management Information Systems
[9] JAIS - Journal of the Association for Information Systems

Cybersicherheitszertifizierung nicht vorweisen können, am offenen Markt mit fehlendem Vertrauen bestraft. In der Publikation werden zwei weitere Entscheidungsbetrachtungen von IT-Outsourcing-Partnern vorgestellt: theoretische Betrachtung und transparente Betrachtung. Bei der theoretischen Betrachtung handelt es sich um eine Risikokalkulation, die aber auf Grund notwendiger Daten für IT-Outsourcing-Kunden nur schwierig umzusetzen ist. Wie der Name bereits sagt, wird bei der transparenten Betrachtung versucht einen direkten Einblick in die Arbeitsweise des IT-Outsourcing-Partners zu erhalten. Es wird dabei auch auf weitere Partner in zweiter, dritter oder vierter Ebene in der Supply Chain hingewiesen. Auch für diese Betrachtung werden viele Herausforderungen in der Praxistauglichkeit geortet.
Des Weiteren wird in der Arbeit auf das sich durch Outsourcing ändernde Risikoprofil eines Unternehmens hingewiesen. So ändert sich dieses hin zu einer Kombination aus eigenen Risken und einer Teilmenge der Risiken des IT-Outsourcing Partners. Dieses erweiterte Risiko wird mit Studien wie jener von Vasishta et al. [35] unterstrichen. Diese zeigt, dass mehr als 30% der Datenschutzpannen im Gesundheitswesen bei ausgelagerten IT-Partnern stattfanden.
Benarochs Aufarbeitung bestehender Literatur unterstreicht einerseits das zusätzliche Risiko, das sich durch Auslagerung von IT an Dritte ergibt, sowie andererseits die Relevanz von internationalen Cybersicherheitszertifizierungen und -standards wie SOC1/2[10], ISO 27001 oder NIST SP 800-53, in Zusammenhang mit IT-Outsourcing. [34]

Die 2016 veröffentliche Publikation [36] von John Haller und Charles M. Wallen beleuchtet den Umgang mit Risiken Dritter im Finanzdienstleistungsbereich. Dabei steht die Frage „Wie können Finanzdienstleistungsunternehmen die Risiken Dritter abhängig vom Risikoniveau und der Geschäftsbeziehung steuern?“.
Zunächst wird darauf hingewiesen, dass Third-Party Risk Management (TPRM) schnell unübersichtlich und auch komplex werden kann. Dieses Problem ergibt sich für Unternehmen aller Größenordnungen. Kleine Unternehmen haben womöglich Schwierigkeiten, ausreichende Informationen großer Anbieter zu erhalten oder intern die notwendigen Ressourcen bereitzustellen. Große Unternehmen hingegen müssen oftmals hunderte Geschäftsbeziehungen überblicken und steuern. Als Kernprobleme werden die Identifizierung kritischer Dritter sowie die Einstufung der Kritikalität genannt. Zusätzlich zeigt die Arbeit auf, dass es sich bei TPRM nicht um eine einmalige Angelegenheit handelt, stattdessen vielmehr um einen ständigen Kreislauf, denn sämtliche Aktivitäten müssen periodisch wiederholt werden. Es gilt daher, die Liste der Dritten sowie deren Risikobewertung aktuell zu halten. Eine weitere Herausforderung, die die Autoren hervorheben, ist die notwendige Integration von TPRM in bestehende Unternehmensprozesse und -abteilungen. Demzufolge ist beispielsweise die Beschaffungsabteilung miteinzubeziehen und Cybersicherheitsanforderungen in Vertragsklauseln mitaufzunehmen.
Vor allem Finanzdienstleister sind im Bereich TPRM gefordert, denn sie sind ein attraktives Ziel für Cyberangriffe, setzen oftmals in großen Umfang auf Dritte und sind von mehreren Regularien betroffen. Hier machen Haller und Wallen klar, was die Finanzindustrie benötigt: „einen systematischen Ansatz, der für Konsistenz, Effizienz sowie Vorhersehbarkeit bei der Bewertung und Steuerung von Drittparteirisiken sorgt“[11]. Dabei wird ein allgemeiner und industrieübergreifender Ansatz für TPRM gefordert, der zumindest ein Basisrahmenwerk vorgibt. Andersfalls werden Unternehmen verschiedene Richtungen einschlagen, was hingegen eine Zusammenarbeit zwischen den Parteien wie Geschäftspartnern, Interessensgruppen und Regulatoren erschwert und in Summe ineffizienter gestaltet.
Die Arbeit beschreibt im Allgemeinen, wie die Widerstandsfähigkeit eines Unternehmens hinsichtlich Third-Party-Risiken verbessert werden kann. So wird hervorgehoben, dass TPRM im gesamten Unternehmen stattfinden muss und hierbei auch Verantwortungen geteilt werden. Im Anhang 1 liefert die Publikation eine Übersicht der Aktivitäten zur Verbesserung des TPRM in einem Unternehmen – folgend ein Auszug:

- Aktuelles TPRM anhand eines Standards beurteilen, um Verbesserungen zu identifizieren

[10] SOC - System and Organization Controls
[11] What the financial industry needs is a systematic approach that provides consistency, efficiency, and predictability in assessing and managing third party risk. [34]

- Sicherstellen, dass Anforderungen an Dritte vertraglich geregelt sind
- Sicherstellen, dass relevante Stellen miteinander kommunizieren (Lieferantenmanagement, Sicherheit, IT, …)
- …

Haller und Wallen weisen durch die Publikation auf die Risiken beim Outsourcing hin, vor allem auf die Schwierigkeit, diese zu steuern. Dabei wird speziell auf die Priorität und Herausforderungen im Finanzdienstleistungsbereich eingegangen. Diese sind durch die Verwaltung von Zahlungen, dem ständigen Drang nach Innovationen wie auch der zahlreichen Regularien besonders gefordert im Umgang mit Drittanbieter. [36]

2.1.4. Literaturüberblick

Author et al.	Jahr	Forschungs-methode	Forschungs-konzept	Literatur-übersicht	TP Vorfälle inkl. Detail-beschreibung	Methoden: Identifikation von TP-Risiken	Methoden: Beurteilung von TP-Risiken	TP Risiko-kategorien	Fokus
Aubert	1998	Quali.	Concept	nein	nein	**ja**	**ja**	ja	Risikomangement bei IT-Outsourcing
Charney	2011	Quali.	Concept	nein	nein	**nein**	**nein**	nein	Grundsätze zur Unterstützung von Regierungen, um Cyber Supply Chain Risiken zu adressieren - Fokus auf manipulierte Produkte
Boyson	2014	Quali.	Survey	nein	ja	**nein**	**nein**	nein	Reifegradmodell für das Cyber Supply Chain Risk Management
Windelberg	2015	Quali.	Concept	nein	nein	**nein**	**nein**	nein	Ziele für eine sichere Supply Chain von Cyberprodukten wie Hardware, Software und Dienste
Polemi	2015	Quali.	Concept	nein	nein	**ja**	**ja**	ja	Supply Chain Security Risk Assessment compliant mit ISO 28001, Nachfolger von CYSM aber Vorläufer von MITIGATE (ID 9)
Haller	2016	Quali.	Concept	nein	nein	**nein**	**nein**	nein	Herausforderung Third Party Risk Management in der Finanzindustrie
Dhillon	2016	Mix	Delphi Study	nein	nein	**nein**	**nein**	ja	Informationssicherheitsaspekte beim IT-Outsourcing - Kunden- und Lieferantensicht
Tondel	2016	Quali.	Review, Interview	nein	nein	**ja**	**ja**	nein	Risikobewertung aus Sicht von Cyberversicherern
Pompon	2016	Quali.	Concept	nein	nein	**ja**	**ja**	ja	Praxisorientierter Leitfaden zur Risikobeurteilung von Third-Parties
Malatesta	2016	Quali.	Concept	nein	ja	**ja**	**ja**	nein	Relevanz von Informationssicherheitsrisiken durch Lieferanten sowie ein möglicher Umgang mit diesen
Sunderkrishnan	2016	Quali.	Concept	nein	nein	**nein**	**nein**	nein	Risikobewertung von Lieferanten mit generischen Ansätzen aber kaum IT-Bezug
Gonzales	2016	Mix	Interview	nein	nein	**nein**	**nein**	ja	Umfrage in Spanien zu IT-Outsourcing Gründe und IT-Outsourcing Risiken
Bhatti	2017	Quali.	Concept	ja	nein	**nein**	**nein**	nein	Unterstreicht das limitierte Wissen zu Informationssicherheitsrisikomanagement bei IT-Outsourcing
Papastergiou	2018	Quali.	Concept	nein	nein	**nein**	**ja**	nein	Methode zur Erhebung des Cyber-Risikos eines Supply Chain Services
Almutairi	2018	Quali.	Concept	nein	nein	**nein**	**nein**	nein	PDCA Modell zur Steuerung von Risiken bei IT-Outsourcing Projekten
Colicchia	2018	Quali.	Case Study	ja	nein	**nein**	**nein**	ja	Erforschung der Ansätze in Unternehmen für das Steuern von Cyberrisiken in der Supply Chain
Ghadge	2019	Quant.	Review, Concept	ja	nein	**nein**	**nein**	ja	Systematische Literatursuche zu Cyber-Risiken in der Supply Chain
Sotnikov	2019	-	Webarticle	nein	nein	**nein**	**ja**	nein	Einfacher Überblick zu Third Party Risk Management
Dobrec	2019	-	Webarticle	nein	nein	**nein**	**nein**	nein	Einfacher Überblick zu Third Party Risk Management
Pandey	2020	Quali.	Concept	nein	ja	**nein**	**nein**	ja	Kategorisierung von Cyber-Risiken in der Supply Chain

Author et al.	Jahr	Forschungs-methode	Forschungs-konzept	Literatur-übersicht	TP Vorfälle inkl. Detail-beschreibung	Methoden: Identifikation von TP-Risiken	Methoden: Beurteilung von TP-Risiken	TP Risiko-kategorien	Fokus
Benaroch	2020	Quali.	Concept	nein	nein	**nein**	**nein**	nein	Vertrauen in einen IT-Outsourcing Partner durch Zertifizierungen
Viega	2021	Quali.	Review	nein	nein	**ja**	**nein**	nein	Nachteile und Schwächen von Self-Assessments
Santos	2021	Quali.	Concept	nein	nein	**nein**	**nein**	nein	Metriken in der Informationssicherheit
VanHoy	2021	Quali.	Concept	nein	nein	**nein**	**nein**	nein	Wichtigkeit von Third Party Risk Management
Keskin	2021	Quali.	Exploratory analysis	ja	ja	**ja**	**ja**	nein	Vergleich von Tools zur quantitativen Cyber Third-Party Risikobewertung
Creazza	2021	Mix	Review, Interview	ja	nein	**nein**	**nein**	nein	Befragung von Unternehmen rund um Cyber Supply Chain Risikomanagement und deren relevante Elemente
Boyens	2021	Quali.	Survey	nein	nein	**ja**	**nein**	nein	Beobachtete Praktiken im Bereich Cyber Supply Chain Risk Management

Tabelle 3: Literaturüberblick zu Third-Party Risk Management in der IT

Der Literaturüberblick listet die 27 relevantesten Arbeiten in chronologischer Reihenfolge. Dabei werden die für diese Arbeit wesentlichen Kriterien festgehalten und der Fokus jeder Arbeit kurz beschrieben. So ist direkt erkennbar, welche Arbeiten eine Literaturübersicht liefern, vergangene Sicherheitsvorfälle in Zusammenhang mit Third-Parties aufzeigen, Methoden zur Identifikation oder Bewertung von Third-Parties vorschlagen oder versuchen, Third-Party-Risiken zu kategorisieren.

2.2. Third-Party Risk Management Frameworks

TPRM-Frameworks bieten einen organisierten Ansatz zur Risikominderung. Sie bieten die notwendige Struktur für die Umsetzung sowie die interne Prüfung dieser Tätigkeiten. Unternehmen können diese Frameworks als Leitfaden verwenden, um eine sorgfältige Prüfung von Dritten zu gewährleisten. „Die Wahl eines TPRM-Frameworks hängt von der Unternehmensstruktur, dem Risikoprofil, der Risikobereitschaft, der Geschäftstätigkeit, der Unternehmensgröße und der Standorte ab.“ [2]

In Folge werden die bekanntesten TPRM-Frameworks einerseits überblicksmäßig dargestellt, andererseits werden die Frameworks hinsichtlich der Beantwortung der Forschungsfrage konkret beleuchtet und die dafür wichtigen Informationen extrahiert.

2.2.1. ISO/IEC 27036

Die ISO/IEC 27036 [37] mit der Bezeichnung *Information technology — Security techniques — Information security for supplier relationships* setzt sich aus vier Teilen zusammen:

- Teil 1: Überblick und Konzepte
- Teil 2: Anforderungen
- Teil 3: Leitlinien für die Sicherheit der Informations- und Kommunikationstechnologie Lieferkette
- Teil 4: Leitlinien für die Sicherheit von Cloud-Diensten

ISO/IEC 27036-1– Überblick und Konzepte [37]

Die Norm umfasst jede Lieferantenbeziehung, die Auswirkungen auf die Informationssicherheit haben kann. Des Weiteren wird darauf hingewiesen, dass sowohl Lieferant als auch Erwerber gleichermaßen für eine angemessene Steuerung der Informationssicherheitsrisiken zuständig sind. Neben den Motiven für eine Lieferantenbeziehung wird in der Norm versucht, die Supply Chain - wie in Abbildung 3 zu sehen - grafisch darzustellen.

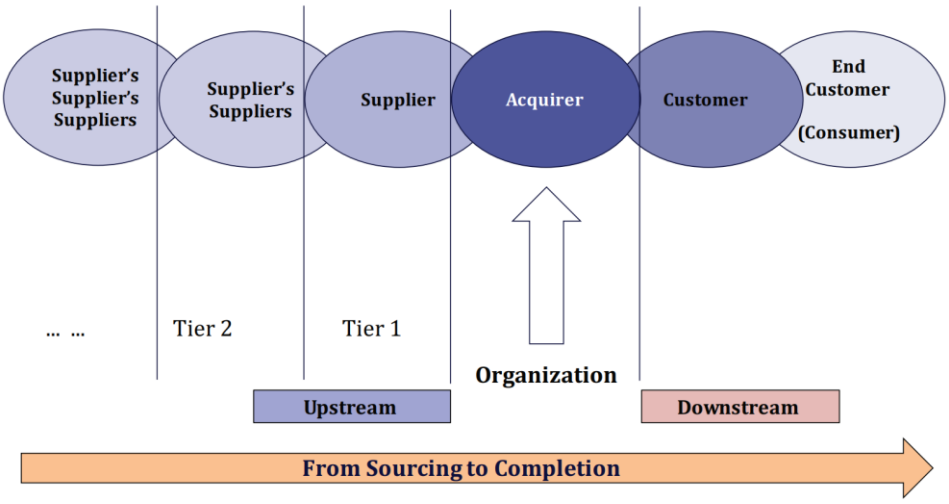

Abbildung 3: Supply Chain Beziehungen laut ISO/IEC 27036 [37]

Die Norm teilt die Risiken in zwei Gruppen: in diejenigen, die beim Erwerb eines Produktes gegeben sind, und diejenigen, die beim Erwerb einer Dienstleistung gegeben sind. Dazu werden auch einige Beispiele genannt:

Produktrisiko	Informationssicherheit	Sofern das gelieferte Produkt Schwachstellen aufweist, sind auch die vom Erwerber abgeleiteten Produkte verwundbar.
Produktrisiko	Qualität	Schlechte Qualität der gelieferten Produkte kann zu Schwächen in der Informationssicherheit der abgeleiteten Produkte führen.
Dienstleistungs-risiko	Physischer vor-Ort Zugriff	Risiko durch den physischen Zugriff auf Systeme des Erwerbers.
Dienstleistungs-risiko	Zugriff auf Informationen und Systeme	Risiko durch Lieferanten vor Ort mit logischem Zugriff auf Informationen und Systeme des Erwerbers.
Dienstleistungs-risiko	Fernzugriff auf interne Informationen und Systeme	Risiko durch den Fernzugriff des Lieferanten auf Informationen und Systeme des Erwerbers.

Tabelle 4: Lieferantenrisiken - Beispiele aus der ISO/IEC 27036 [37]

Unter anderem wird in der Norm die Steuerung von Informationssicherheitsrisiken beschrieben, wobei auch hier nur sehr generisch formuliert wird: „[…] um diese Informationssicherheitsrisiken zu identifizieren und zu managen, sollte der Erwerber die Zusicherung erhalten, dass der Lieferant ein angemessenes Informationssicherheitsmanagement und entsprechende Kontrollen eingeführt hat.“ [37] Für den eigenen Absatz der Informations- und Kommunikationstechnik (IKT) Lieferkette wird Erwerbern zur Einführung eines Frameworks geraten, ohne jedoch ein konkretes Framework zu nennen.

ISO/IEC 27036-2 – Anforderungen

Der ISO/IEC 27036 Teil 2 [38] stellt die Anforderungen an ein Framework für die Informationssicherheit mit Lieferanten in den Fokus. Dieser Teil kann von Erwerbern verwendet werden, um Lieferantenverträge zu definieren, zu verwalten und zu überwachen. Dabei wird im Absatz „Risk management process“ auch auf die Aktivitäten näher eingegangen. Das bereits im Teil eins empfohlene Framework wird hier konkretisiert und dabei auf verwandte Risikomanagement-Normen verwiesen: ISO/IEC 27005, ISO 31000 und ISO/IEC 15288.

Folgende Elemente können laut Teil zwei für die Erhebung des Reifegrads des Lieferanten relevant sein (Absatz 6.1.1.2):

- Bisherige sicherheitsbezogene Performance des Lieferanten
- Nachweise über das pro-aktive Management der Informationssicherheit (etwa in Form einer ISO 27001 Zertifizierung, die das zu erwerbende Produkt inkludiert)
- Nachweise über dokumentierte und getestete Krisen- und Notfallpläne

Nachfolgend die weiteren zu beachtenden Punkte hinsichtlich der Bewertung von Lieferanten:

- Definition der Art der Bewertung, wie etwa ein Self-Assessment oder eine unabhängige Bewertung durch Dritte
- Definition des Detailierungsgrad der Bewertung und die Häufigkeit ihrer Durchführung
- Eine den zu beschaffenden Produkten oder Dienstleistungen angemessene Bewertungsmethode
- Berücksichtigung rechtlicher und behördlicher Auflagen, die sich durch den Kauf ergeben
- Miteinbeziehung anderer Geschäftsbereiche in Bezug auf die Risikobewertung

2.2.2. NIST SP 800-161

Das *National Institute of Standard and Technology (NIST)* stellt die Publikation mit dem Titel *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* [11] frei zur Verfügung.

Für diese Arbeit wird die unter dem Kürzel NIST SP 800-161 [11] *geführte Publikation mit dem Zeitstempel Oktober 2021 verwendet.*

Die Veröffentlichung soll Unternehmen einen Leitfaden bieten, um Cybersicherheitsrisiken in der Supply Chain zu identifizieren, zu bewerten und zu mindern. Es wird der Ansatz verfolgt, das Cybersecurity Supply Chain Risk Management (C-SCRM) in die unternehmensweiten Risikomanagement-Aktivitäten zu integrieren. Die Publikation ist folgendermaßen strukturiert:

- Einleitung (Zweck, Zielgruppe, Hintergrund und Verbindung zu anderen Publikationen)
- Integration von C-SCRM in das unternehmensweite Risikomanagement
- Kritische Erfolgsfaktoren
- Anhänge wie Sicherheitskontrollen, Risikobewertungsprozess und Vorlagen

Das Dokument ist 338 Seiten stark, wodurch auf der einen Seite die ausführliche Behandlung der Thematik unterstrichen wird, auf der anderen Seite aber auch die Schwierigkeit erkennbar wird, den Ansatz zu erfassen und danach in den eigenen Kontext umzulegen. Im Vergleich umfasst die ISO/IEC 27036 66 Seiten (Teil eins und Teil zwei).

NIST SP 800-161: Überblick und Konzepte [11]

Das Dokument weist klar darauf hin, dass es sich beim präsentierten C-SCRM Leitfaden um keine „one-size-fits-all“ Lösung handelt, sondern diese an die Unternehmensgröße, verfügbare Ressourcen sowie die Risikoumstände anzupassen ist. Auch die NIST hebt klar die Komplexität der Thematik hervor, denn Unternehmen haben meist eine Vielzahl von Beziehungen zu ihren Lieferanten, Entwicklern, externen Systemdienstleistern oder anderen IT-Dienstleistern. In Abbildung 4 versucht sie - ähnlich zur ISO/IEC - auch die NIST an einer Darstellung der Supply Chain aus Erwerbersicht.

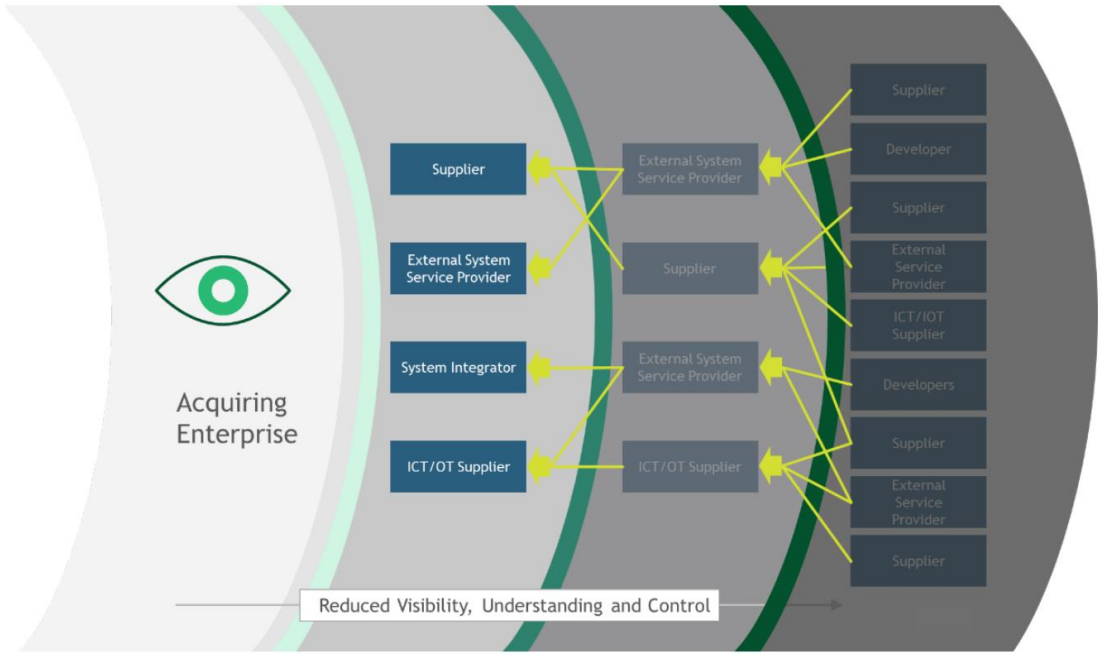

Abbildung 4: Supply Chain Betrachtung nach NIST SP 800-161 [11]

Eine weitere parallele zur ISO/IEC 27036 ergibt sich bei der Aufstellung von Beispielen für Cyberrisiken in der Supply Chain. So werden hier gefälschte oder manipulierte Produkte, der Diebstahl von geistigem Eigentum durch Insider oder das Einschleusen von Schadsoftware durch Dritte als Beispiele angeführt. Darüber hinaus wird eine Einordnung dieser Risiken grafisch dargestellt. Wie in der Abbildung 5 ersichtlich entstehen Risiken dann, wenn Bedrohungen bestehende Schwachstellen in der Supply Chain ausnutzen. Einerseits wird zwischen feindlichen und nicht-feindlichen Bedrohungen unterschieden, andererseits unterscheidet das NIST zwischen externen und internen Schwachstellen. Daraus folgend stellt sich die Frage, mit welcher Wahrscheinlichkeit die Bedrohung die Schwachstelle ausnutzt und welche Auswirkungen dies zur Folge hat.

