Ansatz zur Auswahl von Risikomanagement-Methoden

Martin Latzenhofer · Stefan Schauer
Sandra König · Christian Kollmitzer

Austrian Institute of Technology
{stefan.schauer | martin.latzenhofer
sandra.koenig | christian.kollmitzer}@ait.ac.at

Zusammenfassung

Es existiert eine Vielzahl an unterschiedlichen Risikomanagementframeworks. Bei einem ersten Kontakt mit den Publikationen ist es für den angehenden Risikomanager eine komplexe Aufgabe, das für die jeweilige Organisation in der aktuellen Situation und der individuellen Ziel- und Schwerpunktsetzung optimale Framework auszuwählen. Zudem kann diese Entscheidung nach dem Aufsetzen der Risikomanagementstrukturen in der Organisation nur unter sehr erschwerten Bedingungen revidiert und das Framework gewechselt werden, ohne hohe Sunk Costs zu generieren. Die European Network and Information Security Agency (ENISA) hat im Jahre 2006 eine Vergleichsmethodik entwickelt und die damals wichtigsten Risikomanagementframeworks anhand von 15 Kriterien verglichen. Die Grundidee des vorliegenden Artikels ist es, den Vergleich mit heutigen Frameworks nochmals durchzuführen, die Ergebnisse zu interpretieren und darüber hinaus zu diskutieren, ob die angelegten Bewertungskriterien heute noch zeitgemäß sind. Es werden Verbesserungsvorschläge dargestellt, welche die Potentiale der Frameworks für eine dezidierte Praxisanwendung insbesondere durch kleine und mittlere Unternehmen (KMU) besser sicht- und bewertbar machen. Hierbei wird argumentiert, dass die Schlüsselaspekte Detaillierungsgrad der Ausgestaltung, Organisationsgröße und -komplexität, Branchenrisiken, Risikomanagement-Knowhow und Ressourceneinsatz fokussierter in die Entscheidungskriterien einfließen sollten. Auch berücksichtigt der Methodenvergleich in der angewendeten Form weder Kaskadeneffekte, noch den Umgang mit inhärenter Unsicherheit oder die Anwendung neuerer Bewertungsmethoden.

1 Einleitung

Die Bedeutung von Risikomanagement als fundamentaler Ausgangspunkt für Entscheidungsfindung (Decision Making) ist seit dem letzten Jahrzehnt signifikant gestiegen. Einerseits wird Risikomanagement als probates Mittel gesehen, ex-ante auf eine Organisation oder ein System wirkende Gefahren, die sich in Kombination mit den Schwachstellen zu expliziten Bedrohungen gegen Werte in der Organisation auswachsen, vorab realistisch einzuschätzen und so den eigenen Ressourceneinsatz auf die Entwicklung, den Einsatz und die Überwachung von risikominimierenden Maßnahmen zu legen. Dabei achtet eine Organisation naturgemäß darauf, dieses möglichst effizient anhand ihrer ökonomischen Restriktionen wie Zeit, Geld oder Personalaufwand zu gestalten. Dies ist für den laufenden Betrieb wichtig, denn Risiken sind mannigfaltig, sehr vielschichtig und eben aufgrund der inhärenten Unsicherheit schwer fass- und einschätzbar.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 298-312.

Aufgrund dieser Problematik können Risiken vielfach nur qualitativ eingeschätzt werden, weil Aussagen über Häufigkeiten für eine seriöse quantitative Bewertung meist nicht in ausreichender Detailtiefe vorhanden sind. Auf der anderen Seite versucht man über Risikomanagement, insbesondere bei Compliance-Anforderungen, der vorhandenen Komplexität von Aufgaben in der Organisation zu begegnen und so die erforderlichen strukturgebenden Handlungsempfehlungen zu fokussieren. Zusammenfassend ist Risikomanagement für betriebswirtschaftlich operierende Organisationen ein Mittel zur Optimierung der eigenen Aktivitäten bei gleichzeitig angestrebter günstiger Ausrichtung des operativen Risikos.

Eine wesentliche Entscheidung für die Organisation bei der Einführung von Risikomanagementstrukturen betrifft die Wahl des zugrundeliegenden Risikoframeworks und damit des angewendeten Risikomodells. Bestehende Frameworks unterscheiden sich bei näherer Betrachtung signifikant hinsichtlich ihrer Struktur, der Detailtiefe, der Anwenderperspektive, inhaltlicher Schwerpunktsetzung und der Ausgestaltung. Dennoch können bei allen Ansätzen Gemeinsamkeiten in Herangehensweise, Begrifflichkeiten und Zielorientierung festgestellt werden. Somit stellt sich für den Risikomanager als auch den Prozess-Sponsor die Frage, wie man die Risikomanagementframeworks objektiv einem Vergleich unterziehen und bewerten kann, sodass man sich auf Basis der eigenen Rahmenbedingungen innerhalb der Organisation, der formulierten Zielsetzung und dem erforderlichen Detaillierungsgrad für das optimale – am besten für die jeweilige Situation passende – Risikomanagementframework entscheiden kann.

Die Europäische Agentur für Netz- und Informationssicherheit (European Network and Information Security Agency – ENISA) hat im Jahre 2006 im Rahmen eines Arbeitsprogramms über die Erhebung von Risikomanagement und Risikobewertungsmethoden einen Risikomanagementprozess [Tech08] definiert, der in nachfolgender Abbildung 1 dargestellt ist. Der Prozess identifiziert dabei sechs Phasen mit in Summe 15 Schritten und basiert auf verschiedenen internationalen Standards, Guidelines und Best Practices aus dieser Domäne oder anverwandten Gebieten, bei denen Risikomanagement die Grundlage bildet, wie beispielsweise Informationssicherheit. Zum Zeitpunkt der Definition des ENISA-Prozesses wurden die ISO/IEC 13335 [Inte04], ISO 17799 [Inte00], IT-Grundschutzkatalog [Bund13], NIST SP800-30 [StGF02] und OCTAVE [AlDo01a] als die relevantesten Frameworks angesehen. Obwohl diese mittlerweile alle überarbeitet, aktualisiert oder in anderen Rahmenwerken aufgegangen sind, haben die allgemeine Struktur und insbesondere diese 15 Schritte des ENISA-Prozesses weiterhin Gültigkeit.

Im Rahmen dieses Beitrages werden die von den Prozess-Schritten abgeleiteten Bewertungskriterien [Enis06] für einen Vergleich herangezogen und aktuelle Risikomanagementframeworks verglichen. Die sechs Phasen Bereichsbestimmung (Scoping), Risikobewertung (Risk Assessment), Risikobehandlung (Risk Treatment), Risikoakzeptanz (Risk Acceptance), Risikokommunikation, Risikosensibilisierung und Risikoberatung (Risk Communication and Risk Awareness Consulting) sowie Risikoüberwachung und Überprüfung (Risk Monitoring and Review) bilden den Rahmen für die 15 als Schritte bezeichneten Schlüsselaktivitäten. Diese werden nach einer vierstufigen Skala (von 0 bis 3) anhand ihres Detaillierungsgrades sowie deren jeweiliger Input und Output bewertet, der in einem abstrahierten Angleichungsprofil resultiert, das in weiterer Folge für die visuelle Darstellung und den Vergleich herangezogen wird.

Die im vorliegenden Beitrag analysierten Frameworks sind die ISO 31000 [Inte09], welche momentan den anerkannten allgemeinen Standard für Risikomanagement darstellt; ISO/IEC 27005 [Inte11], der mittlerweile mit sieben Jahren veraltet, aber in der Praxis weit verbreitet ist; NIST SP 800-30/-37/-39 [StGF02], [Nati10], [Nati11], der im US-amerikanischen Raum

wesentliche Bedeutung hat; COBIT for Risk [Info13] als speziell auf Risikomanagement ausgerichtete Variante des Governance-Frameworks; COSO ERM 2017 [CoPw17], die Aktualisierung des etablierten COSO-ERM-Frameworks sowie OCATVE Allegro [RJLW07] als praxisorientierter Prozess zur Implementierung von Risikomanagementstrukturen in Organisationen.