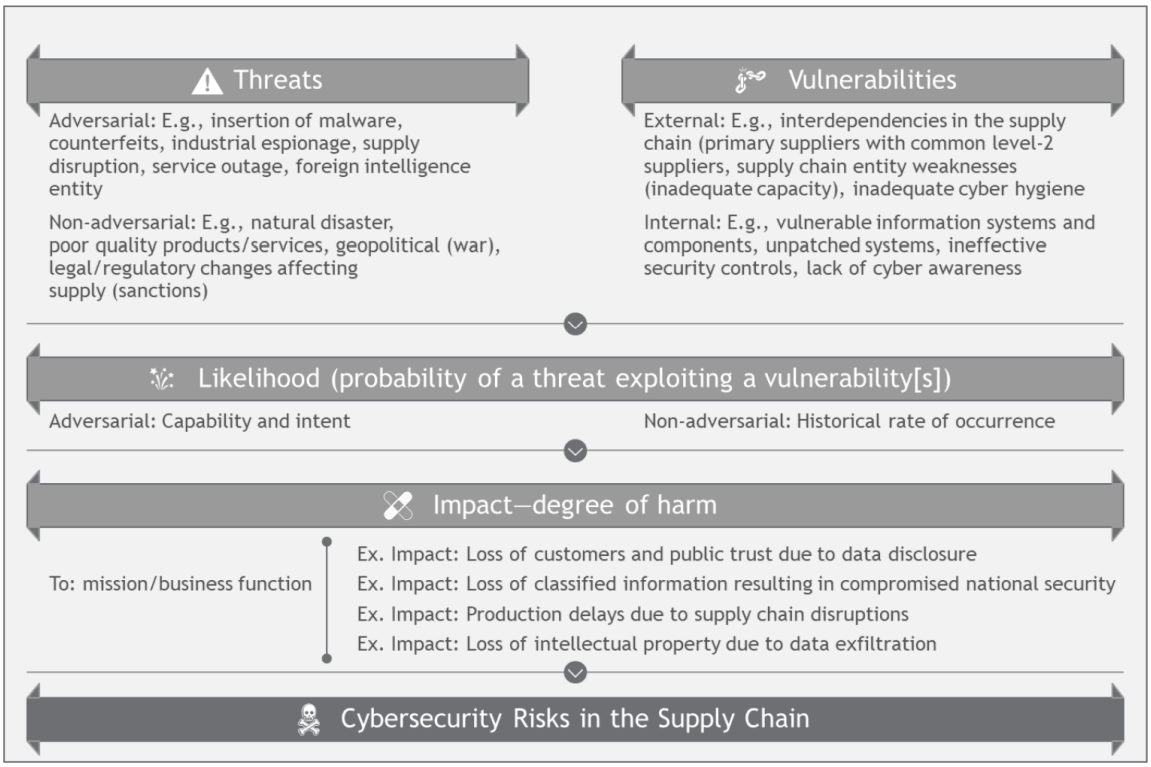

Abbildung 5: Cyberrisiken in der Supply Chain laut NIST SP 800-161 [11]

Die NIST SP 800-161 baut auf einer Vielzahl anderer NIST-Publikationen auf und stellt dabei immer wieder Querverweise her. Nichtsdestotrotz werden die grundlegenden Schritte für ein Third-Party Risk Management dargelegt – folgt eine verkürzte und vereinfachte Interpretation:

- Einführung eines Risikomanagementprozesses laut NIST SP 800-39 (Management von Informationssicherheitsrisiken) sowie eines Risikobewertungsprozess laut NIST SP 800-30 (Leitfaden zur Durchführung von Risikobewertungen)
- Schaffung von Governance, die C-SCRM in Unternehmensrichtlinien miteinbezieht
- **Einsatz eines Risikobewertungsprozesses, der die Analyse der Kritikalität, Bedrohungen und Schwachstellen umfasst**
- Implementierung der Basiskontrollen gemäß NIST SP 800-53
- Einsatz eines Vorfalls-Managements, das Sicherheitsvorfälle durch die Supply Chain miteinbezieht

NIST SP 800-161: Risiken identifizieren und bewerten

In diesem Absatz wird beleuchtet, welchen konkreten Input die NIST-Publikation für das Identifizieren und Bewerten von Third-Party Risiken liefert. Der Anhang G [11] beschreibt den C-SCRM-Prozess nach NIST, der von einem Unternehmen verlangt: (i) den Rahmen für das Risiko abzustecken (d.h. den Kontext für risikobasierte Entscheidungen zu schaffen), (ii) das Risiko zu bewerten, (iii) auf das ermittelte Risiko zu reagieren und (iv) das Risiko fortlaufend zu überwachen. Der beschriebene Prozess wird in Abbildung 6 dargestellt.

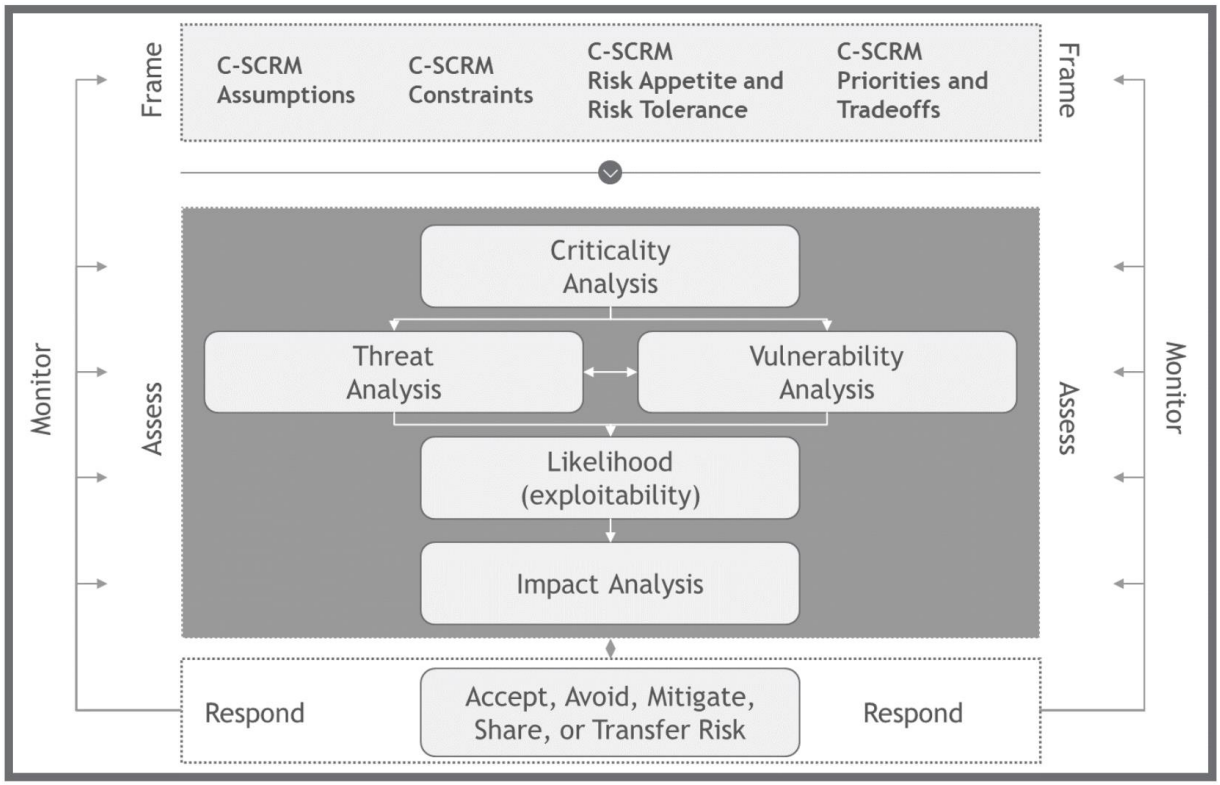

Abbildung 6: Cybersecurity Supply Chain Risiko Management (C-SCRM) nach NIST SP 800-161 [11]

In Folge wird die Phase der Beurteilung („Assess“) genauer betrachtet wie auch beschrieben, da hier eine hohe Relevanz zur Beantwortung der Forschungsfrage erachtet wird. Im Dokument wird diese Phase als „Supply Chain Cybersecurity Risk Assessment“, abgekürzt S-CSRA, bezeichnet. Die Schritte sind wie folgt:

- (Frame) Informationsbeschaffung & Scoping-Analyse
- Kritikalitätsanalyse
- Bedrohungsanalyse
- Schwachstellenanalyse
- Analyse der Auswirkungen
- Analyse der Risikoreaktion

Da das NIST in den folgenden beschriebenen Schritten zwischen Produkten, Dienstleistungen und Lieferanten nicht unterscheidet, wird zur Vereinfachung „Produkt“ als Abkürzung für „Produkte, Dienstleistungen und Lieferanten“ verwendet.

Informationsbeschaffung & Scoping-Analyse
In dieser Phase gilt es, grundlegende Informationen über das Produkt einzuholen. Es ist folglich wichtig, hier den Zweck und das Ziel zu definieren. Darüber hinaus sollte wie in Abbildung 7 eine Systembeschreibung und ein Architekturüberblick erstellt werden. [11]

Supply Chain Risk Management Assessment Scoping Questionnaire		
Section 1: Request Overview	Provide Response:	Response Provided by:
Requestor Name		Acquirer
S-CSRA Purpose and Objective		Acquirer
System Description		Acquirer
Architecture Overview		Acquirer
Boundary Definition		Acquirer
Date of Assessment		Acquirer
Assessor Name		Acquirer
Section 2: Product/Service Internal Risk Overview		
What is the suppliers market share for this particular product/service		Acquirer

Abbildung 7. Supply Chain Risk Management Assessment Scoping - Beispielfragebogen [11]

Kritikalitätsanalyse
In jedem Unternehmen existieren kritische Prozesse, deren Unterbrechung, Manipulation oder Ausfall zu einer Beeinträchtigung der Geschäftsziele führen würde. Derartige kritische Prozesse sind von unterschiedlichen kritischen Systemen, die wiederum auf kritische Komponente (Hardware, Software) angewiesen sind, abhängig. In der Kritikalitätsanalyse werden geschäftskritische Prozesse, zugehörige Systeme und Komponenten sowie unterstützende Dienste identifiziert. Dabei werden auch kritische Lieferanten erfasst – also jene Lieferanten, die durch Produkte oder Dienste einen geschäftskritischen Prozess unterstützen. [11]

Bedrohungsanalyse
In der Bedrohungsanalyse [11] soll festgestellt werden, welche Bedrohungsereignisse, potenzielle Bedrohungsakteure (Staaten, Cyberakteure) und Bedrohungsvektoren (Lieferant zweiter Ebene) sich für das Produkt ergeben. Das NIST stellt dazu folgende Bedrohungsstufen auf:

- Kritisch: Die Informationen deuten darauf hin, dass Angreifer das Produkt unterwandern, kompromittieren oder manipulieren.
- Hoch: Informationen deuten darauf hin, dass Angreifer eine offene oder geheime Beziehung zum Lieferanten aufgebaut haben, mit der Fähigkeit und der Absicht, die Supply Chain zu unterwandern, zu kompromittieren oder zu manipulieren; es gibt jedoch keine bekannten Hinweise auf Unterwanderung, Kompromittierung oder Manipulation.
- Mäßig: Die Informationen deuten darauf hin, dass Angreifer in der Lage sind, aber nicht die Absicht haben, das Produkt zu unterwandern, zu kompromittieren oder zu manipulieren. Umgekehrt haben sie möglicherweise die Absicht, aber nicht die Fähigkeit.
- Niedrig: Die Informationen deuten darauf hin, dass die Gegner weder die Fähigkeit noch die Absicht haben, das Produkt zu unterwandern, zu kompromittieren oder zu manipulieren.

Die Informationen zur Einstufung sollten aus der ersten Phase - der Informationsbeschaffung - zur Verfügung gestellt werden können.

Schwachstellenanalyse
Wie die Überschrift bereits vermuten lässt, werden bei dieser Analyse [11] Schwachstellen des Produkts erhoben und bewertet. Die Analyse sollte dabei berücksichtigen, wie leicht die Schwachstelle durch einen Akteur mit durchschnittlichen Fähigkeiten ausgenutzt werden könnte. Des Weiteren gilt es, die Informationen aus der Bedrohungsanalyse miteinfließen zu lassen, um dadurch erfasste

Bedrohungsakteure oder Absichten zu berücksichtigen. Danach erfolgt eine Einstufung in einer der folgenden Bedrohungsstufen:

- Kritisch: Das Produkt enthält Schwachstellen, die vollständig offengelegt sind (physisch oder logisch) und leicht ausgenutzt werden können.
- Hoch: Das Produkt enthält Schwachstellen, die größtenteils offengelegt sind und halbwegs leicht ausgenutzt werden können.
- Mäßig: Das Produkt, der Dienst oder der Lieferant enthält Schwachstellen, die mäßig offengelegt sind und nur schwer ausgenutzt werden können.
- Gering: Das Produkt, der Dienst oder der Lieferant ist nicht gefährdet und kann wahrscheinlich nicht ausgenutzt werden.

Analyse der Auswirkungen
In der Analyse der Auswirkung [11] wird der potenzielle Schaden, der durch den Verlust, die Beschädigung oder die Kompromittierung des Produktes entstehen würde, bewertet. Nach Abschluss wird eine der folgenden Schadensstufen zugewiesen:

- Kritisch: Wenn das Produkt nicht wie vorgesehen funktioniert, würde dies zu einem Totalausfall des Unternehmens oder zu einer erheblichen und/oder inakzeptablen Beeinträchtigung des Betriebs führen, die nur mit außergewöhnlichem Zeit- und Ressourcenaufwand wiederhergestellt werden könnte.
- Hoch: Wenn das Produkt nicht wie vorgesehen funktioniert, würde dies zu einem schwerwiegenden Ausfall des Unternehmens oder zu einer erheblichen und/oder inakzeptablen Beeinträchtigung des Betriebs führen, die nur mit erheblichem Zeit- und Ressourcenaufwand wiederhergestellt werden könnte.
- Mäßig: Das Versagen des Produkts würde zu einem schwerwiegenden Unternehmensausfall führen, der jedoch ohne langfristige Folgen leicht und schnell behoben werden könnte.
- Gering: Das Versagen des Produkts würde nur zu geringen negativen Auswirkungen auf das Unternehmen führen, die leicht und schnell behoben werden könnten, ohne dass dies langfristige Folgen hätte.

Analyse der Risikoreaktion
Zunächst wird die Wahrscheinlichkeit ermittelt, die sich durch eine Kombination der Ergebnisse der Bedrohungs- und Schwachstellenanalyse ergibt. [11]

Wahrscheinlichkeits-Einstufung					
	Schwachstelle				
		Niedrig	Mäßig	Hoch	Kritisch
Bedrohung	Kritisch	Mäßig	Hoch	Kritisch	Kritisch
	Hoch	Mäßig	Hoch	Hoch	Kritisch
	Mäßig	Niedrig	Mäßig	Hoch	Hoch
	Niedrig	Niedrig	Niedrig	Mäßig	Mäßig

Tabelle 5: Ermittlung der Wahrscheinlichkeit laut S-CSRA [11]

Die Risikobewertung für das Produkt ergibt sich nun aus der Kombination von Wahrscheinlichkeit und Auswirkung. [11]

Risikobewertung					
Wahrscheinlichkeit (Bedrohung und Schwachstelle)	Auswirkung				
		Niedrig	Mäßig	Hoch	Kritisch
	Kritisch	Mäßig	Hoch	Kritisch	Kritisch
	Hoch	Mäßig	Hoch	Hoch	Kritisch
	Mäßig	Niedrig	Mäßig	Hoch	Hoch
	Niedrig	Niedrig	Niedrig	Mäßig	Mäßig

Tabelle 6: Ermittlung der Risikobewertung laut S-CSRA [11]

Auf Basis der Risikobewertung kann das Unternehmen nun entscheiden, ob die Beschaffung des Produkts fortgesetzt werden soll oder nicht.

2.2.3. Allgemeine Risikomanagement Frameworks

In diesem Abschnitt werden allgemeine IT-Risikomanagement-Frameworks, also jene ohne Spezialisierung auf Third-Parties, kurz vorgestellt sowie deren Bezug zu TPRM untersucht.

ISO/IEC 27005
Die ISO/IEC 27005 [13] wird mit dem Titel *Information technology - Security techniques - Information security risk management* geführt. Der internationale Standard beschreibt daher eine Methodik zum Risikomanagement in der Informationssicherheit und ist Teil der ISO 2700x Serie. Der darin beschriebene Prozess ist angelehnt an das generische Risikomanagement der ISO 31000 [39]. Der Prozess setzt sich zusammen aus: Festlegung des Kontexts, Risikoidentifikation, -bewertung, -akzeptanz, -kommunikation und Beratung sowie Risikoüberwachung und -überprüfung.
Der Standard selbst stellt keinen expliziten Bezug zu Third-Party- oder Lieferantenrisikomanagement her. In der bereits untersuchten ISO/IEC 27036 ist ebenfalls kein Querverweis auf die ISO/IEC 27005 zu finden. Monev [40] konnte in seiner Arbeit feststellen, dass keine der kommerziellen Lösungen im Bereich TPRM den Prozess der ISO/IEC 27005 folgen. Der tatsächliche Einsatz der ISO/IEC 27005 als TPRM-Prozess konnte aber, basierend auf der vorliegenden Literatur, nicht endgültig geklärt werden.

NIST Cybersecurity Framework (NIST-CSF)
Das *National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF)* [12] wurde als Antwort auf die im Februar 2013 veranlasste Durchführungsverordnung des US-Präsidenten verfasst. Das Rahmenwerk wurde in einer Kooperation von Industrie und Regierung geschaffen und soll den Schutz der kritischen Infrastruktur fördern. Das Dokument soll diese Betreiber unterstützen, Cyberrisiken zu identifizieren, zu bewerten und zu steuern. Den Kern des Rahmenwerks bilden die fünf Hauptaufgaben: *Identify*, *Protect*, *Detect*, *Respond* und *Recover*. Diese werden jeweils mit Kategorien, Unterkategorien sowie informativen Hinweisen konkretisiert.
In der Hauptaufgabe *Identify* wird Supply Chain Risk Management (ID.SC) als eigene Kategorie geführt. Unternehmen werden hierbei aufgefordert, den Kontext für den Umgang mit Supply Chain Risiken zu schaffen. Es ist daher nötig, einen Prozess einzusetzen, der SC-Risiken identifiziert, bewertet und steuert. Das Framework bietet dazu fünf Unterkategorien, die wiederum mit einer Vielzahl an Verweisen auf COBIT 5, ISO/IEC 27001, NIST SP 800-53 oder CIS CSC[12] ausgeführt werden. Für diese Arbeit besonders bedeutend sind die Unterkategorien ID.SC2 und ID.SC4 wie in der Abbildung 8 ersichtlich.

[12] CIS CSC – Center for Internet Security Critical Security Controls

ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2

Abbildung 8: TPRM-Bewertung im NIST CSF [12]

Konkrete Ansätze für die Bewertung von Lieferanten werden jedoch nicht beschrieben. Dazu wird auf andere Standards, Frameworks und Dokumente verwiesen. Außerdem verweist das Dokument für ein C-SCRM direkt auf die NIST SP 800-161. Der Bezug zwischen TPRM und NIST-CSF ist dennoch klar gegeben.

NIST SP 800-37 (RMF)
Beim *Risk Management Framework for Information Systems and Organizations (RMF)* [41] handelt es sich um eine weitere *Special Publication* aus der 800-Serie des NIST. Das NIST-RMF bietet einen „dynamischen und flexiblen Ansatz zur effektiven Bewältigung von Sicherheits- und Datenschutzrisiken in unterschiedlichen Umgebungen […]“ [41]. Das NIST-RMF kann mit dem NIST-CSF abgestimmt und als Risikomanagementprozess eingesetzt werden, um die Punkte aus dem NIST-CSF umzusetzen. Das NIST-RMF besteht aus sieben Schritten: *Prepare*, *Categorize*, *Select*, *Implement*, *Assess*, *Authorize* und *Monitor*.
Laut Prozess gilt es im ersten Schritt *Prepare*, eine organisationsweite Risikobewertung durchzuführen, dazu gehört auch ein Supply Chain Risk Assessment (SCRA). Auf die Umsetzung dieses SCRA wird im RMF aber nur kurz eingegangen: „Risikobewertungen in der Supply Chain können Informationen aus Lieferantenaudits, Überprüfungen und Informationen aus der Lieferkette umfassen.“ [41] Ein Bezug zwischen TPRM und NIST-RMF ist zwar gegeben, jedoch wird hier nur die Notwendigkeit unterstrichen und für Details auf die bereits oben beschriebene NIST SP 800-161 verwiesen.

Weitere Risikomanagement-Frameworks
Neben den bereits genannten Frameworks gibt es noch die ISO 31000 [39], die sich ebenfalls mit Risikomanagement beschäftig und dabei weder industrie- noch sektorspezifisch ist. Die ISO/IEC 31010 [42] stellt eine Erweiterung der 31000-Norm dar und beschreibt Bewertungsmethoden und -verfahren für das Riskmanagement. Auch das BSI stellt mit dem Standard 200-3 [43] einen mit dem IT-Grundschutz verbundenen Risikomanagementansatz zur Verfügung.