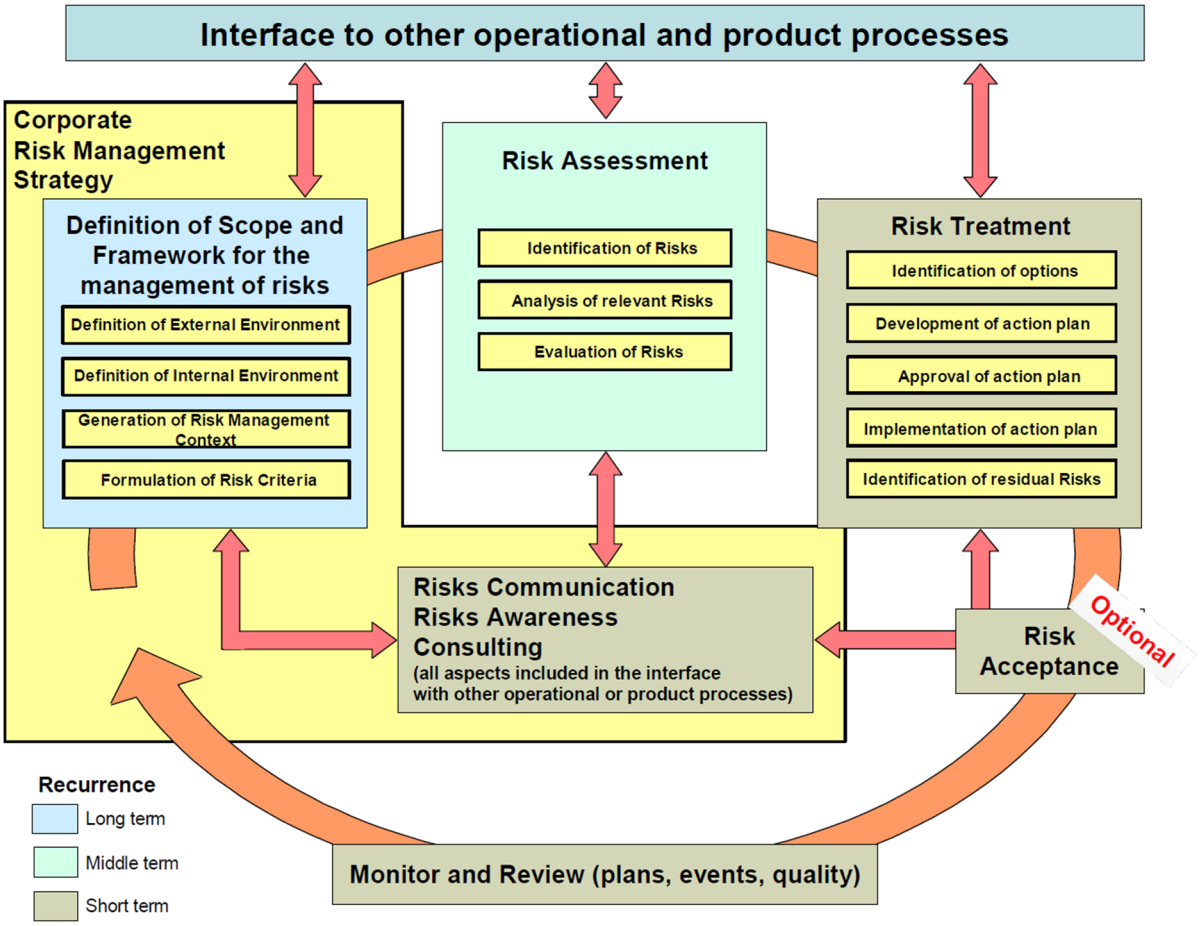

Abb. 1: ENISA Risikomanagementprozess [Tech08]

Nach der Durchführung der konkreten Bewertung der einzelnen Risikomanagementframeworks werden im Artikel die Einzelergebnisse im Gesamtvergleich kritisch betrachtet. Der Methodenvergleich zeigt, welche Frameworks in welchen Komponenten eine starke Akzentuierung aufweisen und so gute Unterstützung für die jeweilige Detailaufgabe bei der Einführung von Risikomanagementstrukturen in einer Organisation liefern können. Die Methodik wird anschließend kritisch gewürdigt und sinnvolle zukünftige Adaptierungen diskutiert.