2.3. Fazit zum Stand der Wissenschaft

Die Wissenschaft ist sich einig darüber, dass es im Umgang mit Risiken, die durch die Geschäftsbeziehungen und Vernetzungen mit Dritten entstehen, viele Herausforderungen gibt. So findet

sich kaum eine Arbeit, die nicht die Komplexität durch die meist große Anzahl an Third-Parties in der eigenen Lieferkette hervorhebt. Auch wenn durchwegs viele wissenschaftliche Arbeiten in diesem Bereich existieren, wird durch fehlende quantitative Arbeiten eine nennenswerte Unreife in diesem Fachgebiet geortet [9]. Dies ist womöglich auch ein Grund dafür, warum sich bislang in der Wirtschaft kein Standard für das TPRM wirklich durchgesetzt hat. Speziell das Identifizieren und Bewerten von Third-Party-Risiken wird in den Publikationen als wichtiger Schritt anerkannt. Zur konkreten Umsetzung liefern jedoch nur wenige Arbeiten hilfreichen Input. Dies gilt auch für die allgemeinen Risikomanagement-Frameworks (ISO 27005, NIST-CSF, NIST-RMF), die den Prozess sowie die Anforderungen klar definieren, dann jedoch keine spezifischen Methoden für die Risikobewertung von Dritten bereitstellen [32]. Auch der spezifische ISO/IEC 27036 Standard stellt nur wenige Anhaltspunkte bereit, um den Reifegrad eines Partnerunternehmens festzustellen beziehungswiese das damit verknüpfte Risiko abzuschätzen. Den mit Abstand ausführlichsten Input für diese Thematik liefert das NIST mit der SP 800-161. Die Publikation fügt sich in die sehr umfangreiche 800-Serie an Spezialpublikationen für Informationssicherheit ein. In dem 338 Seiten Dokument wird zum einen detailliert auf die Risikobewertung eingegangen und zum anderen auch die Umsetzung in der eigenen Organisation mit fertigen Vorlagen erleichtert. Am Ende des Tages handelt es sich bei der SP 800-161 um eine klassische Risikobewertung mit Risikomatrix, die bei einer großen Anzahl an Lieferanten zu entsprechend hohen Aufwand führen wird. Zusammengefasst ist in der Thematik TRPM noch kein wissenschaftlicher Konsens zu entdecken und so ist auch die Anforderung einer holistischen (und effizienten) Identifizierung und Bewertung von Dritten bis dato unerfüllt.

3. Regulatory Compliance und Third-Party Risk Management

Je nach Standort und Branche des Unternehmens zeigt sich nötig, unterschiedliche Gesetze und Vorschriften zu beachten. Diese Disziplin wird als „Regulatory Compliance“ oder nur „Compliance“ bezeichnet, wodurch die Einhaltung dieser Regeln gesteuert werden soll. Für die Definition von Compliance wird oftmals die Aussage von Krügler zitiert: „Der Begriff Compliance steht für die Einhaltung von gesetzlichen Bestimmungen, regulatorischer Standards und Erfüllung weiterer, wesentlicher und in der Regel vom Unternehmen selbst gesetzter ethischer Standards und Anforderungen.“ [44]
In dieser Arbeit werden die gesetzlichen und regulatorischen Auflagen für TPRM beleuchtet, selbst gesetzte Standards in Unternehmen werden nicht untersucht. Die Erhebung schränkt sich auf das Bankwesen in Österreich ein. Es wird daher dargestellt, welche gesetzliche und regulatorische Auflagen eine österreichische Bank im Umgang mit Dritten im Bereich der Informationstechnologie treffen. Darüber hinaus wird evaluiert, ob und welche konkreten Anforderungen sich an die Risikobeurteilung von Dritten ergeben und wie konkret diese formuliert werden.

3.1. Übersicht

Zunächst wurden relevante Regularien durch eine Online-Recherche erhoben. Des Weiteren wurden im Expertengespräch mit Simon Wilfing (Informationssicherheit, Raiffeisen Bank International) weitere zu beachtende Regularien eruiert und anschließend ergänzt. In Summe wurden die in Tabelle 7 neun dargestellten Gesetze, Richtlinien und Verordnungen auf deren Bezug zu TPRM analysiert. Leitfäden der österreichischen Finanzmarktaufsicht (FMA) wurden bewusst ausgenommen, da diese hochgradig jenen der Europäische Bankenaufsichtsbehörde (EBA) entsprechen.

	Bezeichnung	**Regulator**	**Art**	**Version / Datum**	**Geltungsbereich**
EBA Outsourcing	Leitlinien zu Auslagerungen	European Banking Authority	Leitlinie	25.Feb.19	EU
EBA IKT Risikobewertung	Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP)	European Banking Authority	Leitlinie	11.Sep.17	EU
EBA IKT	EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken	European Banking Authority	Leitlinie	28.Nov.19	EU
NISG	Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)	Österreichisches Parlament	Gesetz (EU-Richtlinie)	21.Mär.22	Österreich
DORA	Digital Operational Resilience Act (DORA)	Europäische Kommission	Entwurf EU-Verordnung	24.Sep.20	EU
DSGVO	Datenschutz-Grundverordnung (DSGVO)	Europäische Kommission	EU-Verordnung	04.Mai.16	Weltweit (EU Personendaten)
BWG	Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG)	Österreichisches Parlament	Gesetz	21.Mär.22	Österreich
ZaDiG	Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (Zahlungsdienstegesetz 2018 – ZaDiG 2018)	Österreichisches Parlament	Gesetz (EU-Richtlinie)	21.Mär.22	Österreich
AI Act	Gesetz über künstliche Intelligenz	Europäische Kommission	Entwurf EU-Verordnung	21.Apr.21	EU

Tabelle 7: TPRM relevante Regularien für das österreichische Bankwesen

Die Tabelle 7 führt eine Abkürzung, die Bezeichnung, den Regulator, die Art der Rechtsform, die untersuchte Version und den geografischen Geltungsbereich, in denen die Anforderungen wirken.

Eine Vielzahl der Einträge steht mit Rechtsakten auf EU-Ebene in Verbindung. Es gilt dabei, zwischen EU-Verordnungen und EU-Richtlinien zu unterscheiden. So ist die EU-Verordnung ein verbindlicher Rechtsakt, den alle EU-Länder unmittelbar umsetzen müssen. Hingegen handelt es sich bei einer EU-Richtlinie um ein zu erreichendes Ziel. Es ist hier jedoch Angelegenheit der einzelnen EU-Länder, entsprechende nationale Gesetze abzuleiten. [45] Darüber hinaus ist wichtig, in welcher Phase sich die EU-Verordnung oder -Richtlinie im ordentlichen Gesetzgebungsverfahren befindet. So wurde ein Entwurf lediglich von der EU-Kommission vorgeschlagen, aber noch nicht von EU-Parlament und EU-Rat beschlossen. Es ist daher noch kein gültiges EU-Gesetz. [46]

3.2. European Banking Authority (EBA)

Die Europäische Bankenaufsichtsbehörde (EBA) ist eine EU-Behörde, die den europäischen Bankensektor reguliert und beaufsichtigt. Dabei sind die Finanzstabilität in der EU sowie die Integrität des Bankensektors als oberste Ziele definiert. Eine der Hauptaufgabe der EBA ist die Erstellung von verbindlichen technischen Standards und Leitlinien, wobei drei dieser Werke in Zuge dieser Arbeit analysiert werden. Sowohl die „Leitlinien zu Auslagerungen“, die „Leitlinien für die IKT-Risikobewertung“ als auch die „EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken“ können mit der hier behandelten Thematik in Verbindung gebracht werden. [47]

Leitlinien zu Auslagerungen
In diesen Leitlinien [48] werden Regeln festgelegt, die Finanzinstitute in der EU beim Auslagern zu beachten haben. Im Vordergrund steht die Auslagerung kritischer oder wesentlicher Funktionen. Als Auslagerung wird die Vereinbarung mit einem Dienstleister bezeichnet, der „[…] einen Prozess durchführt, eine Dienstleistung erbringt oder eine Tätigkeit ausführt, die das Institut […] ansonsten selbst übernähme“ [48]. Generell fordert das Dokument den Einsatz eines ganzheitlichen Risikomanagements, das sämtliche Risiken einschließlich derjenigen, die sich durch Vereinbarungen mit Dritten ergeben, ermittelt und steuert. So gilt es, alle Risiken, die mit Dritten zusammenhängen, zu ermitteln, zu bewerten, zu überwachen und zu steuern. Dabei wird auch explizit auf IT-Risiken sowie Cyberrisiken verwiesen. Der Risikobewertung wird ein eigener Absatz gewidmet. Dieser weist auf den Einsatz einer Szenarioanalyse hin, um den Risikoumfang und die Auswirkungen auf das operationale Risiko zu erheben. Darüber hinaus werden für kleine und nicht komplexe Institute qualitative Ansätze zur Risikobewertung akzeptiert. Von großen und komplexen Instituten werden hingegen komplexere Ansätze gefordert, die interne und externe Verlustdaten für die Szenarioanalysen verwenden. Folgende Mindestanforderungen an die Risikobewertung werden aufgestellt:

- Einstufung der Sensitivität sowie der erforderlichen Sicherheitsmaßnahmen der Funktionen, Daten und Systeme, die die Auslagerung betreffen
- Gründliche risikobasierte Analyse der Funktionen, Daten und Systeme, die die Auslagerung betreffen
- Die Folgen des Standorts des Dienstleisters (EU versus außerhalb der EU)
- Die politische Stabilität und Sicherheitslage einschließlich Gesetze und Vorschriften
- Vorgabe für die Vertraulichkeit, Integrität und Verfügbarkeit der Auslagerung

Noch vor Vertragsabschluss und der Risikobewertung ist es wichtig, eine Due-Diligence-Prüfung durchzuführen, die die Eignung des Dienstleisters sicherstellen soll. So muss das Institut sicherstellen, „[…], dass der Dienstleister über die geschäftliche Reputation, angemessene und ausreichende Fähigkeiten, Fachkenntnisse, Kapazitäten, Mittel (z. B. personelle und finanzielle Mittel, IT-Ressourcen), Organisationsstruktur und gegebenenfalls die erforderliche(n) aufsichtliche(n) Zulassung(en) oder Registrierung(en) zur Wahrnehmung der kritischen oder wesentlichen Funktion in zuverlässiger und

professioneller Weise verfügt, um seine Verpflichtungen während der Laufzeit des Vertragsentwurfs zu erfüllen.“ Außerdem wird auf die Durchführung von Sicherheitspenetrationstests verwiesen, die im Einklang mit den *Leitlinien der EBA für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses* stehen sollten.

Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP)

In diesen Leitlinien [49] geht es um die behördliche Überprüfung von Instituten hinsichtlich der Ermittlung und Bewertung von Risiken in Zusammenhang mit Informations- und Kommunikationstechnologie (IKT). Dabei wird auch das IKT-Auslagerungsrisiko berücksichtigt oder, anders ausgedrückt, die Existenz und Ausprägung eines Third-Party Risk Managements erhoben. Die zuständigen Behörden müssen bewerten, ob das Institut IKT-Risiken bei der Auslagerung entsprechend berücksichtigt. Im Detail werden folgende Punkte für die Überprüfung durch Behörden genannt:

- Erfolgte eine Bewertung der Auswirkungen der IKT-Auslagerung während des Beschaffungsprozesses (Due-Diligence-Prüfung). Das Institut sollte die IKT-Kontrollen des Dienstleisters überprüfen und diese Überprüfung auch regelmäßig aktualisieren.
- Vorhandene Überwachung der IKT-Risiken durch ausgelagerte Dienstleistungen
- Überwachung der Einhaltung des Dienstleistungsniveaus sowie der Dienstleistungsvereinbarung (SLA)
- Existenz geeigneter Mitarbeiter, Ressourcen und Kompetenzen zur Überwachung und Steuerung von IKT-Risiken, die durch Auslagerung entstehen

Im Anhang des Dokuments werden fünf IKT-Risikokategorien genannt, wobei auch IKT-Auslagerungsrisiken beschrieben werden, d.h. es handelt sich hier um Third-Party Risiken im IT-Umfeld.

IKT-Auslagerungs-risiken	Unzureichende Resilienz der Dienste von Drittanbietern oder anderer Gruppen-unternehmen	Die Nichtverfügbarkeit kritischer IKT-Auslagerungsdienste, Telekommunikationsdienste und -einrichtungen. Verlust oder Beschädigung kritischer/sensibler Daten, die dem Dienstanbieter anvertraut sind	• Nichtverfügbarkeit wesentlicher Dienste durch Ausfälle in (ausgelagerten) IKT-Systemen oder Anwendungen von Lieferanten. • Unterbrechung von Telekommunikationsverbindungen. • Stromversorgungslücken.
	Unangemessene Auslagerungs-politik	Wesentliche Verschlechterung der Dienste oder Ausfälle aufgrund ineffizienter Vorbereitung oder Kontrollprozesse des ausgelagerten Dienstanbieters. Eine ineffiziente Auslagerungspolitik kann zu einem Mangel an geeigneten Kompetenzen und Kapazitäten im Hinblick auf die vollständige Ermittlung, Bewertung, Minderung und Überwachung der IKT-Risiken führen und die operativen Kapazitäten der Institute einschränken.	• Mangelhafte Ereignishandhabungsverfahren, vertragliche Kontrollmechanismen und Garantien in der Dienstanbietervereinbarung, die die Abhängigkeit von Schlüsselkräften von Dritten und Verkäufern erhöhen. • Unangemessene Änderungsmanagementkontrollen in Bezug auf die IKT-Umgebung des Dienstanbieters können zu umfassenden Diensteinschränkungen oder -ausfällen führen.
	Unzureichende Sicherheit der Drittanbieter oder anderer Gruppenunter-nehmen	Gehackte IKT-Systeme der Drittanbieter mit direkten Auswirkungen auf die ausgelagerten Dienste oder beim Dienstanbieter gespeicherte kritische/vertrauliche Daten. Dienstanbieter, die einen unberechtigten Zugriff auf beim Dienstanbieter gespeicherten kritischen/sensiblen Daten erhalten	• Das Hacken von Dienstanbietern durch Kriminelle oder Terroristen als Einstiegspunkt in die IKT-Systeme der Institute oder zum Zugriff/ zur Zerstörung kritischer oder sensibler Daten, die beim Dienstanbieter gespeichert sind. • Böswillige Mitarbeiter des Dienstanbieters versuchen, sensible Daten zu stehlen und zu verkaufen.

Abbildung 9: IKT-Auslagerungsrisiken laut EBA [49]

EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken

In diesen Leitlinien [50] werden Anforderungen zur Steuerung der IKT- und Sicherheitsrisiken festgelegt, die Institute erfüllen müssen. Die Leitlinien umfassen Anforderungen an die Informationssicherheit, die die Cybersicherheit miteinschließt. Im Kapitel 1.2.3 wird auch die Nutzung von Drittanbietern kurz behandelt,

wobei hier primär auf die *EBA-Leitlinien zu Auslagerungen* verwiesen wird. Wiederholt wird von Instituten gefordert, bei Auslagerung die Verfügbarkeit von IKT-Diensten und -Systemen zu gewährleisten. Es ist also nötig, verhältnismäßige Ziele, Maßnahmen und Mindestanforderungen an die Informationssicherheit aufzustellen sowie zu überwachen. Konkrete Anforderung an die Bewertung von Third-Parties sind in diesen Leitlinien nicht enthalten.

3.3. Netz- und Informationssystemsicherheitsgesetz (NISG)

Aufgrund der EU-Richtlinie „Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen“ [51] wurde in Österreich das „Netz- und Informationssystemsicherheitsgesetz (NISG)“ [52] erlassen. Auf dessen Grundlage wurde wiederum die „Netz- und Informationssystemsicherheitsverordnung (NISV)“ [53] umgesetzt. Durch das NIS Fact Sheet [54] wird speziell eine nähere Erläuterung für Betreiber wesentlicher Dienste durch das Bundesministerium für Inneres zur Verfügung gestellt. Die beschriebene Hierarchie wird in Abbildung 10 dargestellt.

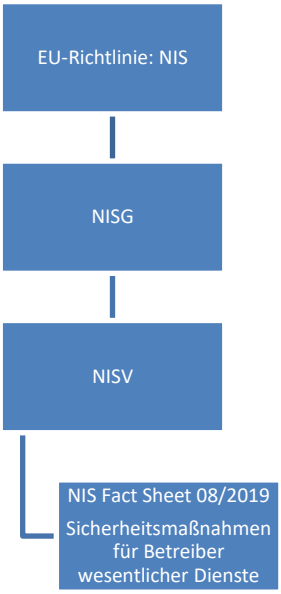

Abbildung 10: Umsetzungshierarchie der EU-NIS-Richtlinie in Österreich

In der NISV [53] wird der Sektor Bankwesen als wesentlicher Dienst eingeordnet. Betroffene Betreiber wesentlicher Dienste werden durch das Bundesministerium festgelegt und mittels Bescheids informiert. Aufgrund dieser Einordnung ergeben sich für betroffene Unternehmen entsprechende Anforderungen. So wird in der NISV auch ein entsprechender Umgang mit Dienstleistern, Lieferanten und Dritten gefordert. Konkret gilt laut § 14 der NISV:

- „Anforderungen an Dienstleistern, Lieferanten und Dritte für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme sind festzulegen und periodisch zu überprüfen.“ [53]
- „Die Leistungsvereinbarungen mit Dienstleistern und Lieferanten sind periodisch zu überprüfen und zu überwachen.“ [53]

Eine Konkretisierung beider Punkte findet sich im NIS Fact Sheet [54]. Der Betreiber ist aufgefordert, ein Gesamtbild zu erstellen, das das Ökosystem einschließlich Dienstleister und Lieferanten darstellt. Als Zweck werden die Identifikation und Bewertung von Risiken, die sich aus den Beziehungen ergeben, genannt. Für

die Bewertung der Dienstleister sollen die Eckpunkte Reife, Vertrauen, Zugriffsebene und Abhängigkeit evaluiert werden:

Reife	Über welche technischen Fähigkeiten verfügen die Dienstleister, Lieferanten und Dritten in Bezug auf Cybersicherheit?
Vertrauen	Kann ich davon ausgehen, dass die Absichten des Dienstleisters, Lieferanten und Dritten mir gegenüber vertrauenswürdig und diese selbst zuverlässig sind?
Zugriffsebene	Welche Zugangsrechte haben die Dienstleister, Lieferanten und Dritten zu Netz- und Informationssystemen?
Abhängigkeit	Inwieweit ist die Beziehung zu Dienstleistern, Lieferanten und Dritten für die Tätigkeit entscheidend?

Tabelle 8: Bewertungsfragen aus dem NIS Fact Sheet [54]

Darüber hinaus gilt es für Netz- und Informationssysteme, die durch Dritte erbracht werden, sogenannte Service Level Agreements (SLA) festzulegen. In diesen werden auch Sicherheitsanforderungen definiert, deren Einhaltung periodisch zu überprüfen ist. [54]

3.4. Digital Operational Resilience Act (DORA)

Beim Digital Operational Resilience Act (DORA) handelt es sich um einen Vorschlag der Europäischen Kommission, durch den erreicht werden soll, dass alle Parteien im Finanzsystem über notwendige Sicherheitsvorkehrungen verfügen, um Informations- und Kommunikationstechnik- (IKT) wie auch Cyber-Risiken zu minimieren. Dadurch sollen Anforderungen an die IKT im Finanzbereich konsolidiert und gestärkt werden. Der Vorschlag umfasst neun Kapiteln, die sich unter anderem mit IKT-Risikomanagement, Management von IKT-Vorfällen, Testung von IKT-Systemen, Informationsaustausch und auch dem Risikomanagement von IKT-Drittanbietern befassen. Die Thematik rund um IKT-Drittanbieter wird im Kapitel V auf den Seiten 58 bis 75 ausführlich dargelegt. [55] Das Kapitel teilt sich dazu auf zwei Abschnitte:

- Abschnitt 1: Grundsätze für eine zuverlässige Steuerung des Risikos durch IKT-Drittanbieter
  In diesem ersten Abschnitt werden allgemeine Grundsätze definiert. Es wird direkt klargestellt, dass die Verantwortung beim Outsourcing immer beim Finanzunternehmen bleibt. So werden Finanzunternehmen verpflichtet, einen Informationsregister über IKT-Drittanbieter zu führen und diesen auch jährlich der zuständigen Behörde zu melden. Darüber hinaus werden Gründe aufgelistet, die jedenfalls zu einer Kündigung des IKT-Dienstes führen müssen. Des Weiteren sind Unternehmen angehalten, Ausstiegsstrategien zu entwickeln. Die Bewertung des IKT-Risikos wird nur vage beschrieben, da wird es nötig, alternative Lösungen in Betracht zu ziehen und bei Auslagerung kritischer Funktionen die Vorteile und Risiken abzuwägen. Allenfalls sind Rechte und Pflichten des Finanzunternehmens und des IKT-Drittanbieters eindeutig zu regeln und vertraglich festzuhalten. Bei allen Punkten wird wiederholt auf die Europäischen Aufsichtsbehörden (ESAs) hingewiesen, die mit der Erarbeitung der Konkretisierung in Form eines technischen Regulierungsstandards (RTS) beauftragt wurde. Dieser RTS liegt zum jetzigen Zeitpunkt (21. März 2022) öffentlich nicht vor. [55]
- Abschnitt 2: Aufsichtsrahmen für kritische IKT-Drittanbieter
  Im zweiten Abschnitt wird die Erstellung eines Aufsichtsrahmens beschrieben, der bedeutende IKT-Drittanbieter (wie zum Beispiel Big Techs) für die gesamte EU-Finanzindustrie einheitlich und verstärkt regulieren soll. Dabei soll eine Aufsichtsinstanz auf EU-Ebene ernannt werden, die zusätzliche Befugnisse zur Überwachung dieser kritischen IKT-Drittanbieter erhält. Diese

Aufsichtsinstanz bewertet, ob kritische IKT-Drittanbieter umfassende, robuste und wirksame Vorkehrung zur Steuerung von IKT-Risiken einsetzen. Zur Wahrnehmung dieser Aufgaben erhalten sie zusätzliche Befugnisse wie etwa eine ausführliche Dokumenteneinsicht bei IKT-Drittanbietern oder das Recht auf Vor-Ort-Prüfungen. Auch hier wurden die ESAs zur Erarbeitung eines RTS beauftragt. [55]

Aktuell handelt es sich bei DORA lediglich um einen Entwurf, der daher zum jetzigen Zeitpunkt keine Verpflichtungen für das österreichische Bankwesen mit sich bringt. Außerdem liefert die vorliegende Version kaum Angaben zur konkreten Bewertung von IKT-Drittanbietern. Hierzu wurden die ESAs beauftragt, entsprechende Konkretisierungen zu erarbeiten.

3.5. Datenschutz-Grundverordnung (DSGVO)

Die Datenschutz-Grundverordnung (DSGVO) [56] wurde 2016 durch den Europäischen Rat und das Parlament veröffentlicht. Sie ist seit 25. Mai 2018 die Grundlage des Datenschutzrechts in der EU wie auch in Österreich und regelt die Verarbeitung personenbezogener Daten. Das bereits länger bestehende Datenschutzgesetz (DSG) ergänzt die DSGVO nur noch. Im Artikel 4 werden die in der Verordnung verwendeten Begriffe definiert. Beim „Verantwortlichen“ handelt es sich um die „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.“. Ein „Auftragsverarbeiter“ wird als eine „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet“ bezeichnet. Nimmt eine österreichische Bank einen Clouddienst in Anspruch und lässt dort Kundendaten verarbeiten, so fungiert die Bank als Verantwortlicher und der Cloudanbieter als Auftragsverarbeiter. Digitales Outsourcing ist meist also mit der elektronischen Verarbeitung von personenbezogenen Daten verbunden, wodurch der Artikel 28 der DSGVO zu beachten ist. Der Auftragsverarbeiter (zum Beispiel IT-Dienstleister oder Cloudanbieter) muss geeignete technische und organisatorische Maßnahmen (TOMs) so umsetzen, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Darüber hinaus muss die Verarbeitung vertraglich geregelt sein und zumindest „Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen“ definiert werden. [56]

Laut Artikel 28 darf der Verantwortliche nur mit Auftragsverarbeitern arbeiten, die ausreichende Garantien (TOMs) bieten, und wird somit auch zur Überprüfung externer Dienstleister verpflichtet. Im Abschnitt 2 Artikel 32 wird die Sicherheit der Verarbeitung und der dazugehörigen TOMs konkretisiert. So gilt es, TOMs zu implementieren, die den Stand der Technik, die Implementierungskosten, die Art, den Umfang, die Umstände und den Zweck der Verarbeitung berücksichtigen. [56] Als Beispiel werden die folgenden Mindestmaßnahmen [56] genannt:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
- Fähigkeit zur raschen Wiederherstellung der Daten
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Zusätzlich wird in Artikel 32 auf genehmigte Zertifizierungsverfahren in Artikel 42 verwiesen, die als Faktor für die Erfüllung der erforderlichen Maßnahmen herangezogen werden können. Konkrete Zertifizierungen werden jedoch in der DSGVO nicht genannt. Laut der Datenschutzbehörde (DSB) existieren - Stand heute (22.03.2022) - noch keine derartigen anerkannten Zertifizierungen [57].

Gerade durch den letzten Punkt in Artikel 32 Absatz 1, in dem Mindestmaßnahmen aufgelistet werden, wird eine eindeutige Brücke zur Thematik Third-Party Risk Management geschlagen. So fordert die DSGVO eine regelmäßige Risikobewertung aller vorhandenen Auftragsverarbeiter. Abgesehen von der Zertifizierung, wobei auch hier noch keine offiziell anerkannte existiert, ist in der Verordnung keine konkrete Methodik zur Risikobewertung von Dritten beschrieben.

3.6. Bankwesengesetz (BWG)

Das Bundesgesetz über das Bankwesen [58] wurde 1993 initial veröffentlicht und trat 1994 in Kraft. Da sich der regulatorische Teil dieser Arbeit auf das Bankwesen in Österreich bezieht, ist eine Analyse des Bankwesengesetzes unumgänglich.
Im § 25 wird die Thematik Auslagerung und der Rückgriff auf Dritte (Dienstleister) geregelt. Auch wenn hier die Art der Auslagerung nicht näher spezifiziert wird, ist eine Auslagerung von IT-Diensten unter Berücksichtigung dieses Abschnitts zu behandeln. Wie bereits in anderen Gesetzen wird auch in der BWG eine schriftliche Vereinbarung für die klare Aufteilung von Rechten und Pflichten zwischen Bank und Dienstleister gefordert. Darüber hinaus ist die Finanzmarktaufsicht (FMA) über die beabsichtigte Auslagerung wesentlicher bankbetrieblicher Aufgaben vor Abschluss zu informieren. Außerdem wird bei Rückgriff auf Dritte auf angemessene Vorkehrungen in der Anlage zu § 25 verwiesen. Die Anlage wird als „Auslagerungsbedingungen“ betitelt und umfasst 12 Punkte [58]. Die Folgenden wurden für diese Arbeit als relevant eingeordnet:

- „der Dienstleister hat die Ausführung der ausgelagerten Aufgaben ordnungsgemäß zu überwachen und die mit der Auslagerung verbundenen Risiken angemessen zu steuern“ [58]
- “das Kreditinstitut hat weiterhin mittels der hierfür notwendigen Fachkenntnisse die ausgelagerten Aufgaben wirkungsvoll zu überwachen und die mit der Auslagerung verbundenen Risiken zu steuern” [58]
- „der Dienstleister hat alle vertraulichen Informationen, die das Kreditinstitut und seine Kunden betreffen, zu schützen“ [58]

Bei der Auflistung ist auffällig, dass sowohl das Kreditinstitut wie auch der Dienstleister von den gesetzlichen Bedingungen betroffen ist. So wird im obigen Aufzählungspunkt eins auch der Dienstleister für die Steuerung der Risiken, die mit der Auslagerung verbunden sind, verpflichtet. Die Steuerung der verbundenen Risiken durch das Kreditinstitut werden nicht näher spezifiziert, die Anforderung einer Risikobewertung kann jedoch impliziert werden.

3.7. Zahlungsdienstegesetz (ZaDiG)

Durch das Zahlungsdienstegesetz [59] werden Bedingungen für Zahlungsdienstleister in Österreich gesetzlich geregelt. Damit werden sowohl die Rechte und Pflichten der Dienstleister als auch der Nutzer definiert. Bei Zahlungsdiensten handelt es sich um Tätigkeiten wie Bareinzahlungen, Barabhebungen, Zahlungsvorgänge oder auch Online-Dienste, die Informationen über ein Zahlungskonto halten. Als Zahlungsdienstleister werden daher unter anderem Kreditinstitute gemäß des BWGs definiert, wodurch eine klassische österreichische Bank auch dieser gesetzlichen Auflage Folge leisten muss.

Im § 21 der „Auslagerung von Aufgaben“ wird definiert, dass die Auslagerung (einschließlich IT-Systeme) weder negative Auswirkungen auf die Qualität interner Kontrollen noch die Beaufsichtigung der FMA haben darf. Auch das Zahlungsdienstegesetz fordert eine schriftliche Vereinbarung der Rechte und Pflichten zwischen Zahlungsinstitut und Dienstleister. Ebenfalls ident zum BWG muss die FMA über eine geplante Auslagerung vorab informiert werden. [59]

Durch § 85 werden Zahlungsdienstleister verpflichtet, eine aktualisierte und umfassende Bewertung der operationellen und sicherheitsrelevanten Risiken jährlich der FMA zu melden. Dabei sind Risikominderungsmaßnahmen und Kontrollmechanismen hinsichtlich Ihrer Effizienz vorzulegen. [59]

3.8. Gesetz über künstliche Intelligenz (AI Act)

Beim Gesetz über künstliche Intelligenz [60] handelt es sich aktuell um einen Vorschlag für eine EU-Verordnung, die in der Version vom 21. April 2021 vorliegt. Durch die Verordnung sollen einheitliche Vorschriften für den Einsatz künstlicher Intelligenz („KI-Systeme“) in der Union geschaffen werden. Darüber hinaus werden damit verbotene Praktiken und Anforderungen an Hochrisiko-KI-Systeme aufgestellt. Die Verordnung soll sowohl für Anbieter wie auch Nutzer von KI-Systemen in der Union gelten. Prinzipiell werden drei Risikostufen von KI-Systemen festgelegt: diejenige, die verboten sind und ein unannehmbares Risiko darstellen (zum Beispiel eine unterbewusste Verhaltensmanipulation von Personen); diejenige, die als Hochrisiko-KI-Systeme geführt werden (zum Beispiel eine mögliche nachteilige Auswirkung auf die Grundrechte oder mögliche Gefährdung der Sicherheit); und alle anderen, die ein geringes oder minimales Risiko darstellen und daher durch Verordnung kaum reguliert werden. [60]
Da der AI Act auch für Nutzer gelten soll, könnte er als EU-Verordnung direkt auch für jene Unternehmen relevant werden, die KI-Systeme einsetzen; mitunter auch für Banken in Österreich, die Produkte auf Basis von künstlicher Intelligenz einsetzen oder einsetzen wollen. Im Artikel 29 regelt die Verordnung die Pflichten der Nutzer von Hochrisiko-KI-Systemen. Primär sind Nutzer dazu verpflichtet, den Betrieb des KI-Systems anhand der „Gebrauchsanweisung“ zu überwachen. [60] Wer aber nun die Klassifizierung der KI-Systeme wie auch die Risikobewertung vornimmt, ist momentan unklar [61]. Die Verantwortung für das in der Verordnung beschriebene Risikomanagementsystem für Hochrisiko-KI-Systeme ist aktuell nicht klar definiert.
Auch wenn der AI Act aktuell noch nicht in Kraft ist und eine eindeutige Einordnung in das Thema Third-Party Risk Management schwierig ist, sollten Unternehmen, die KI-Systeme einsetzen, mit Regulierungen in diesem Bereich rechnen und diese auch entsprechend berücksichtigen. Eine klare Forderung nach einer Risikobewertung der KI-Anbieter durch KI-Nutzer kann aus dem Vorschlag nicht abgeleitet werden.

3.9. Fazit der regulatorischen Anforderungen

Zusammenfassung der Anforderungen an das TPRM mit Fokus auf die Risikobewertung aus regulatorischer Betrachtung für das österreichische Bankwesen.

	Forderung eines TPRM	**Verpflichtungen**	**Kurzfassung**	**Methodik zur Risikobewertung von Dritten**
EBA Outsourcing	Ja	Ja	Leitlinien für Institute, die bei der Auslagerung zu beachten sind. Dabei werden auch Mindestanforderungen an die Risikobewertung Dritter aufgestellt.	Szenarioanalyse Due-Diligence-Prüfung Sicherheitspenetrationstests
EBA IKT Risikobewertung	Ja	Ja	Leitlinien für Behörden für die Überwachung von Instituten hinsichtlich derer Tätigkeiten, um IKT-Risiken zu bewerten. Dabei werden auch Anforderung an die Bewertung von IKT-Auslagerungsrisiken beschrieben.	Due-Diligence-Prüfung
EBA IKT Risiken	Ja	Ja	Generelle Leitlinie zur Steuerung der IKT- und Sicherheitsrisiken. Die Behandlung von Third-Party Risiken wird auch hier mit Verweis auf die EBA Outsourcing Leitlinien gefordert.	Nicht spezifiziert
NISG	Ja	Ja	Durch die abgeleitete NISV, die für Betreiber wesentlicher Dienste gilt, ergeben sich im Wesentlichen zwei Anforderung:	Nicht spezifiziert

			Identifikation und Bewertung von Third-Party Risiken, Festlegung von Sicherheitsanforderungen sowie deren periodische Überprüfung.	
DORA	Ja	Nein	Bei DORA handelt es sich um einen umfassenden Entwurf der EU-Kommission mit dem Ziel IKT-Risiken aller Teilnehmer im Finanzsystem zu minimieren. Das Risikomanagement für IKT-Drittanbieter wird ausführlich beschrieben - konkrete Angaben zur Bewertung sind jedoch nicht zu finden. Hierzu wurden die ESAs beauftragt, einen RTS zu erarbeiten.	Nicht spezifiziert
DSGVO	Ja	Ja	Durch die DSGVO wird der Verantwortliche dazu verpflichtet, ausschließlich Auftragsverarbeiter einzusetzen, die geeignete technische und organisatorische Maßnahmen einsetzen. Darüber hinaus ist ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung dieser Maßnahmen zu implementieren. Als konkrete Möglichkeit wird die Prüfung von Zertifizierungen genannt.	Due-Diligence-Prüfung Zertifizierungen
Bankwesengesetz	Ja	Ja	Durch das Bankwesengesetz wird sowohl das Finanzinstitut als auch der Dienstleister zur Überwachung und Steuerung der Auslagerungsrisiken verpflichtet. Konkreter wird jedoch auf das notwendige Third-Party Risk Management oder die Risikobewertung nicht eingegangen.	Nicht spezifiziert
Zahlungsdienste-gesetz	Ja	Ja	Das ZaDiG weist eine hohe Ähnlichkeit zum BWG auf und fordert eine umfassende Bewertung der operationalen und sicherheitsrelevanten Risiken, jedoch ohne dedizierte Aufforderung in Richtung Auslagerungsrisiken.	Nicht spezifiziert
Vorschlag AI Act	Nein	Nein	Der AI Act versucht, einen Rechtsrahmen für den Einsatz von künstlicher Intelligenz zu schaffen. Dabei wird durch einen risikobasierten Ansatz eine Einstufung der KI-Systeme gefordert, aus der sich unterschiedliche Regulierungsausprägungen ergeben. Eine Forderung einer Risikobewertung der KI-Anbieter durch Nutzer geht aus dem aktuellen Vorschlag nicht hervor.	Nicht gefordert

Tabelle 9: Compliance Assessment für TPRM im österreichischen Bankwesen

In der Tabelle 9 werden die Ergebnisse der Untersuchung tabellarisch aufbereitet. In der Spalte „Forderung eines TPRM“ wird festgehalten, ob direkt eine Steuerung der Risiken durch Dritte gefordert wird. Die Spalte „Verpflichtungen“ hält fest, ob die Regulierung aktuell zu Verpflichtungen führt. Denn sofern es sich nur um einen Gesetzesvorschlag handelt, ist eine Konformität zum jetzigen Zeitpunkt nicht erforderlich, wenn auch empfehlenswert. Neben einer Kurzfassung wird festgehalten, ob konkrete Methoden zur Risikobewertung genannt werden.

Durch die Untersuchung wird klar, welchen Stellenwert die Thematik rund um Dritte auch auf regulatorischer Ebene eingenommen hat. So wird die Umsetzung entsprechender Maßnahmen im Umgang mit Risiken durch Dritte für österreichische Banken aus verschiedensten Richtungen gefordert. Gesetzliche Forderungen existieren auf nationaler und europäischer Ebene durch NISG, DSGVO, Bankwesengesetz oder Zahlungsdienstegesetz; ebenso durch die branchenspezifische Bankenaufsicht EBA, die dazu auch konkretere Vorschriften in ihren Leitlinien festlegt. Auch wenn die Regulatoren unterschiedliche Intensionen verfolgen, wie etwa die EBA den Schutz des Finanzmarkts oder die DSGVO den Schutz personenbezogener Daten, so ist das verfolgte Ziel immer ein ähnliches. Unternehmen sollen auch bei Auslagerung oder der Zusammenarbeit mit Dritten entsprechende Maßnahmen ergreifen, um die Sicherheit gewährleisten zu können. Entscheidet sich eine Bank nun zur Auslagerung wesentlicher IT-

Funktionen oder hat dies bereits getan, ist es notwendig, zumindest die EBA Leitlinien, das NISG, die DSGVO, das Bankwesengesetz und das Zahlungsdienstegesetz zu beachten.

Durch die Untersuchung ergeben sich zusätzlich die folgenden beiden Erkenntnisse:
(1) Die Forderungen sowie der Inhalt in Richtung TPRM weisen unter den Regularien eine hohe Ähnlichkeit auf. So wird häufig die vertragliche Vereinbarung zwischen den Parteien genannt, um etwa die Rechte und Pflichten festzulegen. Auch die periodische Risikoüberprüfung des Dritten wird wiederholt gefordert. Dadurch ergibt sich in der Compliance-Tätigkeit der Vorteil, dass die Konformität mit einem Regulator die Wahrscheinlichkeit erhöht, auch mit anderen Regularien konform zu sein. Oder anders gesagt ist die Umsetzung einer TPRM-Maßnahme womöglich für mehrere Regulatoren von Relevanz.
(2) Auch wenn die Forderung nach einer Risikobewertung Dritter meist klar hervorgeht, bietet nur die EBA einige Punkte dazu, wie die Umsetzung konkret auszusehen hat. Es scheint, als gäbe es eine Parallele zur Literatur, in der ebenfalls die Relevanz von TPRM sowie der Risikobewertung außer Frage steht. Am Ende stehen jedoch keine klaren und einheitlichen Anweisungen zur Verfügung. So verweist keiner der Regulatoren auf ein entsprechendes TPRM-Framework oder weiterführende Ressourcen zur Thematik. Dadurch verstärkt sich die Annahme der Literaturrecherche, nach der sich nicht nur in der Wissenschaft, sondern auch in der Wirtschaft bis dato kein einheitlicher Ansatz für TPRM durchgesetzt hat.

4. Third-Party Risk Management as a Service (TPRM-as-a-Service)

Die Wissenschaft, Sicherheitsvorfälle aus der Vergangenheit oder auch Regulatoren zeigen deutlich, dass TPRM mittlerweile zu einer unumgänglichen Disziplin für Unternehmen geworden ist. Viele Organisationen befinden sich in einem riesigen Netzwerk umgeben von Dritten aufgrund der Supply Chain oder auch aufgrund von Outsourcing gewisser Dienste. Die Steuerung der Risiken, die damit zusammenhängen, wird immer komplexer. Wie aber den vorhergehenden Kapiteln dieser Arbeit zu entnehmen ist, ist eine einfache Lösung oder auch ein allgemeiner Ansatz aktuell nicht vorhanden. Aufgrund dessen müssen Unternehmen, die ein seriöses TPRM implementieren möchten (oder müssen) entsprechende Fachkräfte und auch Ressourcen aufbringen. Für große Unternehmen ist dieser Schritt wohl leichter möglich als für kleinere. Infolgedessen hat sich in den letzten Jahren ein neuer Markt gebildet: TPRM-as-a-Service. Dienstleister werben mit einer Lösung für dieses Problem und geben an, diese komplexe Aufgabe zu übernehmen. So wirbt ein amerikanisches Beratungsunternehmen mit dem folgenden Text für die TPRM-Unterstützung: „Viele Organisationen verfügen nicht über die Ressourcen oder die Bandbreite, um eine TPRM-Abteilung aufzubauen oder gar ein TPRM-Gremium zu ernennen.“ [62] Unternehmen haben somit die Möglichkeit, Dritte damit dazu beauftragen das Risiko der Dritten zu steuern beziehungsweise dabei zu unterstützen.

In diesem Abschnitt soll ein Einblick in diesen TPRM-as-a-Service-Markt geschaffen werden. Zusätzlich zum Überblick der Anbieter am Markt wird erforscht, wie diese das TPRM für Unternehmen umsetzen beziehungsweise dabei unterstützen. Der Fokus liegt wiederholt auf der Methodik, die zum Einsatz kommt, um die Risikoidentifikation und -bewertung der Dritten durchzuführen. Es wurden dazu einerseits öffentlich zugängliche Informationen ausgewertet, andererseits ein österreichischer Anbieter direkt kontaktiert und evaluiert.

4.1. Anbieterübersicht

Mithilfe einer Onlinesuche wurden Dienstleister für TPRM am Markt eruiert. Es wurde dabei konkret nach TPRM-as-a-Service Anbieter gesucht, die sich auf IT- oder Cyber-Risiken beziehen. Explizit ausgenommen und unbeachtet blieben in diesem Schritt reine Softwareprodukte, die etwa den TPRM-Prozess unterstützen beziehungsweise ein Online-Risk-Scoring durchführen (Produkte wie SecurityScorecard, BitSight, OneTrust Vendorpedia, UpGuard Vendor Risk, Prevalent, …). In Tabelle 10 werden die betrachteten TPRM-as-a-Service Anbieter gelistet. Die Tabelle listet neben dem Unternehmensnamen

auch den Hauptsitz, Auskunft darüber, ob ein Firmensitz in Österreich existiert und wie das TPRM-Service bezeichnet wird.

Unternehmensname	Hauptsitz	Sitz in AT	TPRM Bezeichnung
KSV1870 Nimbusec GmbH	AT	Ja	Third Party Cyber-Risk Management
Deloitte	CH	Ja	Third Party Risk Management
Ernst & Young Global Limited	UK	Ja	Third-Party-Risiko-Management
Guidepoint Security	US	Nein	Third-Party Risk Management as a Service
Schneider Downs Consulting	US	Nein	TPRM Officer as a Service
Kroll	US	Nein	Third-Party Cyber Risk Management
RSI Security	US	Nein	Third Party Risk Management Services
Halock	US	Nein	Third-Party Risk Management Services
CyberSecOp Consulting	US	Nein	Third Party Risk Management Services

Tabelle 10: Anbieter von TPRM-as-a-Service

Mit *KSV1870 Nimbusec GmbH*, *Deloitte* und *Ernst & Young Global Limited* befinden sich drei Anbieter direkt in Österreich. Alle anderen Dienstleister befinden sich in den Vereinigten Staaten von Amerika.

4.2. Auswertung öffentlicher Daten

Die aus Absatz 4.1 ermittelten Anbieter stellen öffentlich Informationen über das gebotene TPRM-Service zur Verfügung. Die öffentlich gebotene Informationsmenge schwankt aber stark, dennoch kann dadurch eine Tendenz der eingesetzten Methoden abgelesen werden, wie das Risiko der Dritten bewertet wird. Die folgende Auflistung startet mit häufiger bis hin zu seltener bei TPRM-as-a-Service Anbieter eingesetzten Risikobewertungstechniken:

- Third-Party Questionnaires

  Der Einsatz von Fragebögen in einem sogenannten „Self-Assessment“ ist die am häufigsten verwendete Form der Risikobewertung. Darüber hinaus ist die Methodik sehr einfach umzusetzen. Dem Dritten wird eine Liste von Fragen zugesendet und für die Beantwortung eine Frist gesetzt. [29] Derartige Selbst-Einschätzungen werden in der Literatur immer wieder kritisch betrachtet, da es sich oftmals um nicht verifizierte Aussagen des Partners handelt. Es wäre daher ein großer Fehler, sich ausschließlich auf diese Selbst-Einschätzung des Dritten zu verlassen. [6]
- Risiko-Monitoring

  Beim Risiko-Monitoring handelt es sich weniger um eine konkrete Methode als vielmehr um eine wiederholte Risikobeurteilung. Die große Problematik mit Überprüfungen von Dritten vor Vertragsabschluss (oft auch als Due-Diligence-Prüfung bezeichnet) ist, dass es in einer Momentaufnahme besteht, die bereits überholt ist, bevor es zum Abschluss kommt. Über diese Problematik herrscht Konsens in der Wissenschaft, Wirtschaft und auch durch Regulatoren, von denen Risiko-Monitoring als Standard im TPRM betrachtet wird. Es geht darum, die Sicherheitskontrollen des Dritten regelmäßig zu überprüfen und danach auch an Verbesserungen zu arbeiten. Dazu können unterschiedliche Bewertungsmethoden wie das Self-Assessment, Online-Risk-Rating (siehe Punkt 3) oder auch Vor-Ort-Audits (siehe Punkt 4) zum Einsatz kommen. [4]
- Online-Screening / Online-Risk-Rating

  Wie auch in Abschnitt 2.1.2 zu Keskin [14] beschrieben, handelt es sich hier um „nicht-invasive Risikobewertungsplattformen, welche durch öffentlich verfügbare Informationen versuchen das

Cyberrisiko von Unternehmen einzuschätzen“. Die primären Indikatoren, die hier herangezogen werden, sind: Fehlkonfiguration des Netzwerks (zum Beispiel öffentliche offene Ports oder unsichere TLS-Konfiguration), Softwarestatus (zum Beispiel Metadaten über den Patching-Status), Web Domains (zum Beispiel Schwachstellen der Internetseite), unternehmensbezogene Informationen (zum Beispiel Unternehmensbereich oder auch geleakte Daten), historische Datendiebstähle (zum Beispiel Pressemitteilungen). [14]

- Vor-Ort-Audit

  Das Maß der Dinge ist die direkte Überprüfung vor Ort. Dabei ist die Vorbereitung ein wichtiger Bestandteil, um die Agenda, einzuholende Informationen und Interviewpartner festzulegen. Mit dieser Methode können Informationen über Risiken und Kontrollen nicht nur direkt eingeholt, sondern auch verifiziert werden. Auf der anderen Seite ist dieses Vorgehen sehr ressourcenaufwendig. Daher wird es im TPRM meist nur für Schlüsselpartner eingesetzt und dabei oftmals auch auf externe Berater und Auditoren zurückgegriffen. [29]

- Schwachstellen-Scans und Penetration-Tests

  Durch Schwachstellen-Scans wird aktiv nach Sicherheitsmängel gesucht, die ein Angreifer ausnutzen könnte. Der Partner sollte dazu die eigenen öffentlichen IP-Adressen zur Verfügung stellen, um den Scan entsprechend zielgerichtet ausführen zu können. Penetration-Tests gehen dann nochmals einen Schritt weiter, wobei Tester tatsächlich versuchen, in das Firmennetzwerk einzudringen. Es handelt sich daher um eine echte Simulation einer Attacke von außen. In beiden Fällen sollte der Dritte, der getestet wird, vorab involviert und eine „Permission-to-attack“ eingeholt werden.