2 Risikomanagementmethoden

In diesem Abschnitt werden die einzelnen Risikomanagementframeworks vorgestellt, welche für den Methodenvergleich betrachtet werden. Es folgt jeweils eine kurze Einführung zur Herkunft und Intention, eine rudimentäre Beschreibung der hinterlegten Prozessschritte sowie eine kurze Zusammenfassung der spezifischen Charakteristika. Für eine detailliertere Beschreibung sei hier auf die jeweiligen Referenzen aus der Literatur verwiesen.

2.1 ISO 31000

Der internationale Standard für Risikomanagement, ISO 31000:2009 [Inte09], beschreibt Prinzipien und Richtlinien für die Implementierung von Risikomanagement und geht dabei nicht nur auf den operativen Prozess, sondern besonders auch auf generelle Prinzipien und das darunter liegende Framework ein. Eine Besonderheit der ISO 31000 ist die zweistufige Struktur mit einem Risikomanagement-Framework einerseits und dem operativen Risikomanagement-Prozess andererseits. Das top-down aufgestellte Risikomanagement-Framework folgt einem iterativen und kontinuierlichen Verbesserungszyklus nach dem allgemeinen Plan-Do-Check-Act (PDCA)-Zyklus. Der operative Risikomanagementprozess ist bottom-up umgesetzt und stellt die verschiedenen Risiken in einen organisatorischen Kontext, bewertet und behandelt diese. Während des gesamten Risikomanagementprozesses stellen zwei Teilprozesse die Kommunikation und Beratung sowie die Überwachung und Überprüfung sicher.

Die Umsetzung des Risikomanagementprozesses erfolgt in fünf generischen Schritten, welche den Prozess weiter aufspalten: Erstellen des Zusammenhangs, Risikoidentifikation, Risikoanalyse, Risikobewertung und Risikobehandlung. Im Detail werden dabei zu Beginn die Rahmenbedingungen für das Risikomanagement in Bezug auf die Organisation festgelegt, die potentiellen Bedrohungen sowie deren Eintrittswahrscheinlichkeit und Auswirkungen identifiziert und miteinander in Beziehung gesetzt. Die resultierende Liste von Risiken wird entsprechend des Kontextes der Organisation bewertet und nach ihrer Wichtigkeit sortiert, woraus sich direkt eine Vorgehensweise zur Risikobehandlung ablesen lässt. Parallel läuft ein Kommunikationsprozess mit den Stakeholdern des Risikomanagements sowie die Umsetzung und Integration in die Entscheidungsfindungsprozesse der Organisation und das Abhalten von Informationsveranstaltungen und Schulungen in Bezug auf Risikomanagement. Die Überwachung und Überprüfung sowie kontinuierliche Verbesserung des Frameworks stellt sicher, dass die Leistung und Wirksamkeit des Risikomanagements anhand von Indikatoren gemessen und auf Grundlage der Ergebnisse ständig verbessert wird.

2.2 ISO/IEC 27005

Der Standard ISO/IEC 27005:2011 [Inte11] ist Teil der ISO 2700x-Normenfamilie und stellt darin einen erweiterten Risikomanagementprozess dar, der speziell auf die Anforderungen in der Informationssicherheit abgestimmt ist. Der in der ISO 27005 definierte Risikomanagementprozess basiert auf dem von der ISO 31000 beschriebenen Prozess und enthält Details zu den Anforderungen an die Informationssicherheit, die als Erweiterung für ein effizientes Informationssicherheitsmanagementsystem (ISMS) dienen. Darin wird deutlich, dass es neben den allgemeinen fünf Schritten aus der ISO 31000 auch einen zusätzlichen Schritt "Risikoakzeptanz" und zwei Entscheidungspunkte ("Bewertung zufriedenstellend" und "Behandlung zufriedenstellend") gibt (siehe [Inte11]).

Der Prozess selbst ist explizit als ein kontinuierlicher Prozess konzipiert (was in der ISO 31000:2009 nicht eindeutig vermerkt ist), der nach dem ersten Durchlauf periodisch wiederholt werden muss. Einzelne Schritte wie Risikobewertung und Risikobehandlung können jedoch aufgrund der beiden Entscheidungspunkte sofort einen Neustart des Prozesses auslösen. Wenn die Ergebnisse der Risikobewertung oder die Effizienz der während der Risikobehandlung identifizierten Risikominderungsaktivitäten eine bestimmte (vordefinierte) Qualität nicht aufweisen oder das Restrisiko nach Risikoübernahme zu hoch ist, kann der Prozess mit verfeinerten Parametern zur Neubewertung aller vorherigen Schritte nochmals durchlaufen werden.