- Zertifizierungsnachweise

  Durch anerkannte Zertifizierungen wie etwa der ISO 27001 kann nachgewiesen werden, dass etwa ein Informationssicherheits-Managementsystem konform der ISO umgesetzt wurde. Auch Benaroch [34] hat in seiner Arbeit die Relevanz und die Anerkennung einer Zertifizierung für Informationssicherheit festgehalten. Eine Zusammenfassung dieser Arbeit befindet sich in Abschnitt 2.1.3. Darüber hinaus konnte bereits festgestellt werden, dass auch die DSGVO eine Zertifizierung als Nachweis für die Umsetzung der TOMs akzeptiert. Des Weiteren ist hier anzumerken, dass die Abfrage nach Zertifizierungen oftmals durch Punkt eins „Third-Party Questionnaires“ mitabgedeckt wird.

- Externe Auditberichte

  Viele IT-Dienstleister setzen oftmals bereits eigenständig auf externe IT-Audits, um die Compliance-Anfragen der Kunden effizienter bearbeitet zu können. Der Bericht eines seriösen Auditors kann ein guter Indikator für die Sicherheitslage eines Unternehmens sein. Derartige externe Audits kosten meist viel Geld und drängen betroffene Unternehmen automatisch zu höherer IT-Sicherheit. Wichtig ist darauf zu achten, welcher Bereich und Dienst auditiert wurde. [29]

	Third-Party Questionnaires	Risiko-Monitoring	Online Screening / Risk Rating	Vor-Ort-Audit	Schwachstellen-Scans/ Penetration Tests	Zertifizierungen	External Audit Reports
KSV1870 Nimbusec GmbH	X	X	X	X			
Deloitte	X		X				
Ernst & Young Global Limited		X		X			
Guidepoint Security	X	X	X			X	
Schneider Downs Consulting	X						
Kroll	X	X	X		X		
RSI Security					X		
Halock	X	X		X	X		X
CyberSecOp Consulting	X	X	X				
Ergebnis	**7**	**6**	**5**	**3**	**3**	**1**	**1**

Tabelle 11: Auswertung öffentlicher Information der TPRM-Anbieter

In Tabelle 11 werden die Ergebnisse der Auswertung tabellarisch dargestellt und somit aufgezeigt, wie die TPRM-as-a-Service-Anbieter die Risikobewertung durchführen. Das „Third-Party Questionnaire“, zu Deutsch Fragebogen für Dritte, ist laut dieser Erhebung die am häufigsten eingesetzte Bewertungstechnik. Dadurch kann die Aussage von Pompon bestätigt werden: „der üblichste Weg zur Analyse des Third-Party-Risikos ist die Übermittlung einer Fragenliste“ [29].

4.3. CyberRisk Rating von KSV1870

Für diesen Abschnitt wurden die öffentlichen Informationen ausgewertet und zusätzlich wurde ein persönliches Gespräch mit dem CEO der KSV1870 Nimbusec GmbH (kurz: Nimbusec) geführt. Die persönliche Kommunikation mit CEO Alexander Mitter fand am 29. März 2022 im Rahmen einer virtuellen Besprechung statt. Auf Wunsch des Gesprächspartners wurde sowohl auf eine Aufnahme wie auch Transkription verzichtet. Die hier vorhandenen Informationen sind aber ohnehin meist durch öffentliche oder zur Verfügung gestelltes Dokumentationsmaterial dargelegt und wurden im Gespräch lediglich verifiziert. Andernfalls werden Hintergrundinformationen sichtlich hervorgehoben und dazu auf das persönliche Gespräch verwiesen.

Die Nimbusec wurde 2013 gegründet und befindet sich mit 74,50 % im Mehrheitseigentum der Firma KSV1870 Holding AG [63]. Beim Kreditschutzverband 1870 handelt sich um einen unabhängigen Gläubigerschutzverband in Österreich, der vor allem durch seine Bonitätsauskünfte und -beobachtungen bekannt ist. Das ursprüngliche Produkt der Nimbusec setzt auf Website-Sicherheit, das nach wie vor zur Verfügung steht und auch für das CyberRisk Rating herangezogen wird. Durch das Tool sollen Sicherheitsvorfälle wie unsichere Web-Konfiguration, Defacement oder Denylisting, die den öffentlichen

Webauftritt eines Unternehmens betreffen, erkannt werden. Das TPRM-Service, das hier im Fokus steht, befindet sich seit September 2020 im Praxiseinsatz. [64] Durch das CyberRisk Rating sollen Unternehmen eine einfache Möglichkeit erhalten, den Ansprüchen der DSGVO sowie der NIS nachzukommen, durch die, wie bereits in Absatz 3 beschrieben, ein Risikomanagement für Dienstleister, Lieferanten und Dritte gefordert wird. Laut Nimbusec ist es um ein durch die österreichische operative NIS-Behörde (Bundesministerium für Inneres) anerkanntes Verfahren für das Lieferantenrisikomanagement. [65] Dadurch stellen vor allem die Betreiber wesentlicher Dienste oder größere Unternehmen die Hauptkundengruppe der Nimbusec dar.

4.3.1. Ablauf

Prinzipiell kann jedes Unternehmen weltweit durch das CyberRisk Rating bewertet werden. Der Bewertungsablauf steht auf Deutsch und Englisch zur Verfügung. Die Abwicklung an sich erfolgt über ein Webportal der Nimbusec, auf das sowohl der Anforderer der Bewertung (Kunde) als auch der zu bewertende Lieferant entsprechenden Zugriff erhalten (in Abbildung 11 dargestellt). [64]

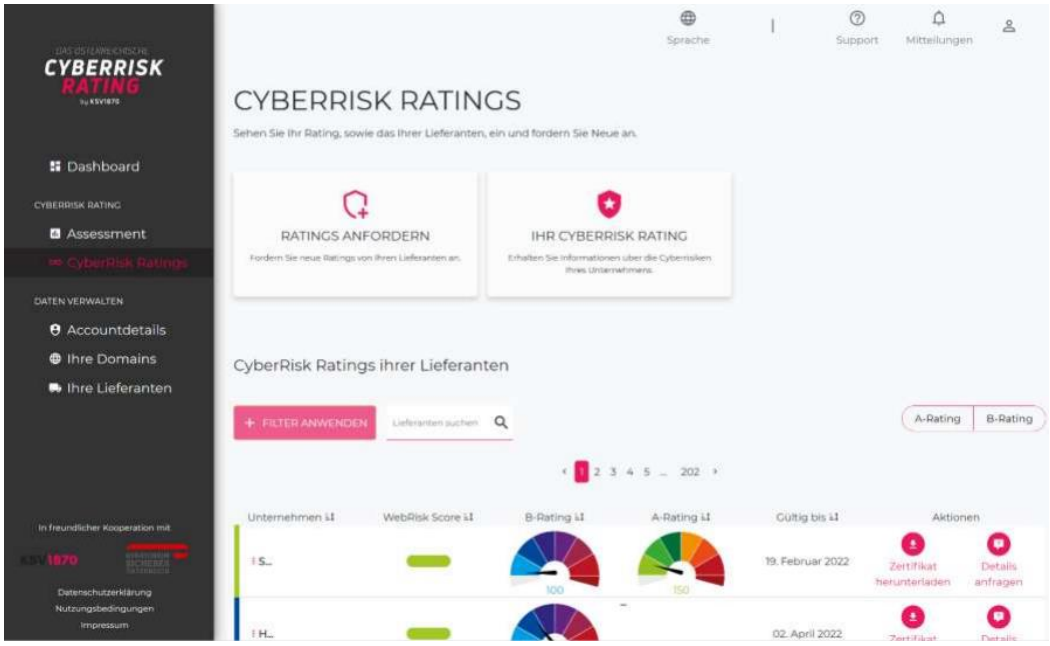

Abbildung 11: CyberRisk Rating Portal - Kundensicht [64]

Der Ablauf [64] [65] des CyberRisk Ratings sieht wie folgt aus:

- 1 - Kunde: Bekanntgabe der zu bewerteten Lieferanten
- 2 - Nimbusec: Web-Risk Score (C Score) wird erhoben
- 3 - Kunde: Auswahl der Lieferanten für das Rating
- 4 - Nimbusec: Bewertungsprozess wird durchgeführt
  - 4.1: Kontaktierung des Lieferanten mit Online-Fragebogen
  - 4.2: Validierung der Antworten
  - 4.3: Korrekturmöglichkeit für den Lieferanten
  - 4.4: Endgültige Verifizierung der Antworten
  - 4.5 (Optional): Audit der Angaben

- 4.6: Dokumentation und Festlegung des CyberRisk Rating Scores
- 5 - Nimbusec: Löschung aller detaillierten Bewertungsunterlagen

In Folge werden die oben genannten Schritte konkreter beleuchtet.

Schritt 1

Zunächst ist es Aufgabe des Kunden, alle Lieferanten im Portal einzutragen. Hierzu steht auch eine Upload-Funktion zur Verfügung. [64]

Schritt 2

Für alle Lieferanten nimmt Nimbusec nun eine Vorevaluierung mithilfe des Web-Risk Indikators vor. Es besteht hierbei in einer Prüfung mittels Tools aus der Nimbusec-Eigenentwicklung, mit denen die öffentliche Webseite auf nicht-intrusive Weise überprüft wird. Alexander Mitter macht im Gespräch nochmals klar, dass es sich hier lediglich um einen Indikator handelt, der kaum Rückschlüsse auf die gesamte IT-Sicherheit des Unternehmens zulässt (A. Mitter, persönliche Kommunikation, 25. März 2022). Deshalb hat der Web-Risk Score auch keinen direkten Einfluss auf das Rating des Unternehmens und wird separat für den Auftraggeber ausgewiesen. [65]

Schritt 3

Im Schritt 3 werden die Lieferanten, die den CyberRisk Rating Prozess durchlaufen sollen, ausgewählt. Bei Bedarf unterstützt Nimbusec den Kunden, sie risikobasiert auszuwählen. Nimbusec setzt dazu auf mehrere Modelle, mit denen die Kritikalität der Lieferanten bestimmt werden soll (A. Mitter, persönliche Kommunikation, 25. März 2022). Aus der Kritikalität wird auch die Anforderung beziehungsweise das notwendige Rating des Lieferanten abgeleitet. Dazu stehen die folgenden drei Stufen zur Verfügung: [64] [65]

- B Rating – Basissicherheitslevel

  Zur Erreichung des B Ratings muss ein Basissicherheitslevel durch den Lieferanten nachgewiesen werden. Laut Verfahren handelt es sich dabei um Anforderungen für ein grundlegendes Schutzniveau, das von jeder Organisation (auch von kleinen) erfüllt werden kann. Die Bewertungsmethode ist ein Self-Assessment. Nachweise sind nur im Bedarfsfall vorzulegen. Die Anforderungen werden durch eine Beschreibung der eingesetzten Kontrollen sowie der Nennung existierender Nachweise dargestellt. Aktuell gibt es 14 Anforderungspunkte. [65]
- A Rating – Fortgeschrittenes Sicherheitslevel

  Zur Erreichung des A Ratings muss ein fortgeschrittenes Sicherheitslevel durch den Lieferanten nachgewiesen werden. Die Bewertungsmethode und auch das Vorgehen sind ident zum B Rating. Der Fragen- beziehungsweise Anforderungskatalog erweitert sich jedoch: aktuell gibt es elf zusätzliche Anforderungen. [65]
- A+ Rating – Fortgeschrittenes Sicherheitslevel

  Zur Erreichung des A+ Ratings muss ident zum A Rating ein fortgeschrittenes Sicherheitslevel durch den Lieferanten nachgewiesen werden. Hierbei kommt jedoch ein unabhängiges Audit durch eine qualifizierte Stelle zum Einsatz, die die Anforderung aus dem A Rating überprüft. Im Sinne der NIS ist eine qualifizierte Stelle dazu berechtigt, Sicherheitsvorkehrungen bei Betreibern wesentlicher Dienste zu überprüfen. Die Auditoren führen dabei ein sogenanntes „third-party conformity assessment“ durch. Dabei gilt es, dem Auditor die geforderten Nachweise vorzulegen und plausibel zu machen. Der Auditor muss zu jeder Anforderung festhalten, inwiefern diese durch die Organisation erfüllt wird. Die Letztentscheidung liegt beim Auditor. [65]

Schritt 4

Die im Schritt 3 ausgewählten Lieferanten inklusive Anforderungsstufe werden nun in den Bewertungsprozess gesendet. Hierin besteht das Herzstück der Dienstleistung von Nimbusec. Zunächst wird geprüft, ob bereits ein Rating für das betroffene Unternehmen in der Datenbank vorliegt. Laut Nimbusec befinden sich aktuell rund 1500 bewertete Unternehmen in der Datenbank (A. Mitter, persönliche Kommunikation, 25. März 2022). Sofern es noch keinen Eintrag gibt, wird das betroffene Unternehmen via E-Mail gebeten, den entsprechenden Fragebogen auszufüllen. Sofern es sich um ein A+ Rating handelt, wird eine qualifizierte Stelle mit dem Audit beauftragt. [65]

Wenn das Unternehmen einer Bewertung zustimmt, erhält es einen Link zum Portal, wo (1) die Anforderung als umgesetzt oder nicht umgesetzt markiert wird und (2) bei Vorhandensein die Umsetzung beschrieben werden muss. [65]

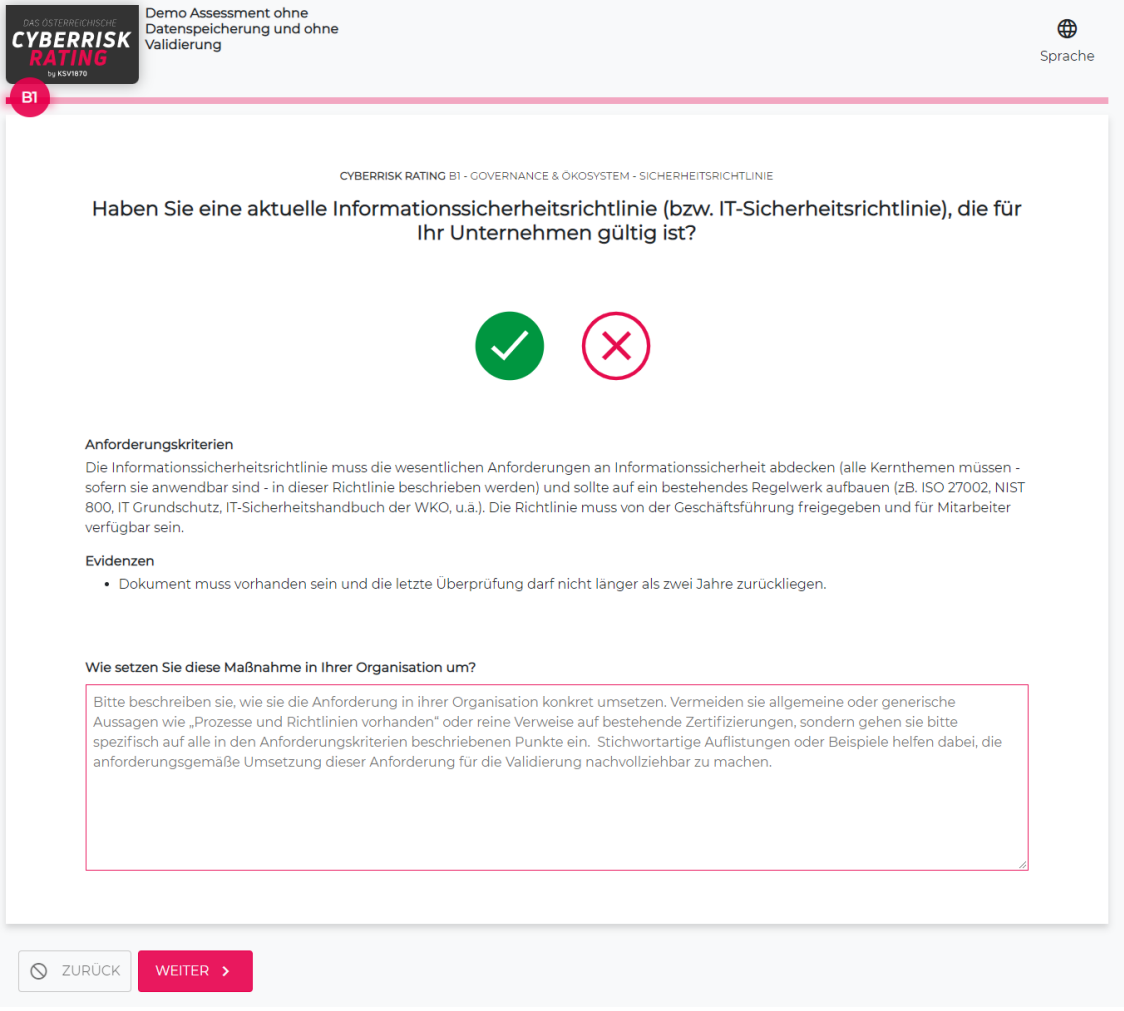

Abbildung 12: CyberRisk Rating Online-Fragebogen (demo.cyberrisk-rating.at)

Sollte das Unternehmen nach dreimaliger Kontaktaufnahme nicht reagieren, wird die Geschäftsleitung mit einem eingeschriebenen Brief über die Sachlage informiert und zur Teilnahme eingeladen. Sollte es auch hier innerhalb von zwei Wochen keine Rückmeldung geben, erhält das Unternehmen ein „Null-Rating", welches dem Kunden gemeldet und so auch in der Datenbank abgelegt wird. [65]

Sobald der Fragebogen ausgefüllt wurde, startet der Validierungsprozess. Die Antworten werden dabei durch die Cyber Trust Services GmbH validiert. Tätig dabei sind Personen mit mindestens einer gängigen Personenzertifizierung im Bereich Cybersicherheit sowie mindestens 3 Jahren Berufserfahrung in diesem Bereich. Nach der Validierung hat der Lieferant die Möglichkeit, die Antworten noch einmal zu korrigieren. Danach wird die Rückmeldung endgültig verifiziert. Im Rahmen der Validierung werden stichprobenartig Audits durch qualifizierte Stellen eingesetzt. Dasselbe gilt auch bei Verdacht auf Unregelmäßigkeiten. Die bewertete Organisation muss daher jederzeit in der Lage sein, die im Self-Assessment angegeben Nachweise liefern zu können. [65]

Auf Basis der erfüllten und verifizierten Anforderungen ergibt sich ein Rating-Score für das Unternehmen. Dieser reicht wie beim KSV1870 üblich von 100 (beste Bewertung – minimales Risiko) bis 700 (schlechteste Bewertung – höchstes Risiko). [65]

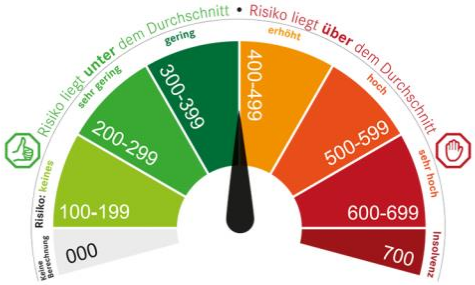

Abbildung 13: CyberRisk Rating Score durch KSV1870 Nimbusec GmbH

Das Bewertungsergebnis wird dem Kunden wiederum im Webportal zur Verfügung gestellt. Die Bewertungsdaten und -details erhält der Auftraggeber jedoch nicht. Diese müssten bei Bedarf direkt beim entsprechenden Lieferanten eingeholt werden, wodurch das bewertete Unternehmen die volle Kontrolle über die Bewertungsdaten behält. Das Rating ist für ein Jahr gültig. [65]

Schritt 5

Sobald das finale Rating vorliegt, werden alle Bewertungsdaten der bewerteten Organisation verschlüsselt und signiert zugesendet. Zwei Wochen nachdem diese durch die Organisation heruntergeladen wurden, werden diese bei Nimbusec gelöscht. In Falle eines A+ Ratings oder Stichprobenaudits werden Auditoren mittels Code-of-Conduct dazu verpflichtet, ebenfalls alle Unterlagen nach Abschluss des Audits zu löschen. [65]

4.3.2. CyberRisk Rating Schema

Zur Wahrung des Schemas wurde ein eigenes Governance Modell aufgestellt. Als Eigentümer fungiert das Kuratorium Sicheres Österreich (KSÖ), das zur Erhöhung der Cybersicherheit in Österreich verpflichtet ist. Das KSÖ hat dazu ein Cyber Risk Advisory Board aufgestellt, das durch acht Vertreter aus den unterschiedlichen NIS-Sektoren für Betreiber wesentlicher Dienste besetzt ist. So findet sich dort jeweils ein Vertreter aus dem Bereich Banken, Gesundheit, Finanzmarktinfrastruktur, Digitale Infrastruktur, Energie, Trinkwasser, Verkehr und Öffentliche Verwaltung. Dadurch soll sichergestellt werden, dass das CyberRisk Schema entsprechend gestaltet und auch weiterentwickelt wird. Das Cyber Risk Management Board übernimmt die operative Steuerung und setzt sich ebenfalls aus mehreren Parteien zusammen: KSV1870, KSÖ und Cyber Trust Services GmbH. [65]