2.3 NIST SP800-30

Das National Institute of Standards and Technology (NIST) ist eine US-Verwaltungsbehörde, die mit der Standardisierung von Verfahren und Prozessen beauftragt ist und laufend Richtlinien („Special Publications“ – SP) insbesondere zum Thema Informationssicherheit herausgibt. Die Special Publications SP 800-30 [Nati12] und SP 800-39 [Nati11] widmen sich dem Thema Risikomanagement. Dabei beschreibt die SP 800-30 ein zweiteiliges Rahmenwerk ähnlich der ISO 31000, das aus dem Risikomanagement und der Risikobewertung besteht.

Der Risikomanagementteil umfasst die vier Komponenten "Frame", "Assess", "Respond" und "Monitor", die an den in Abschnitt 2.1 erwähnten PDCA-Zyklus erinnern und die übergeordneten Schritte darstellen. Die SP800-39 fokussiert stärker auf den Bereich der Informationssicherheit und beschreibt einen detaillierteren Prozess für das Risikomanagement in diesem Kontext, welcher dem Prozess der ISO/IEC 27005 ähnelt. Beide Frameworks in Kombination verfolgen das Konzept eines mehrstufigen Risikomanagements („Multitiered Risk Management“), welches eine Eingliederung des Risikomanagements in alle Schichten der Organisation unterstützen soll. Die Aufteilung erfolgt dabei in Organisation („Organization Tier“), Geschäft („Mission/Business Tier“) und Informationssysteme („Information Systems Tier“), wodurch die Risikobewertung auf unterschiedlichen Hierarchieebenen, von der strategischen bis hin zu taktischen Ebene, durchgeführt wird. Der operative Risikobewertungsprozess befindet sich in der zweiten Komponente "Assess" des Risikomanagementprozesses. Er besteht aus vier Hauptschritten, wobei Schritt zwei in die fünf Hauptschritte der Risikobeurteilung unterteilt ist, welche bereits aus der ISO 31000 bekannt sind.

2.4 COBIT 5 for Risk

COBIT (Control Objectives for Information and Related Technology) hat sich seit seiner ersten Vorstellung 1996 von einem anfänglichen Audit-Leitfaden für IT-Prüfer hin zu einem übergreifenden Governance-Framework für Enterprise-IT in der aktuellen Version 5 entwickelt [Info12a]. Der Herausgeber, die US-amerikanische Information Systems Audit and Control Association (ISACA), hat so die inhaltliche Ausrichtung als auch die jeweils angesprochenen Zielgruppen sukzessive verbreitert. Darüber hinaus legte die ISACA vertiefende Publikationen zu einzelnen Aspekten basierende auf COBIT 5 vor, insbesondere das hier relevante Risikomanagement. COBIT for Risk [Info13] ist ein umfassender Guide in Bezug auf den Risikoaspekt für unterschiedlichste Anspruchsgruppen in Organisationen.

Als Kernelement im COBIT-Framework ist einer von sieben Enablern den Prozessen gewidmet. Die Prozesse selbst sind aus der Standardpublikation COBIT 5 – Enabling Processes [Info12b] entnommen,

wobei von den 37 Prozessen zwei Core-Risikomanagementprozesse – jeweils einer für die Einbettung des Frameworks in die Organisation und den tatsächlichen operativen Risikomanagementprozess – und zwölf davon betroffene Schlüsselprozesse mit Risikomanagement instanziiert und dahingehend detaillierter beschrieben werden (siehe Abbildung 2). Die Inputs, Outputs und Management- respektive Governance Practices werden auf das Thema Risikomanagement hin ebenso näher spezifiziert. Dieses Subset der COBIT-Prozesse kann als eigenständiges Risikomanagementframework verstanden werden. Es reflektiert ebenso wie die ISO 31000 die Aufteilung in strategisch-taktische Frameworkeinbettung und den eigentlichen operativen Risikomanagementprozess, die sich in den beiden Core-Prozessen manifestiert.

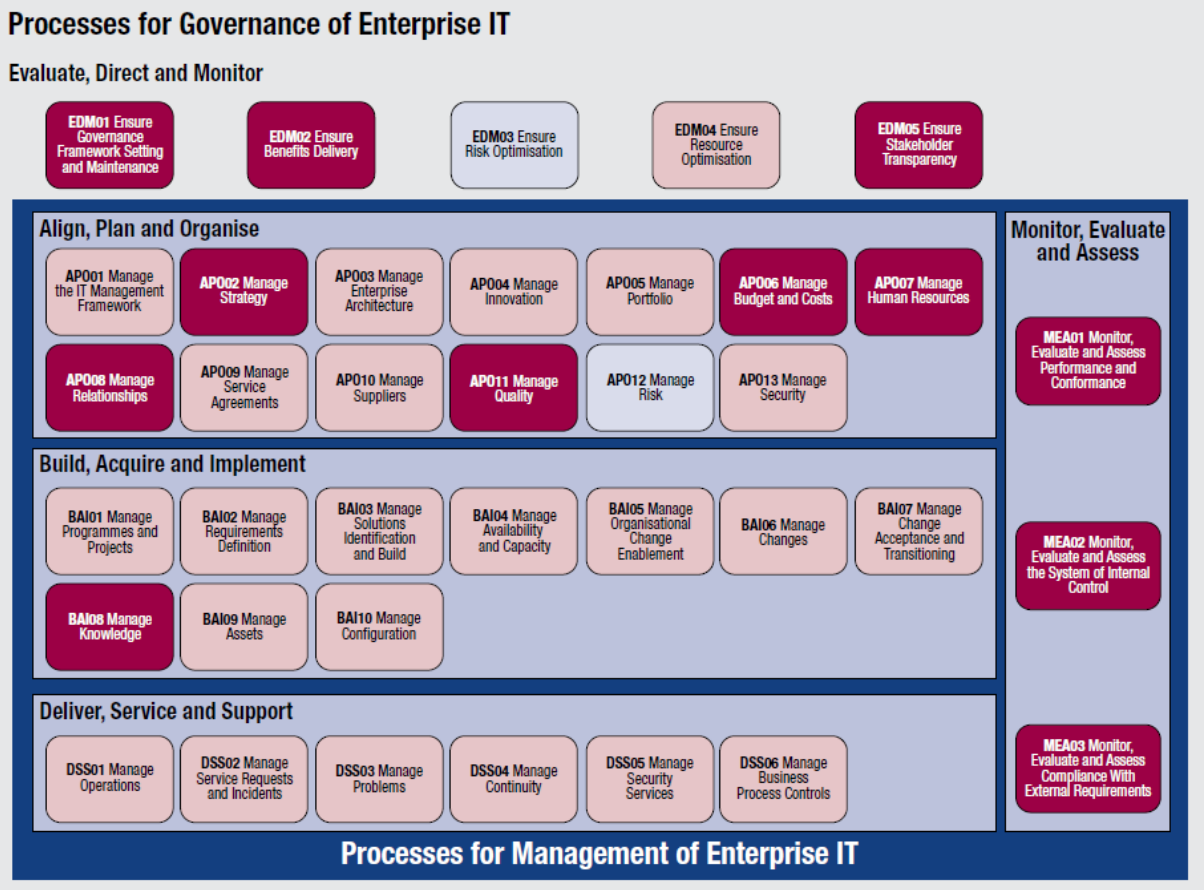

Abb. 2: COBIT for Risk Core- (hellblau) und betroffene Prozesse (dunkelrot) [Info13]

2.5 COSO ERM 2017

Das Committee of Sponsoring Organizations of the Treadway Commission (COSO) hat sein aus dem Jahr 2004 stammendes Enterprise Risk Management Framework kürzlich grundlegend aktualisiert [CoPw17]. Das Hauptziel des Frameworks ist es, Risikomanagern spezifische Methoden und Techniken für das Management von operativen Risiken in die Hand zu geben, welche sehr narrativ beschrieben und auch über verschiedene praxisrelevante Use Cases illustriert werden. COSO ERM 2017 besteht aus fünf Hauptkomponenten, die insgesamt 20 Prinzipien umfassen, die in Abbildung 3 dargestellt sind.