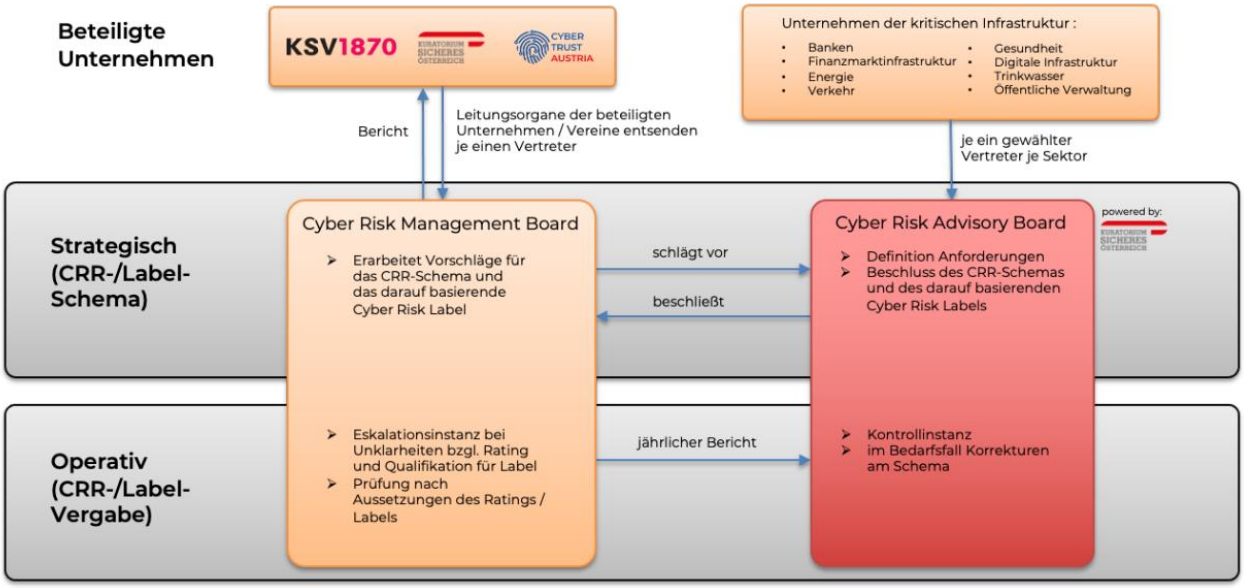

Abbildung 14: CyberRisk Rating Governance Modell [65]

4.4. Fazit zu TPRM-as-a-Service

Vor allem die zahlreichen Regulatoren haben Unternehmen dazu gedrängt, das Thema TPRM aktiv anzugehen und entsprechende Konformität zu etablieren. Wie aber bereits in der Einführung dieses Kapitels erwähnt, ist eine Umsetzung mit internen Ressourcen für viele Unternehmen oftmals schwierig zu stemmen beziehungsweise entsprechende Fachexpertise und Erfahrung beim Aufbau eines TPRM wertvoll. Gerade deshalb hat sich ein Markt gebildet, in welchen sowohl Software- wie auch Dienstleistungslösungen für TPRM angeboten werden. So finden sich neben US-Anbietern auch in Österreich mindestens drei Unternehmen, welche eine Art TPRM-as-a-Service im Bereich der Informationssicherheit anbieten. Speziell die KSV1870 Nimbusec GmbH hat sich auf diese Thematik spezialisiert und unter Einbindung verschiedenster Partner, ein praxistaugliches Bewertungsverfahren von Dritten etabliert, das international eingesetzt werden kann. Nimbusec bietet Unternehmen durch das CyberRisk Rating eine Möglichkeit, die Risikobewertung von Dritten auszulagern, wodurch der interne Aufwand für TPRM minimiert werden kann. Dabei wird die Kritikalität der Lieferanten in Form von unterschiedlichen Anforderungsstufen berücksichtigt. Darüber hinaus untermauert der Abschnitt die wissenschaftliche Aussage, nach der der Fragebogen aktuell die am häufigsten eingesetzte Form der Bewertungsmethoden ist.

5. Modell zur Risikobewertung Dritter

Die hohe Relevanz von TPRM wurde bereits mehrfach unterstrichen. Zusätzlich fordern Regulatorien aus unterschiedlichen Intensionen, dass Unternehmen ihre Dritten entsprechend überprüfen und die IT-Sicherheit berücksichtigen. Doch in der Wissenschaft, in Frameworks und auch in Regulatorien sind kaum konkrete Anweisungen für die Umsetzung eines TPRM zu finden. Zumeist sind es Beratungsunternehmen, die diese Lücke erkannt haben und etwa mit TPRM-as-a-Service werben.

In diesem Abschnitt soll diese Lücke im wissenschaftlichen Bereich gefüllt werden, indem ein Modell für Unternehmen geboten wird, durch das die Risikobewertung Dritter möglichst holistisch umgesetzt werden

kann. Dazu werden einerseits die möglichen Bewertungsmethoden beschrieben und eingeordnet, andererseits ein generischer TPRM-Prozess vorgestellt. Als Basis dafür dient der untersuchte Stand der Wissenschaft mit Publikationen und Frameworks, Informationen aus Regularien wie auch TPRM-as-a-Service Ansätzen. Darüber hinaus fließen in diesen Absatz auch Vorgehensweisen führender Technologien im Bereich TPRM mit ein, die in diesem Abschnitt zusätzlich untersucht wurden.

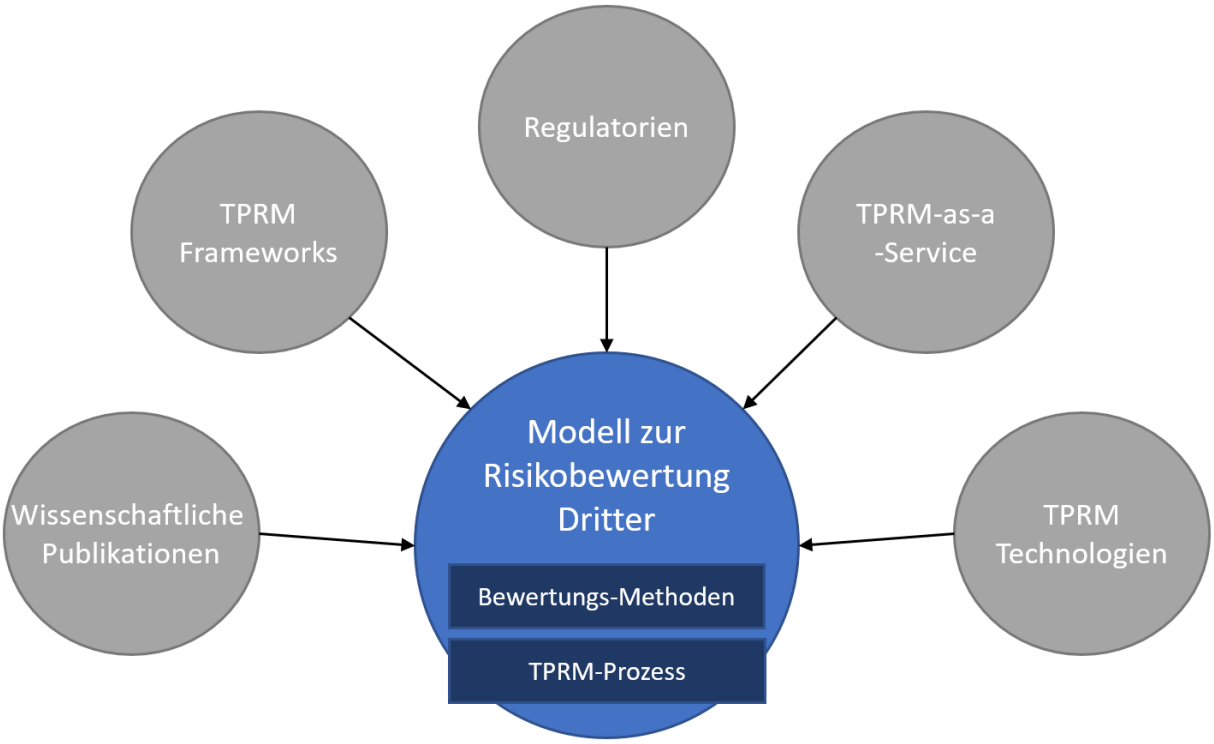

Abbildung 15: Input für das Modell zur Risikobewertung von Dritten

5.1. Risikobewertungs-Methoden

Für die Risikobewertung Dritter können viele unterschiedliche Methoden verwendet werden. In Zuge dieser Arbeit wurden bereits Techniken aus der Literatur, Standards und Frameworks, Regularien und TPRM-as-a-Service-Anbietern erhoben und betrachtet. Um in diesem Absatz nun einen Methoden-Überblick liefern zu können, wurden zusätzlich noch zwei laut Gartner [16] führende TPRM-Tool-Anbieter (Prevalent und OneTrust) betrachtet und deren eingesetztes Vorgehen untersucht. Prevalent stellt online eine Vielzahl an Dokumenten zu TPRM zur Verfügung [66] [67] [68]. Mit OneTrust wurde ein persönliches Gespräch geführt, um mehr über deren Bewertungsablauf zu erfahren.

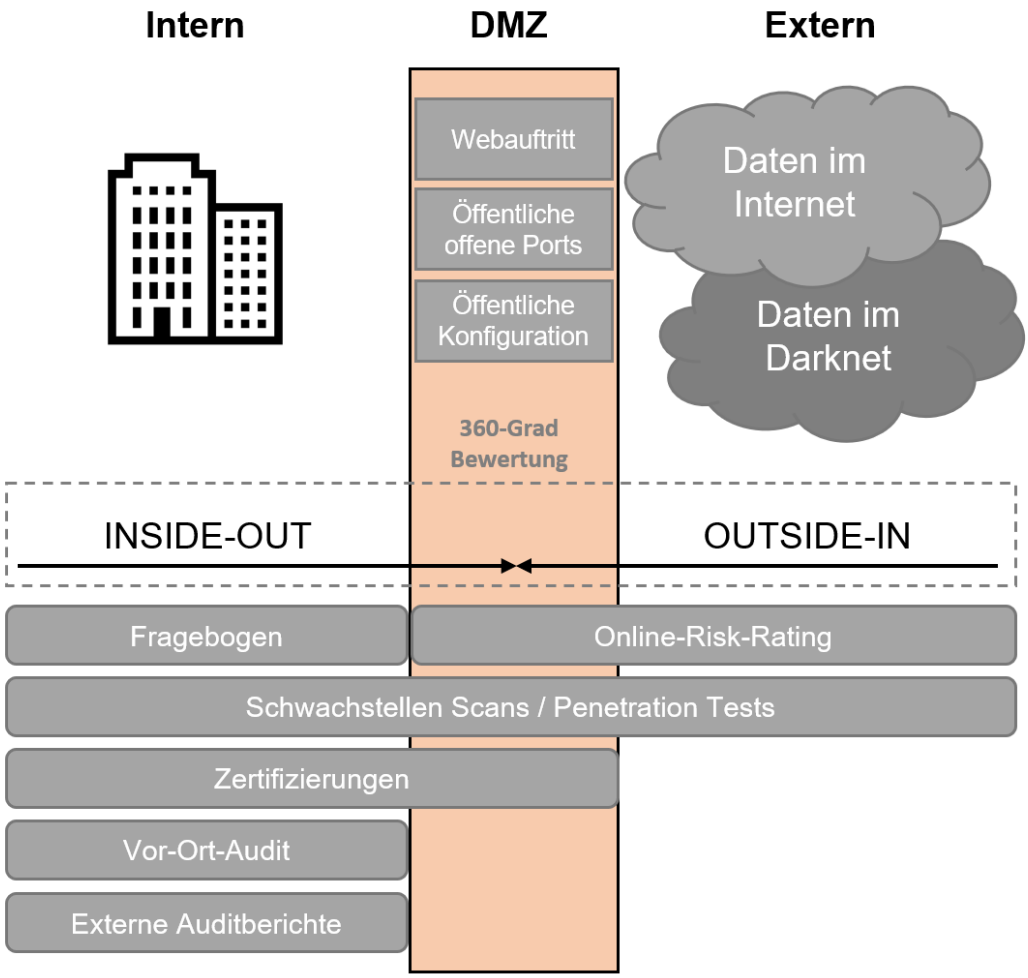

Abbildung 16: 360-Grad Bewertung durch Inside-out und Outside-in Techniken

Wie in Abbildung 16 ersichtlich können TPRM-Bewertungs-Methoden in „Inside-out“ und „Outside-in“ Methoden eingeteilt werden. Die Einteilung und Bezeichnung von Inside-out und Outside-in sind bereits in Artikeln von Prevalent zu finden [66]. Die Darstellung oben, wie auch die Zuordnung der Methoden, wurde jedoch in Zuge dieser Arbeit definiert. Dazu werden die Methoden durch den Standpunkt kategorisiert, aus dem eine Bewertung durchgeführt wird. So wird bei einer Outside-in-Bewertung versucht, ein Unternehmen von außen zu bewerten. Die dafür bekannteste Methodik ist das Online-Risk-Rating beziehungsweise Online-Risk-Scoring, bei dem auf öffentlich zugängliche Daten im Internet und auch dem Darknet zugegriffen wird. Durch Fragebögen, Vor-Ort-Audits oder Auditberichte kann diese externe Betrachtung ergänzt werden, wobei man von Inside-out-Bewertungen spricht. Eine möglichst holistische Bewertung ergibt sich durch die Kombination von Methoden aus beiden Bewertungskategorien, wodurch eine sogenannte 360-Grad-Bewertung erreicht werden kann [67].

Fragebogen

Bei der am häufigsten eingesetzten Bewertungstechnik des Fragebogens müssen zumindest die folgenden Punkte definiert werden [66]:

- Welcher Fragebogen kommt für die Bewertung zum Einsatz? Wird ein Industrie-Standard verwendet oder kommt ein eigener Fragebogen zum Einsatz?

- In welcher Form werden Nachweise eingeholt? Muss der Lieferant die eigenen Angaben durch Nachweise bestätigen? In welchem Umfang müssen Nachweise zur Verfügung gestellt werden? Wie werden diese Nachweise validiert?

Der eingesetzte Fragebogen zur Beurteilung eines Lieferanten spielt eine wesentliche Rolle und sollte daher sorgfältig ausgewählt werden. Hierbei gilt es auch, zu entscheiden, ob alle Dienstleister mit demselben Fragebogen beurteilt oder angepasste Fragebögen verwendet werden. Vor- und Nachteile ergeben sich aus beiden Szenarien. So erhält man bei einem gleichbleibenden Fragebogen eine gewisse Konsistenz und die Möglichkeit des direkten Vergleichs aller Dritten. Darüber hinaus können beim Einsatz standardisierter Fragebögen die Antworten aus Dienstleistersicht wiederverwendet und auch für andere Partner herangezogen werden. Auf der anderen Seite sind Lieferantenbeziehungen höchst unterschiedlich. Es gibt kritischere und weniger kritische Dritte. Außerdem sind gewisse Themenbereiche im Fragebogen nicht für alle relevant, woher Ineffizienz und erhöhter Aufwand entstehen. [66]

Sowohl in der Publikation der NIST [4], in Dokumenten von Prevalent [67] als auch im persönlichen Gespräch mit dem Vertrieb von OneTrust wird der Standard Information Gathering Fragebogen (SIG Fragebogen) immer wieder erwähnt. Es handelt sich dabei um einen kommerziellen Fragebogen des Unternehmens *Shared Assessments*. Laut eigenen Angaben wird der entwickelte Fragebogen zur Bewertung Dritter von mehr als 15.000 Organisationen weltweit eingesetzt [69]. Als prominentes Referenzunternehmen setzt auch Google den SIG Fragebogen ein und stellt die Ergebnisse für Google-Cloud-Kunden auf Anfrage zur Verfügung [70]. Zum aktuellen Zeitpunkt (16.04.2022) wird der SIG Fragebogen für 4000 Dollar angeboten. Der Fragebogen deckt dabei die folgenden 18 Risikobereiche ab:

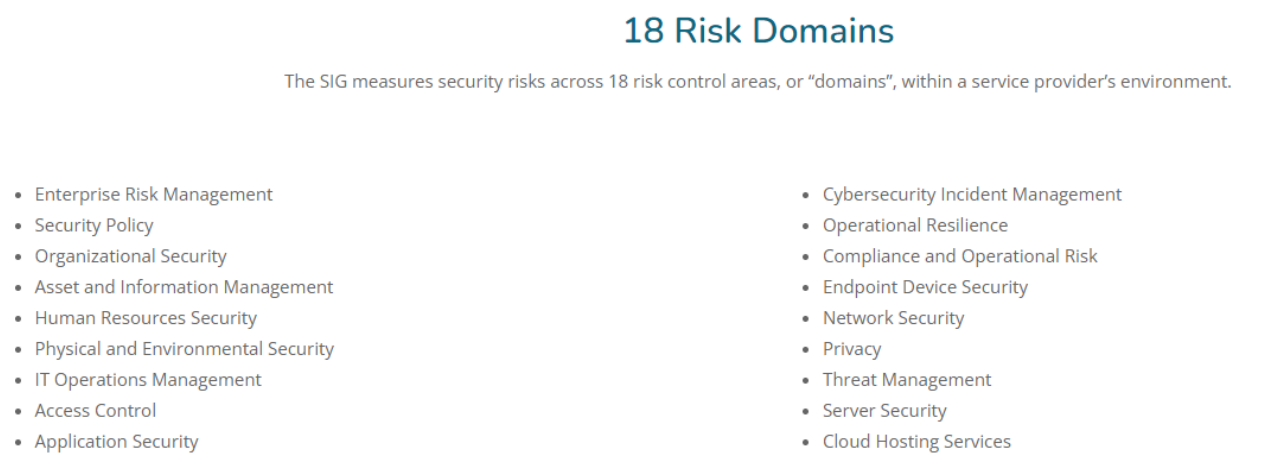

Abbildung 17: SIG Fragebogen von Shared Assessments - 18 Risikobereiche

Ein genereller Nachteil von Fragebögen ist die fehlende Verifizierung der Angaben durch den Dritten. Wie bereits erwähnt schreibt Viega [6], dass es ein Fehler wäre, sich auf die Angaben der Lieferanten in einem Self-Assessment blind zu verlassen, denn nach eigenen Erfahrungen wurden Lieferanten beobachtet, die in der Selbsteinschätzung zu Sicherheitskontrollen falsche Angaben gemacht haben. Für diese notwendige Verifizierung ergeben sich nun unterschiedliche Möglichkeiten. Beim CyberRisk Rating von KSV1870 wird primär auf Nachweise verzichtet und stattdessen auf eine ausführliche Beschreibung der abgefragten Sicherheitskontrollen durch den Lieferanten gesetzt. Anhand der detaillierten Beschreibung durch den Dritten, in Kombination mit entsprechend erfahrenen Personal für die Verifizierung, soll ein hohes Maß an Garantie für die Angaben erreicht werden. Andere verlassen sich hingegen bei der Validierung ausschließlich auf Nachweise in Form von Dokumenten je Frage und fordern stattdessen keinerlei Beschreibung. Auch klassische Audits setzen auf vollständige oder stichprobenartige Nachweise für angegebene vorhandene Kontrollen. In diesem Punkt unterscheiden sich daher die Ansätze in der Praxis

und auch durch Regulatorien gibt es keine konkreten Vorgaben. So wurde auch der Nachweis-freie-Ansatz der KSV1870 durch die NIS-Behörde zur Erfüllung der NIS-Gesetzes-Anforderungen für Lieferantenrisiken als konform bestätigt [71]. Es ist jedoch wichtig, hier einen Ansatz zu wählen, durch welchen die Angaben der Lieferanten verifiziert werden können.

Online-Risk-Rating

Beim Online-Risk-Rating handelt es sich um ein Outside-in-Verfahren, welches den Fragebogen ergänzen kann. Die Methodik wurde bereits in Absatz 4.2 näher beschrieben und auch im Literatureinblick durch die Arbeit von Keskin et al. [14] grundlegend beschrieben. An dieser Stelle findet sich noch eine Übersichtsbewertung durch das Tool SecurityScorecard [72]. Wie in Abbildung 18 zu erkennen, werden durch das Tool zehn Bereiche mit einem Ratingscore versehen. Die Bereiche, das Bewertungsschema und die verwendeten Daten unterscheiden sich von Tool zu Tool.

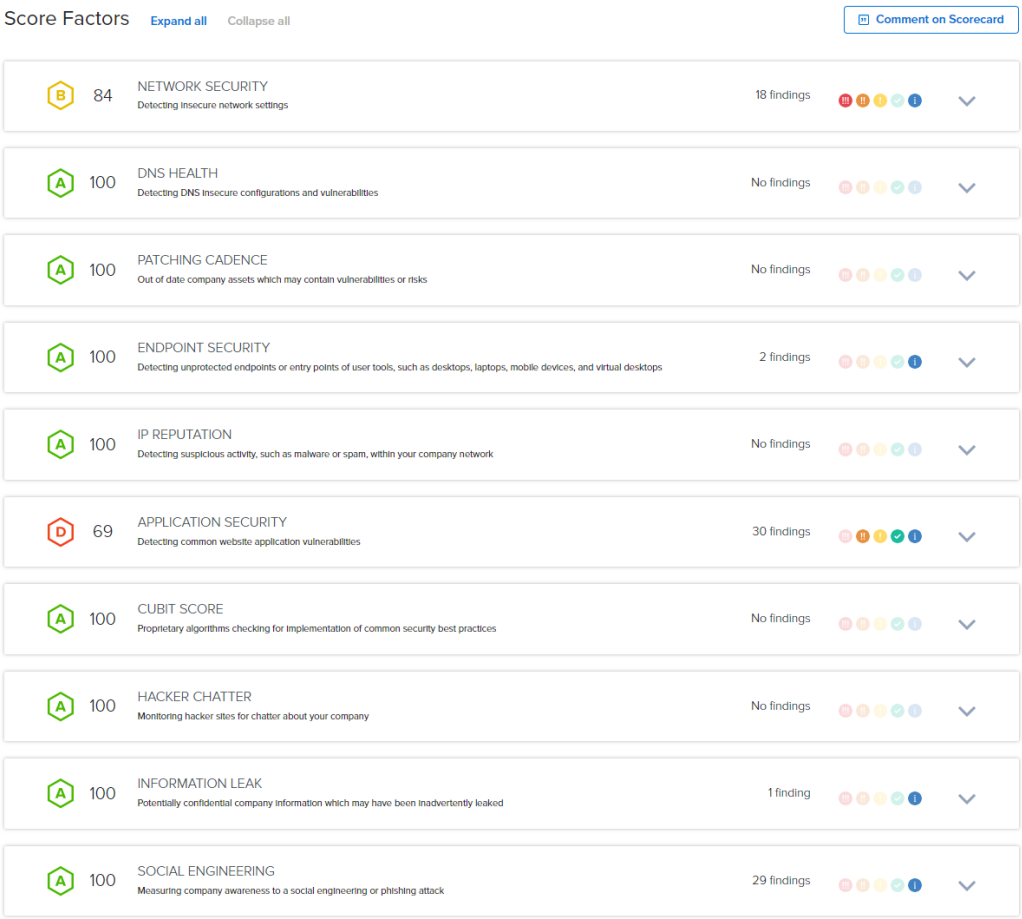

Abbildung 18: Beispiel für ein Online-Risk-Rating Tool (SecurityScorecard)

Schwachstellen Scans und Penetration Tests

Diese Methodik kann sowohl als Outside-in- wie auch als Inside-out-Technik genutzt werden. So ergibt sich die Möglichkeit, dass das nicht-invasive Online-Risk-Rating durch einen aktiven Schwachstellen-Scan von außen ergänzt wird. Darüber hinaus können interne Schwachstellen-Scans und ihre Ergebnisse für die Beurteilung herangezogen werden. Auch der Einsatz eines Penetration-Tests für ein dediziertes System oder Produkt, das womöglich vom Lieferanten bezogen wird, kann für die Beurteilung relevante Informationen liefern. Diese Methodik sollte jedoch nicht als Einzelbewertungstechnik, sondern vielmehr als ergänzende Informationsquelle eingesetzt werden.