Die erste Komponente “Governance & Culture” adressiert das Setup in der Organisation, die Definition der Kernwerte und die verhaltensbezogenen Erwartungen, die Zuverlässigkeit und Verantwortlichkeit der Organisation. Die Komponente “Strategy & Objective Setting” definiert nun konkrete Anforderungen an ein Risikomanagement in der Organisation, also Geschäftskontext, Risikoappetit, alternative Strategien und Geschäftsziele. Wurde das Framework aufgesetzt, muss die Organisation den operativen Risikomanagementprozess aktiv steuern, was in der Komponente “Performance” beschrieben wird. Darin identifiziert, bewertet und priorisiert der Risikomanager die Risiken, implementiert risikominimierende Maßnahmen und entwickelt ein Risikoportfolio. In der Komponente “Review & Revision” überprüft der Risikomanager Veränderungen der Risiken und der Ergebnisleistung. Die letzte Komponente “Information, Communication & Reporting” subsumiert Aktivitäten zur Information und Kommunikation an alle Anspruchsgruppen.

Ein starker Fokus des Frameworks liegt auf der Einbettung von Risikomanagementaktivitäten in die aktuell verfolgte Strategie, die Geschäftsziele und in das aktuelle Leistungsvermögen der Organisation. Auch hier lässt sich eine Zweiteilung in einen organisatorischen und operativen Risikomanagementprozess ablesen. Die narrative Gestaltung der Beschreibung mag strukturelle Defizite erkennen lassen, dennoch bietet COSO ERM 2017 durch die Gestaltung und Untermauerung durch praxisrelevante Beispiele für die Ausgestaltung des Risikomanagementprozesses. Das sehr neue Framework thematisiert auch aktiv das Problem der kaskadierenden Risiken, die aus der Praxis bekannten ständigen Veränderungen der Risiken sowie die dadurch erforderliche kontinuierliche Anpassung der Risikoprofile sowie der eingesetzten Maßnahmen und es diskutiert auch Kosten-Nutzen-Implikationen.

Abb. 3: COSO ERM Risikomanagementkomponenten und -prinzipien [CoPw17, adaptiert]

2.6 OCTAVE Allegro

Das ursprüngliche Framework, das die Grundlage der OCTAVE-Methode (Operationally Critical Threat, Asset and Vulnerability Evaluation) bildete, wurde im September 1999 vom Software Engineering Institute (SEI) der Carnegie Mellon University publiziert [AlDo01a, AlDo01b]. Diese wurde als OCTAVE-S weiterentwickelt [ADSW05], um eine weniger ressourcenintensive Methode für kleine Fertigungsbetriebe anzubieten. Schließlich wurde OCTAVE Allegro im Mai 2007 veröffentlicht [RJLW07]. Die ursprüngliche OCTAVE-Methode ist in drei Phasen unterteilt; diese umfassen die organisatorische zusammen mit der technologischen Sicht, ähnlich zur dreistufigen Struktur der NIST SP800-30, sowie die Entwicklung der allgemeinen Strategie. Da diese Phasen einen recht umfangreichen und kostspieligen Prozess darstellen, führen OCTAVE-S und OCTAVE Allegro ein einfacheres Verfahren ein. Der OCTAVE-Allegro-Prozess kann somit von einer einzelnen Person durchgeführt werden. Die Methode wird von mehreren Workshops vorangetrieben, um die erforderlichen Informationen zu sammeln. OCTAVE Allegro konzentriert sich auf die informationsrelevanten Ressourcen, deren Nutzung, Speicherung, Verarbeitung und Transport, um eine umfassende und robuste Bewertung der operativen Risikoumgebung einer Organisation durchzuführen.

OCTAVE Allegro wird in acht Schritten durchgeführt, die in vier Phasen organisiert sind. In Phase 1 – Establish Drivers – werden interne Kriterien zur Risikomessung festgelegt, die im letzten Schritt verwendet werden, um die Auswirkungen eines Risikos auf das Geschäftsziel einer Organisation zu bewerten.