Zertifizierungen
Zertifizierungen nehmen im TPRM eine wichtige Rolle ein. Dies stellt auch Benaroch [34] in seiner Arbeit fest. So werden diese in der DSGVO explizit als Möglichkeit zur Nachweiserbringung der vorhandenen technischen und organisatorischen Maßnahmen erwähnt. Auch die ISO 27036 [38], die in Absatz 2.2.1 beschrieben wurde, weist auf eine Zertifizierung (konkret die ISO 27001) als Nachweis über das pro-aktive Management der Informationssicherheit hin. Das haben auch Anbieter von Cyberversicherungen wahrgenommen, für die Zertifizierungen eine wesentliche Rolle spielen [22]. In Abbildung 16 wurde die Methodik primär als Inside-out eingeordnet, erstreckt sich aber auch über die Schnittstelle hin zu Outside-in, da Zertifizierungsnachweise oftmals öffentlich ausgewiesen werden und daher auch bei der Beurteilung von außen direkt berücksichtigt werden können. Vorhandene Zertifizierungen wie ISO 27001, SOC 2[13] oder auch TISAX[14] bescheinigen, dass das Unternehmen entsprechende Maßnahmen zur Wahrung der Informationssicherheit ergriffen hat und dies unabhängig überprüft wurde. So handelt es sich bei SOC 2 um einen Prüfungsstandard für Outsourcing, der durch das amerikanische Institut für Wirtschaftsprüfer zur Verfügung gestellt wird. Bei einer SOC 2 Zertifizierung wird durch einen externen Auditor das IT-Rechenzentrum in Bezug auf Sicherheit, Verfügbarkeit, Integrität, Vertraulichkeit und Datenschutz geprüft [73]. Bei TISAX hingegen handelt es sich um einen branchenspezifischen Prüf- und Austauschmechanismus in der Automobilindustrie. Dieser soll die IT-Sicherheit zwischen Autoherstellern und ihren Dienstleistern und Lieferanten sicherstellen [74]. Auch der KSV1870 gemeinsam mit der Cyber Trust Services GmbH versucht, eine Art branchenunabhängige Zertifizierung in Form des Cyber Trust Labels zu etablieren. So kann ein Unternehmen mit entsprechendem CyberRisk Rating das *Cyber Trust Label* oder das *Cyber Trust Label Gold* anfordern [65]. Dadurch wiederum sollen andere Organisationen direkt erkennen können, dass das Unternehmen ein gewisses Maß an IT-Sicherheit erfüllt.

Vor-Ort Audit
Beim Vor-Ort Audit handelt es sich um eine Inside-out Methodik. Diese Beurteilung kann den Fragebogen sowohl ergänzen wie auch ersetzen. Der KSV1870 stellt das Vor-Ort oder auch Remote-Audit durch qualifizierte Stellen zur Verfügung, das für kritischste Dienstleister und Lieferanten empfohlen wird. Weitere Details finden sich dazu in Absatz 4.2 und Absatz 4.3.1.

Externe Auditberichte
Externe Auditberichte liegen meist nicht öffentlich vor, daher wird diese Methodik als Inside-out eingeordnet. Es obliegt daher den Bewerteten diese Auditberichte zur Verfügung zu stellen. Die Relevanz solcher Berichte für die Beurteilung wurde bereits in Absatz 4.2 hervorgehoben. So liefert etwa ein SOC 2 Bericht wesentliche Informationen [73] über einen Dritten:

- Beschreibung des internen Kontrollsystems
- Beurteilung des Kontrolldesigns in Hinblick auf Angemessenheit und Ziele
- Wirksamkeit der Kontrollen inklusive Testszenarien und Ergebnisse

Sofern derartige unabhängige Auditberichte vorliegen, können diese für die Beurteilung herangezogen werden.

5.2. Allgemeiner TPRM-Prozess

In Zuge dieser Arbeit wurden sowohl im Absatz 2.2 (ISO/IEC 27036, NIST SP 800-161, ISO/IEC 27005, NIST CSF) wie auch im Absatz 4.3 (KSV1870 CyberRisk Rating) bereits einige TPRM-Frameworks und -Prozesse beschrieben. Ziel dieses Abschnitts ist es, einen generischen und allgemein gültigen, jedoch konkreten und praxistauglichen TPRM-Prozess vorzustellen. Dazu wurden noch weitere öffentliche Frameworks, Prozesse und Methoden für das TPRM gesichtet und berücksichtigt (Tabelle 12). Diese

[13] Service Organization Control 2 (SOC2)
[14] Trusted Information Security Assessment Exchange (TISAX)

stammen aus Unternehmen, die TPRM-Software-Lösungen anbieten oder bei der TPRM-Umsetzung als Beratungsunternehmen unterstützen:

Autor / Unternehmen	Organisationtype	Titel
Prevalent	TPRM-Software-Lösung	Six Steps to Complete Third-Party Risk Management [67]
Prevalent	TPRM-Software-Lösung	Navigating the Vendor Risk Lifecycle: Keys to Success at Every Stage [66]
Prevalent	TPRM-Software-Lösung	Third-Party Profiling & Tiering Template [68]
OneTrust	TPRM-Software-Lösung	Third-Party Risk Management Demo
ISACA	Consulting	A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance [75]
Ernst & Young	Consulting	Developing a Successful GRC Third Party Risk Management Program by Understanding Strategies and Industry Trends [76]

Tabelle 12: TPRM-Frameworks, -Prozesse und -Methoden aus dem Software- und Beratungsbereich

Auch wenn sich alle untersuchten Ansätze in gewissen Punkten voneinander unterscheiden, sind die TPRM-Themen, die zu berücksichtigen sind, immer ähnlich.

In Abbildung 19 wird der erarbeitete generische TPRM-Prozess zunächst grafisch dargestellt. Dieser setzt sich aus sechs Prozessschritten zusammen, die in den folgenden Unterabschnitten näher beschrieben werden.

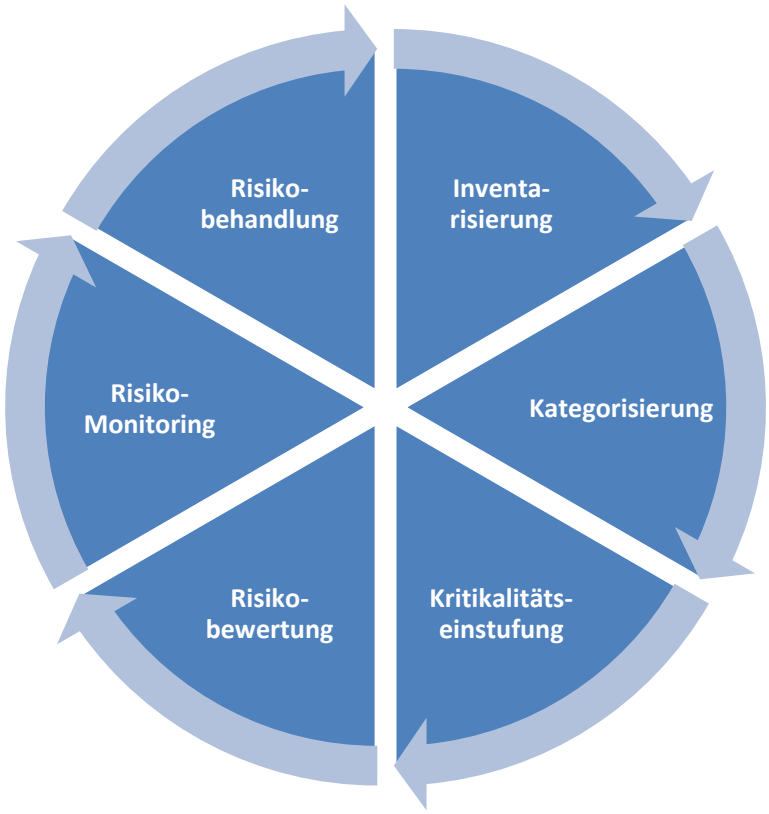

Abbildung 19: Generischer TRPM-Prozess

5.2.1. Third-Party Inventarisierung

Im ersten Schritt wird darauf geachtet, alle relevanten Dritten zu identifizieren. Diese doch einfach klingende Aufgabe kann aber auch direkt eine große Herausforderung darstellen. Denn es stellt sich die Frage: Wer sind meine Lieferanten und Dienstleister und welche davon sind für das TPRM in Bezug auf IT-Sicherheit von Relevanz. Verschärft wird diese Herausforderung dadurch, dass bekannte Frameworks (auch die NIST SP 800-161 [11]) oder auch TPRM-as-a-Service Anbieter (etwa KSV1870 startet mit dem Upload aller Lieferanten) diesen ersten Schritt als Voraussetzung und daher „Out-of-Scope“ sehen. Je nach Organisation ergibt sich hier eine andere Ausgangssituation. So sollte zunächst geprüft werden, ob nicht bereits eine Lieferantenliste aufgrund eines übergeordneten Third-Party Risk Managements besteht. Demzufolge sollten andere Abteilungen befragt werden, welche ebenfalls für ein TPRM oder Lieferantenmanagement in Fragen kommen. Dazu zählen abseits von IT und IT-Sicherheit vorneweg die Einkaufs-, Compliance- wie auch Rechtsabteilung. Sofern eine derartige Inventarisierung noch nicht stattgefunden hat, können Rechnungs- und Zahlungsdaten, Vertragsverwaltungsdatenbanken oder das Enterprise Resource Planning (ERP) System als erste Basis dienen. Es sollte eine Echtzeit-Datenbank der Dritten geschaffen werden, in der Informationen aus verschiedensten Systemen vereint, sowie neue Dritte hinzugefügt und alte zeitnah entfernt werden. [76]

Output: Echtzeit-Third-Party-Datenbank

5.2.2. Third-Party Kategorisierung

Nicht alle Drittunternehmen sind gleich und auch nicht alle sind für das TPRM relevant. Es ist daher wichtig, dass Dritte segmentiert werden, um diese anschließend aus einer Risikobetrachtung beurteilen zu

können. Dies ist vor allem dann relevant, wenn die Liste der Dritten, wie in großen Unternehmen üblich, lang ist. Laut Ernst and Young [76] gibt es Unternehmen, die mit einer Liste von mehr als 5000 Dritten konfrontiert sind. In der Kategorisierung sollten zumindest die folgenden Punkte [75] berücksichtigt werden:

- Art der Geschäftsbeziehung

  Um welche Art Geschäftsbeziehung handelt es sich beziehungsweise welche Leistung wird durch den Dritten erbracht? Werden durch den Dritten Produkte zur Verfügung gestellt oder eine Dienstleistung erbracht?
- Einfluss auf Kernprozesse

  Wie kritisch ist der Dritte für die Kernprozesse des Unternehmens? Wie kritisch sind die Produkte oder Dienstleistungen des Dritten für meine Produkte oder Dienstleistungen?
- Alleinstellungsmerkmal

  Handelt sich bei dem Dritten um den einzigen, der das Produkt oder Dienstleistung zur Verfügung stellen kann?
- Datenaustausch

  Welche Art von Daten (z. B. Unternehmensgeheimnisse, Finanzdaten oder Kartenzahlungsinformationen (PCI), personenbezogene Daten, Gesundheitsdaten) werden mit dem Dritten ausgetauscht?
- Form des Datenaustauschs

  Wie (z. B. Cloud, E-Mail, Secure File Transfer (SFTP)) werden die Daten mit dem Dritten ausgetauscht?
- Art des Dritten

  Um welche Art (z. B. öffentliche Einrichtung, Privatunternehmen, Regierung) Dritter handelt es sich? Je nach Organisation können sich unterschiedliche Compliance-Anforderungen ergeben.
- Formeller Vertrag

  Existiert ein formeller Vertrag mit dem Dritten, in dem auch Vertragsbestimmungen (SLAs) definiert wurden?
- Hosting-Standort

  Wo (z. B. Cloudbetreiber und Standort, beim Dritten, vor Ort) wird das Service betrieben?

Somit wird die TP-Inventarisierung um wesentliche Risikoinformationen erweitert, was wiederum eine Basis für die nächsten Schritte darstellt.

Output: Echtzeit-Third-Party-Datenbank inklusive Kategorisierungsinformationen

5.2.3. Third-Party Kritikalität – Risikoausgangslage

In diesem Schritt geht es darum, die Kritikalität der Dritten zu bestimmen. Oder anders ausgedrückt, wie hoch ist das Risiko, das sich durch die Geschäftsbeziehung mit dem Dritten für das eigene Unternehmen ergibt. Es geht hier explizit noch nicht darum, wie sicher der Dritte selbst ist. Dieser Zustand wird auch als Risikoausgangslage (im Englischen: „inherent risk“) bezeichnet. Es geht um das Risiko, das von einem Dritten ausgeht, bevor jegliche Maßnahmen ergriffen wurden. Dieser Faktor wird anschließend die eigentliche Risikobewertung und dessen Ausprägung beeinflussen. Zur Bestimmung der Kritikalität werden die Informationen aus dem Schritt der Kategorisierung herangezogen. Sowohl die NIST SP 800-161 [11] wie auch Prevalent [68] schlagen dazu vor, den Lieferanten ein Kritikalitätslevel nach vorgegebener Kritikalitätsmatrix zuzuweisen. Es handelt sich um eine qualitative Bestimmung. Die Kritikalitätsmatrix könnte wie folgt aussehen:

Kritikalität	Risikofaktoren
Hoch	• Der Dritte stellt ***Kernkomponenten*** für die eigenen Produkte und Dienstleistungen zur Verfügung. Der Ausfall des Produkts oder der Dienstleistung würde zu einem ***Totalausfall*** des Unternehmens oder einer erheblichen Beeinträchtigung führen. • Der Dritte ist ***der Einzige***, der das Produkt oder die Dienstleistung zur Verfügung stellen kann. • Der Dritte hat ***Zugriff auf sensible Informationen***.
Mittel	• Der Dritte stellt ***Komponenten*** für die eigenen Produkte und Dienstleistungen zur Verfügung. Der Ausfall des Produkts oder der Dienstleistung würde zu einem ***schweren Ausfall*** des Betriebs führen. • Der Dritte ist ***nicht der Einzige***, der das Produkt oder die Dienstleistung zur Verfügung stellen kann. • Der Dritte hat nur ***begrenzt Zugriff auf sensible Informationen***.
Niedrig	• Der Dritte stellt nur ***wenige oder keine Komponenten*** für die eigenen Produkte und Dienstleistungen zur Verfügung. Der Ausfall des Produkts oder der Dienstleistung hätte ***kaum Auswirkungen*** auf das Unternehmen. • Der Dritte ist ***nicht der Einzige***, der das Produkt oder die Dienstleistung zur Verfügung stellen kann. • Der Dritte hat ***Zugriff auf nicht sensible Informationen***.

Tabelle 13: Beispiel einer Kritikalitätsmatrix zur Einstufung der Dritten [11] [68]

Die Einstufung der Dritten wird in der Third-Party-Datenbank festgehalten.

Output: Kritikalitätseinstufung der Third-Parties

5.2.4. Third-Party Risikobewertung

Durch die vorhergehenden Schritte wurde die Basis für die eigentliche Risikobewertung geschaffen. So sollte an dieser Stelle eine Liste aller Dritten inklusive Kategorisierungsdaten und Kritikalitätsstufe vorliegen. Der folgende Ansatz zur Risikobewertung teilt sich in zwei Schritte:

- Schritt 1 - Analyse: Angepasst an die Kritikalität des Dritten werden umfangreichere Anforderungen abgeprüft und dazu unterschiedliche Methoden eingesetzt.
- Schritt 2 - Bewertung: Durch die identifizierten Abweichungen wird das Risiko je Dritten ermittelt.

Analyse
Im ersten Schritt der Risikobewertung, nämlich in der Analyse, werden bekannte und bereits vorgestellte Methoden angepasst an die Kritikalität des Partners eingesetzt. In welcher Form die Analyse zu erfolgen hat, wird am besten anhand einer Matrix definiert, die in Folge als Vorgabe dient.

Die Tabelle 14 stellt dazu einen möglichen Ansatz bereit. Dabei werden je Kritikalität zwei Analyseoptionen angeboten. Je nach Kritikalität des Dritten besteht die Analyse aus mindestens zwei bis hin zu vier Teilen. Grundlegend wird für jeden Dritten ein Online-Risk-Rating eingesetzt, wodurch der erste Teil für alle Dritten gegeben ist. Soll nun ein Dritter der Kritikalitätsstufe „Niedrig“ analysiert werden, so kann zwischen einem Fragebogen-Light oder dem Nachweis einer Zertifizierung gewählt werden. Beim Fragebogen-Light handelt es sich um einen definierten Fragebogen, der nur die grundlegenden Anforderungen der IT-Sicherheit abbildet. Die zugelassenen Zertifizierungen in Option 2, wie etwa eine ISO 27001, gilt es festzulegen.

Ähnliches gilt für Dritte der Stufe „Mittel“, die durch den Fragebogen-Standard oder den Nachweis mehrerer Zertifizierungen bewertet werden. Bei Unternehmen der höchsten Kritikalitätsstufe kommt ein dritter Analyseteil hinzu. In diesem kann zwischen einem Vor-Ort-Audit oder Sichtung eines unabhängigen externen Auditberichts gewählt werden. Bei allen Kritikalitätsstufen kann optional ein Schwachstellen-Scan oder Penetration-Test eingesetzt werden.

Kritikalität	Teil 1	Teil 2	Teil 3	Optional
Hoch Option 1	Online-Risk-Rating	Fragebogen-Full	Vor-Ort-Audit	Schwachstellen-Scan Penetration-Test
Hoch Option 2		Zertifizierungen	Externer Auditbericht	
Mittel Option 1	Online-Risk-Rating	Fragebogen-Standard		Schwachstellen-Scan Penetration-Test
Mittel Option 2		Zertifizierungen		
Niedrig Option 1	Online-Risk-Rating	Fragebogen-Light		Schwachstellen-Scan Penetration-Test
Niedrig Option 2		Zertifizierung		

Tabelle 14: Mögliche Matrix zur Risikoanalyse abhängig der Kritikalität des Dritten

Durch diesen Analyseansatz wird:

1) sichergestellt, dass immer sowohl eine Outside-in wie auch Inside-out Methode zum Einsatz kommt.
2) sichergestellt, dass die Analyse risikobasiert und möglichst effizient abgewickelt wird.
3) sichergestellt, dass immer zwei mögliche Analysepfade existieren, wodurch auch Dritte, für welche eine Methode nicht möglich ist oder sie diese verweigern (zum Beispiel das Vor-Ort-Audit), angemessen analysiert werden können.

Alle in der Matrix verwendeten Methoden wurden bereits im Absatz 5.1 beschrieben. Der eingesetzte Fragebogen wird dabei an die Kritikalität des Dritten angepasst. Er unterscheidet sich in der Anzahl der Fragen. So finden sich in diesem Vorschlag ein Fragebogen-Light, Fragebogen-Standard und Fragebogen-Full. Dadurch soll ein risikobasiertes sowie effizientes Vorgehen erreicht werden. Ein derartiger Ansatz ist auch im CyberRisk Rating [65] zu finden, wobei dort zwei Fragebögen eingesetzt werden. Im Basiskatalog der KSV 1870 werden 14 Anforderungen definiert, im fortgeschrittenen sind es 25.

Bewertung
Unabhängig der eingesetzten Methoden werden durch die Analyse Abweichungen oder auch sogenannte „Findings“ identifiziert. Diese Abweichungen gilt es nun, in den Kontext der Geschäftsbeziehung zu stellen und dabei die daraus möglichen Auswirkungen sowie die Wahrscheinlichkeit zu bestimmen. Hierzu kann der Ansatz der NIST SP 800-161 [11] verwendet werden, der bereits im Absatz 2.2.2 im Detail beschrieben wurde. Zunächst wird für jede Abweichung sowohl die Wahrscheinlichkeit als auch die Auswirkung bestimmt, woher sich eine Risikobewertung je Abweichung (Tabelle 15) ergibt.

Risikobewertung					
	Auswirkung				
		Niedrig	Mittel	Hoch	Kritisch
	Kritisch	Mittel	Hoch	Kritisch	Kritisch
	Hoch	Mittel	Hoch	Hoch	Kritisch
	Mäßig	Niedrig	Mittel	Hoch	Hoch
Wahrscheinlichkeit	Niedrig	Niedrig	Niedrig	Mittel	Mittel

Tabelle 15: Mögliche Risikobewertungsmatrix je Abweichung

Um nun eine Risikobewertung je Dritten zu erhalten, wird je Risikoeinstufung eine Punktezahl definiert. Folgend eine mögliche Punktezahl je Risikoeinstufung:

- **Niedrig**: 10 Punkte
- **Mittel**: 30 Punkte
- **Hoch**: 70 Punkte
- **Kritisch**: 100 Punkte

Diese Punkte werden anschließend für jede Abweichung zu einer Risikosumme addiert. Die Risikosumme kann danach auf einer Risikoskala dargestellt werden:

Risikosumme:	< 90	90-190	190-290	290-390	390-490	> 490
Risiko:	Klein	Sehr gering	Gering	Erhöht	Hoch	Sehr hoch

Abbildung 20: Mögliche Risikoskala für die Risikobeurteilung je Dritten

Das Bewertungsvorgehen kann anhand eines Beispiels mit dem Dienstleister A veranschaulicht werden: Für den Dienstleister A wurden in der Analyse zehn Abweichungen identifiziert. Die Bewertung ergibt, dass es sich dabei laut Matrix (Tabelle 15) um fünf niedrige, zwei mittlere, zwei hohe und eine kritische Abweichung handelt. Addiert folgt daher eine Risikosumme von 320 (2*10+2*30+2*70+100), d.h. der Dienstleister A stellt ein erhöhtes Risiko dar.

Durch die Analyseausprägung je Kritikalität sowie den garantierten Mix aus Outside-in- und Inside-out-Methoden ergibt sich ein risikobasierter wie auch holistischer Ansatz zur Bewertung von Lieferanten und Dienstleistern.

Alternative: Risikobeurteilung auslagern
Wie in Absatz 4 beschrieben, gibt es für Unternehmen die Möglichkeit, diesen Schritt der Risikobewertung auszulagern. Die Tabelle 16 stellt eine mögliche Matrix auf, die das Service der KSV 1870 einsetzt, um diesen Schritt umzusetzen. Auch hier wird auf die jeweilige Kritikalität des Dritten Rücksicht genommen und dadurch eine ausgelagerte und risikobasierte Bewertung vorgenommen. Das CyerRisk Rating der KSV 1870 stellt danach für jeden Lieferanten eine Bewertung, wie in Abbildung 13 gezeigt, zur Verfügung. Durch dieses Rating wird jedoch der Unternehmenskontext nur teilweise berücksichtigt. So können zwar je Kritikalität Anforderungen an den Dritten gestellt werden, aber die Abweichungen werden anhand genereller Gewichtungen der KSV 1870 bewertet und nicht auf den eigenen Unternehmenskontext umgelegt. So ist die Bewertung von Lieferant A immer die gleiche, obwohl womöglich Kontrollen nicht umgesetzt wurden, die für eine Geschäftsbeziehung zu Unternehmen A relevant, für Unternehmen B jedoch irrelevant sind.

Kritikalität	KSV 1870 Teil 1	KSV 1870 Teil 2
Hoch	Web-Risk Indikator	A+ Rating – Fortgeschrittenes Sicherheitslevel
Mittel	Web-Risk Indikator	A Rating – Fortgeschrittenes Sicherheitslevel
Niedrig	Web-Risk Indikator	B Rating – Basissicherheitslevel

Tabelle 16: Mögliche Risikobewertung mit KSV1870 abhängig der Kritikalität des Dritten

Output: Risikobasierte und holistische Bewertung der Third-Parties

5.2.5. Third-Party Risiko-Monitoring

Das Online-Risk-Rating bietet sich für das Risiko-Monitoring an und sollte daher als fixer Bestandteil etabliert werden. So bieten TPRM-Plattformen wie OneTrust auch automatisierte Abläufe, wo ein Lieferant automatisch mit einem definierten Fragebogen konfrontiert wird, sollte das Online-Risk-Rating unter ein definiertes Niveau fallen (P. Schürrle von OneTrust, persönliche Kommunikation, 13. April 2022). Darüber hinaus sollte wiederum in eine Matrix aufgesetzt werden, die definiert, wie häufig die Risikobewertung erfolgt. Auch hierbei sollte die Kritikalität des Dritten berücksichtig werden, damit ein an den Dritten angepasster Zyklus etabliert werden kann.

Kritikalität	Häufigkeit der Bewertung
Hoch	Jährlich
Mittel	Alle zwei Jahre oder bei Bedarf
Niedrig	Alle drei Jahre oder bei Bedarf

Abbildung 21: Mögliche Matrix zur Häufigkeit der Risikobewertung

Als weitere Option stellen sich interne wie auch externe Schwachstellen-Scans an, die periodisch wiederholt werden. Dazu werden am besten unabhängige Dritte eingesetzt, die anschließend einen Bericht zur Verfügung stellen. [29] Diese Option sollte vor allem für kritischen Dritte angewendet werden, um die Wahrscheinlichkeit eines Sicherheitsvorfalls, der für das eigene Unternehmen schwerwiegende Folgen haben könnte, zu minimieren.

Output: Periodische Risikobeurteilung je Third-Party

5.2.6. Third-Party Risikobehandlung

In dieser Arbeit steht die Risikobewertung im Vordergrund. Nichtsdestotrotz gehört zu einem vollständigen Prozess auch die Risikobehandlung, die an dieser Stelle kurz beschrieben wird. Wie bei allen anderen Risiken geht es auch bei Risiken durch Dritte darum, die Wahrscheinlichkeit oder die damit verbundenen Auswirkungen zu minimieren. Dies lässt sich erreichen, indem der Dritte zusätzliche oder angepasste Sicherheitskontrollen implementiert – eben jene, die bei der Beurteilung nicht oder mangelhaft implementiert waren. Es handelt sich um eine logische Konsequenz, deren Umsetzung aber mit unterschiedlichen Schwierigkeiten verknüpft sein kann. So wird es womöglich Dritte geben, die die daraus entstehenden Kosten auf das eigene Unternehmen abzuwälzen versuchen. [29] Wie im Risikomanagement üblich kann das Risiko aber auch transferiert, verhindert oder akzeptiert werden [13]. Vor allem das Verhindern (Geschäftsbeziehung nicht eingehen oder auflösen) oder auch Akzeptieren (Risiko wird durch Geschäftsleitung akzeptiert) sind denkbare Optionen im TPRM [29]. An dieser Stelle bietet es sich an, gemeinsam mit dem Dritten einen Reaktionsplan zu erarbeiten und abzustimmen. So könnte dieser

festlegen, dass Risiken der Stufe „Niedrig“ in den nächsten 120 Tagen behoben werden, Risiken der Stufe „Mittel“ in den nächsten 90 Tagen und Risiken der Stufe „Hoch“ in den nächsten 30 Tagen behoben werden. [2] Da dieser Schritt entsprechenden Aufwand erzeugt, kann auch hier die Kritikalität des Dritten zur Priorisierung dienen, um mit kritischen Dritten entsprechend schneller einen Reaktionsplan zu vereinbaren.

Output: Risikoreaktionsplan je Third-Party

6. Fazit

Ziel dieser Diplomarbeit war es, zu erheben, wie IT-Sicherheitsrisiken von Dritten holistisch identifiziert und bewertet werden können. Zusätzlich sollten regulatorische und gesetzliche Anforderungen hinsichtlich der Umsetzung eines TPRM untersucht werden.

Durch die Literaturrecherche konnte festgestellt werden, dass der Thematik rund um TPRM sowie Supply-Chain Risk Management durch die immer größere, auch globale Vernetzung von Unternehmen ein hoher Grad an Komplexität zugesprochen wird. Darüber hinaus wird die hohe Relevanz der Thematik in einer Vielzahl an Arbeiten bestätigt, denn viele IT-Sicherheitsvorfälle konnten in Untersuchungen auf die Geschäftsbeziehung mit Dritten zurückgeführt werden. So wurden auch auf EU-Ebene Projekte zur Förderung dieses Forschungsbereiches finanziert, um Cyberrisiken in der Supply-Chain besser abschätzen zu können. Dennoch wird in diesem Forschungsgebiet rund um IT-Sicherheitsrisiken durch Third-Parties eine erhebliche Unreife geortet. So konnte in den Untersuchungen der wissenschaftlichen Arbeiten keine konkrete Umsetzung für die holistische Identifizierung und Bewertung von Third-Party-Risiken entdeckt werden.

Auch die Untersuchung dedizierter Frameworks für das TPRM zeigte, dass nur die NIST SP 800-161 konkrete Anweisungen für die Umsetzung liefert. Andere Frameworks wie die ISO/IEC 27036, ISO 27005, NIST-CSF oder NIST-RMF formulieren Prozesse und Anforderung mit hoher Flughöhe, stellen jedoch nur wenige konkrete Anhaltspunkte zur Verfügung, um die Risiken Dritter tatsächlich zu identifizieren und zu bewerten.

Die Compliance-Untersuchung zeigte, dass TPRM von österreichischen Banken sowohl durch nationale, EU-spezifische und durch bankenspezifische Regularien gefordert wird. Die Forderungen durch EBA, NISG, DORA, DSGVO, Bankwesengesetz und Zahlungsdienstegesetz hinsichtlich TPRM sind meist sehr ähnlich wobei die EBA die konkretesten Anweisungen liefert. Damit zeigt die Untersuchung, dass TPRM nicht nur im wissenschaftlichen Kontext als relevant eingestuft wird, sondern auch von vielen Regularien eingefordert wird. Ein weiterer Punkt, der durch die Untersuchung festgestellt wurde, ist, dass Zertifizierungen sowohl in wissenschaftlichen Arbeiten wie auch in Regularien als relevantes Instrument für das TPRM gesehen werden.

Als Herausforderungen auf der Gegenseite für Unternehmen steht jedoch die hohe Komplexität, wie auch die Erkenntnis, dass klare Anweisungen und Leitfäden zur Umsetzung von TPRM kaum vorhanden sind. So wurden in Zuge der Arbeit auch Dienstleister untersucht, die TPRM-as-a-Service anbieten, um Unternehmen bei der TPRM-Umsetzung zu unterstützen. Neben US-Anbietern konnte hierbei festgestellt werden, dass das österreichische Unternehmen KSV 1870 Nimbusec GmbH ein bereits verbreitetes und praxistaugliches Bewertungsverfahren von Dritten zur Verfügung stellt, das den Aufwand auf Unternehmensseite stark reduzieren kann.

Im Laufe der Arbeit wurde ein Modell zur Risikobewertung Dritter erstellt, das sowohl die möglichen Methoden wie auch einen generischen TPRM-Prozess anbietet. Dazu wurden die Informationen aus den

untersuchten wissenschaftlichen Publikationen, TPRM-Frameworks, Regularien, TPRM-as-a-Service Anbietern wie auch TPRM-Technologie-Anbietern in einen praxistauglichen und prägnanten Leitfaden überführt. Außerdem konnte mithilfe der Untersuchung eine Kategorisierung der gängigen Bewertungsmethoden erreicht werden. Einerseits Outside-in-Methoden, wobei der Dritte von außen mit öffentlich verfügbaren Daten bewertetet wird. Hierzu werden meist sogenannte Risk-Scoring-Tools eingesetzt. Andererseits Inside-out-Methoden, wobei interne Informationen erhoben werden, die anschließend in die Bewertung einfließen. Die Untersuchung hat gezeigt, dass die am häufigsten eingesetzte Inside-out-Methode der Fragebogen ist. Um IT-Sicherheitsrisiken Dritter nun holistisch identifizieren und bewerten zu können, gilt es Outside-in- und Inside-out-Methoden zu kombinieren, wodurch eine 360-Grad-Bewertung erreicht wird. Zusätzlich wurde ein risikobasierter TPRM-Prozess erarbeitet, durch den eine 360-Grad-Bewertung garantiert, aber abhängig der Kritikalität des Dritten erfolgt. Dementsprechend werden Dritte, deren Geschäftsbeziehung besonders kritisch für das eigene Unternehmen sind, genauer unter die Lupe genommen und dazu auch mehr Anforderungen gestellt, als es für weniger kritische Geschäftspartner gilt. Die Forschung zeigt auch auf, wie wichtig eine periodische Bewertung der Dritten ist, um die sich ständig ändernde Risikosituation durch Dritte akkurat abbilden zu können.

Durch die Arbeit wird eine konkrete Umsetzung zur Bewertung Dritter aufgezeigt, die durch Regularien gefordert wird, so aber in der Literatur nicht zu finden ist. Zukünftige Forschung könnte an diese Arbeit anknüpfen, indem das Model in der Praxis getestet und falls nötig erweitert wird. Des Weiteren könnte künftige Forschung TPRM-Technologien näher untersuchen, um unter anderem deren Vor- und Nachteile zu erheben.

7. Literaturverzeichnis

[1] M. Almutairi und S. Riddle, „State of the art of IT outsourcing and future needs for managing its security risks," in *2018 International Conference on Information Management and Processing (ICIMP)*, 2018.

[2] G. C. Rasner, Cybersecurity and Third-Party Risk: Third Party Threat Hunting, Wiley, 2021, p. 480.

[3] P. I. LLC, „A crisis in third-party remote access security," SecureLink, 2021.

[4] J. Boyens, C. Paulsen, N. Bartol, K. Winkler und J. Gimbi, „Key Practices in Cyber Supply Chain Risk Management: Observations from Industry," 2021.

[5] C. Colicchia, A. Creazza und D. A. Menachof, „Managing cyber and information risks in supply chains: insights from an exploratory analysis," *Supply Chain Management: An International Journal,* 2018.

[6] J. Viega und J. B. Michael, „Struggling With Supply-Chain Security," *Computer,* Bd. 54, p. 98–104, 2021.

[7] I. Symantec, *Internet Security Threat Report 2019 [J],* 2019.

[8] B. Ferraro, „Third-Party Risk Management Frameworks: An Overview," May 2021.

[9] A. Ghadge, M. Weiß, N. D. Caldwell und R. Wilding, „Managing cyber risk in supply chains: A review and research agenda," *Supply Chain Management: An International Journal,* p. 18, 2019.

[10] ISO/IEC, „ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships," 2021.

[11] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook und M. Fallon, „Cyber Supply Chain Risk Management Practices for Systems and Organizations," 2021.

[12] M. P. Barrett und others, „Framework for improving critical infrastructure cybersecurity," *National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep,* 2018.

[13] ISO/IEC, „ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management," 2018.

[14] O. F. Keskin, K. M. Caramancion, I. Tatar, O. Raza und U. Tatar, „Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports," *Electronics,* Bd. 10, 2021.

[15] M. Cissé, „Third-party risk management: Strategy to mitigate 'on-premise'and 'cloud'cyber security risks," *Cyber Security: A Peer-Reviewed Journal,* Bd. 3, p. 103–115, 2019.

[16] Gartner, „Gartner Glossary," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/vendor-risk-management. [Zugriff am 28 10 2021].

[17] M. Abdul Moktadir, T. Rahman und R. Sultana, „Selection of best supplier by using AHP tool for managing risk factors in logistics: a case of leather products industry," *Industrial Engineering & Management,* Bd. 6, p. 232, 2017.

[18] Reciprocity , „What is Supply Chain Risk Management?," [Online]. Available: https://reciprocity.com/resources/what-is-supply-chain-risk-management/. [Zugriff am 28 10 2021].

[19] Council of Supply Chain Management Professionals, [Online]. Available: https://cscmp.org/CSCMP/Educate/SCM_Definitions_and_Glossary_of_Terms.aspx. [Zugriff am 28 10 2021].

[20] A. Creazza, C. Colicchia, S. Spiezia und F. Dallari, „Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era," *Supply Chain Management: An International Journal,* 2021.

[21] B. M. Bhatti, S. Mubarak und S. Nagalingam, „A framework for information security risk management in IT outsourcing," 2017.

[22] I. A. Tøndel, F. Seehusen, E. A. Gjære und M. E. G. Moe, „Differentiating Cyber Risk of Insurance Customers: The Insurance Company Perspective," in *Availability, Reliability, and Security in Information Systems*, Cham, 2016.

[23] B. Dobrec, „Strengthening Third-Party Risk Management," *Risk Management,* Bd. 66, p. 6, 2019.

[24] J. T. A. Malatesta III und S. S. Glover, „A Clear and Present Danger: Mitigating the Data Security Risk Vendors Pose to Businesses," in *Sedona Conf. J.*, 2016.

[25] B. A. Aubert, M. Patry und S. Rivard, „Assessing the risk of IT outsourcing," in *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*, 1998.

[26] G. Dhillon, R. Syed und F. de Sá-Soares, „Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors," *Information & Management,* Bd. 54, p. 452–464, 2017.

[27] R. González, J. Gascó und J. Llopis, „Information systems outsourcing reasons and risks: review and evolution," *Journal of Global Information Technology Management,* Bd. 19, p. 223–249, 2016.

[28] R. Rothrock, „Why The Cybersecurity Domino Effect Matters," *Forbes,* 2015.

[29] R. Pompon, „Third-Party Security," in *IT Security Risk Control Management*, Springer, 2016, p. 283–292.

[30] ISO, „ISO/IEC 27001 Information Security Management," *International Standards Organization,* 2013.

[31] S. Papastergiou und N. Polemi, „MITIGATE: a dynamic supply chain cyber risk assessment methodology," in *Smart Trends in Systems, Security and Sustainability*, Springer, 2018, p. 1–9.

[32] N. Polemi und P. Kotzanikolaou, „Medusa: a supply chain risk assessment methodology," in *Cyber Security and Privacy Forum*, 2015.

[33] I. Sotnikov, „Simplifying Third-Party Risk Management," *Risk Management,* Bd. 66, p. 3, 2019.

[34] M. Benaroch, „Cybersecurity Risk in IT Outsourcing—Challenges and Emerging Realities," in *Information Systems Outsourcing*, Springer, 2020, p. 313–334.

[35] N. V. Vasishta, M. Gupta, S. K. Misra, P. Mulgund und R. Sharman, „Optimizing cybersecurity program—evidence from data breaches in healthcare," in *13th Annual Symposium on Information Assurance (ASIA'18)*, 2018.

[36] J. Haller und C. Wallen, *Managing third party risk in financial services organizations: a resilience-based approach,* Accessed, 2018.

[37] ISO/IEC, „ISO/IEC 27036-1:2014 Cybersecurity — Supplier relationships," 2014.

[38] ISO/IEC, „ISO/IEC 27036-2:2014 Part 2:Requirements," 2014.

[39] ISO, „ISO 31000:2018 Risk management — Guidelines," 2018.

[40] V. Monev, „The" Self-Assessment" Method within a Mature Third-Party Risk Management Process in the Context of Information Security," in *2021 International Conference on Information Technologies (InfoTech)*, 2021.

[41] NIST, „Risk Management Framework for Information Systems and Organizations-A System Life Cycle Approach for Security and Privacy," *National Institute of Standards and Technology,* 2018.

[42] ISO, „IEC 31010:2019 Risk management — Risk assessment techniques," 2019.

[43] B. f. S. i. d. Informationstechnik, „BSI-Standard 200-3: Risikomanagement," 2017.

[44] E. Krügler, „Compliance - ein Thema mit vielen Facetten," *Umwelt Magazin,* Bd. 7, p. 50, 2011.

[45] G. K. Europäische Kommission, „Verordnungen, Richtlinien und sonstige Rechtsakte," 2022.

[46] E. P. V. in Deutschland, „Ordentliches Gesetzgebungsverfahren," 2022.

[47] E. B. Authority, *Auftrag und Aufgaben,* 2022.

[48] E. B. Authority, „Guidelines on outsourcing arrangements," 2019.

[49] E. B. Authority, „Guidelines on ICT Risk Assessment under the SREP," 2017.

[50] E. B. Authority, „Guidelines on ICT and security risk management," 2019.

[51] E. Union, „Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union," *EUR-Lex,* 2016.

[52] Bundeskanzleramt, „Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)," 2018.

[53] Bundeskanzleramt, „Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV)," 2019.

[54] B. für Inneres, „NIS Fact Sheet 8/2019: Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste," 2019.

[55] E. Union, „Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014," *EUR-Lex,* 2020.

[56] E. Union, „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)," *EUR-Lex,* 2016.

[57] D. R. Österreich, „Zertifizierungen - Akkreditierung als Zertifizierungsstelle gemäß Art. 43 Abs. 1 DSGVO," 2021.

[58] Ö. Parlament, „Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG)," 2022.

[59] B. für Finanzen, „Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (Zahlungsdienstegesetz 2018 – ZaDiG 2018)," 2018.

[60] E. Kommission, „Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION," *EUR-Lex,* 2021.

[61] P.-M. Carfantan, „EU-Artificial Intelligence Act – Chance oder Risiko für Unternehmen?," *it-daily.net,* 2021.

[62] S. D. Consulting, *TPRM Officer as a Service,* 2022.

[63] FirmenABC, *KSV1870 Nimbusec GmbH.*

[64] A. Mitter, *Das CyberRisk Rating Kurzvorstellung,* 2022.

[65] K. C. R. A. Board, „Cyber Risk Rating & Cyber Trust LabelSchema Policy," 2021.

[66] Prevalent, „Navigating the Vendor Risk Lifecycle: Keys to Success at Every Stage," 2021.

[67] Prevalent, „Six Steps to Complete Third-Party Risk Management," 2019.

[68] Prevalent, „Third-Party Profiling & Tiering Template," 2022.

[69] S. Assessments, „About Shared Assessments," [Online]. Available: https://sharedassessments.org/about/. [Zugriff am 28 04 2022].

[70] Google, „SIG Questionnaire - Compliance," [Online]. Available: https://cloud.google.com/security/compliance/sig. [Zugriff am 28 04 2022].

[71] KSV1870, „Das CyberRisk Rating KSV1870," [Online]. Available: https://cyberrisk-rating.at. [Zugriff am 28 04 2022].

[72] SecurityScorecard, „Security Ratings & Cybersecurity," [Online]. Available: https://securityscorecard.com. [Zugriff am 28 04 2022].

[73] compliance-net, „Prüfungsstandard für Outsourcing – Service Organization Control Report," [Online]. Available: https://www.compliance-net.de/content/pr%C3%BCfungsstandard-f%C3%BCr-outsourcing-service-organization-control-report. [Zugriff am 28 04 2022].

[74] TISAX, „Welcome to TISAX," [Online]. Available: https://enx.com/de-de/tisax. [Zugriff am 28 04 2022].

[75] R. Putrus, „A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance," *ISACA Journal,* 2017.

[76] EY, „Transforming your third-party risk into a competitive advantage," 2018.

[77] M. Windelberg, „Objectives for managing cyber supply chain risk," *International Journal of Critical Infrastructure Protection,* Bd. 12, p. 4–11, 2016.

[78] J. VanHoy, „Third Party Risk Management," *Available at SSRN 3763399,* 2021.

[79] L. Sunderkrishnan, „Vendor Risk Assessment," *EDPACS,* Bd. 54, p. 19–26, 2016.

[80] J. Spencer, E. Weinstein und L. Ellery, „Magic Quadrant for IT Vendor Risk Management Tools," 2021.

[81] H. Santos, A. Oliveira, L. Soares, A. Satis und A. Santos, „Information Security Assessment and Certification within Supply Chains," in *The 16th International Conference on Availability, Reliability and Security*, 2021.

[82] N. Polemi und S. Papastergiou, „Current efforts in ports and supply chains risk assessment," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015.

[83] S. Pandey, R. K. Singh, A. Gunasekaran und A. Kaushik, „Cyber security risks in globalized supply chains: conceptual framework," *Journal of Global Operations and Strategic Sourcing,* 2020.

[84] O. F. Keskin, K. M. Caramancion, I. Tatar, O. Raza und U. Tatar, „Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports," *Electronics,* Bd. 10, p. 1168, 2021.

[85] G. Hodosi und L. Rusu, Risks, Relationships and Success Factors in IT Outsourcing: A Study in Large Companies, Springer, 2019.

[86] J. T. Force, „Security and Privacy Controls for Information Systems and Organizations," 2017.

[87] Y. Cheng, „Information security risk assessment model of IT outsourcing managed service," in *2012 International Conference on Management of e-Commerce and e-Government*, 2012.

[88] S. Charney, E. T. Werner und T. Computing, „Cyber supply chain risk management: Toward a global vision of transparency and trust," *Microsoft Corporation paper,* p. 6–8, 2011.

[89] S. Carnovale und S. Yeniyurt, Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions, Bd. 1, World Scientific, 2021.

[90] S. Boyson, „Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems," *Technovation,* Bd. 34, p. 342–353, 2014.