In der folgenden Phase – Profile Assets – wird eine Sammlung aller informationsrelevanten Ressourcen innerhalb der Organisation (Software, Hardware, Mitarbeiter etc.) erstellt und ausgewertet. Phase 3 – Identify Threats – ermittelt Bedrohungen für diese Ressourcen durch die Analyse einer Reihe von realen Szenarien. In der Endphase – Identify and Mitigate Risks – werden aus den Bedrohungsszenarien Risiken für die kritischen Informationsressourcen abgeleitet und entsprechende Ansätze zur Risikominderung eingeleitet.

3 Ergebnisse

3.1 Durchführung der Evaluierung

Die Evaluierung entspricht der ursprünglichen Durchführungsmethodik bei der Prozess-Bewertung der ENISA. Einerseits konnten durch die simple Wiederdurchführung des Methodenvergleichs die Mankos der vorhandenen Kriterien plakativ herausgearbeitet werden, andererseits erlaubt eine allfällige Anpassung der Bewertungskriterien zukünftig eine Gegenüberstellung der Bewertungen eines Frameworks. Der ENISA-Risikomanagementprozess wird dabei als Referenzpunkt herangezogen und die 15 ebenda beschriebenen Schritte im zu analysierenden Framework versucht zu identifizieren. Als Maß, inwieweit ein einzelner Schritt im Framework repräsentiert wird, erfolgt gemäß Tabelle 1 eine Bewertung von 0 bis 3, wobei auch Zwischenwerte vergeben wurden, um eine feiner granulierte Evaluierung zu ermöglichen.

Tab. 1: Bewertung der Prozesse

Score	Konvergenz zwischen analysiertem Framework und Referenz-Framework
0	Der Prozess ist nicht repräsentiert.
1	Der Prozess ist als Teilbereich beschrieben und mit externer Referenz angegeben.
2	Der Prozess ist angemessen detailliert mit einfachen Instruktionen beschrieben.
3	Der Prozess ist sehr detailliert und ausreichend beschrieben.

Neben dem Prozess kann in weiterer Folge auch gegebenenfalls der Input und der Output für alle oder eine Auswahl der einzelnen ENISA-Schritte mit derselben Metrik bewertet werden, was die Aussagekraft weiter erhöht, jedoch proportional den Zeitbedarf für die Bewertung ebenso. Da primär die Frage der methodischen Anwendbarkeit im Vordergrund stand, wurde die Prozessbewertung für diesen Zweck als ausreichend angesehen. Es wurde jeweils der entsprechende ENISA-Prozess-Schritt im zu untersuchenden Framework identifiziert und dabei die inhaltliche Substanz aus ExpertInnensicht bewertet. Tabelle 2 stellt dies am Beispiel der Einzelbewertung von ISO 31000 dar. Diese hält zur Dokumentationszwecken sowohl die identifizierten Teile der ISO 31000, welche die referenzierten ENISA-Prozess-Schritte implementieren, als auch zusätzlich die Gründe für Abstufungen in der Bewertung fest. Teilweise finden sich die gesuchten Referenzschritte in mehreren Abschnitten des untersuchten Frameworks und müssen dann in Summe gelesen werden, wenn kein 1:1-Mapping möglich ist.

Tab. 2: Einzelbewertung der ISO 31000

Stage A – Definition of Scope and Framework			
#	Process Name	Score	ISO 31000 Step(s)
P.1	Definition of external environment	1,0	5.3 Establishing the context; 5.3.2 Establishing the external context
P.2	Definition of internal environment	1,0	5.3 Establishing the context; 5.3.3 Establishing the internal context
P.3	Generation of risk management context	1,5	5.4.3 Establishing the context of the risk management process
P.4	Formulation of risk criteria	1,5	5.3.5 Defining risk criteria
Stage B -Risk Assessment			
#	Process Name	Score	ISO 31000 Step(s)
P.5	Identification of risks	1,5	5.4 Risk assessment; 5.4.2 Risk identification
P.6	Analysis of relevant risks	1,5	5.4 Risk assessment; 5.4.3 Risk analysis
P.7	Evaluation of risks	1,5	5.4 Risk assessment; 5.4.4 Risk evaluation
Stage C - Risk Treatment			
#	Process Name	Score	ISO 31000 Step(s)
P.8	Identification of options	1,0	5.5.2 Selection of risk treatment options
P.9	Development of action plan	1,5	5.5.2 Selection of risk treatment options; 5.5.3 Preparing and implementing risk treatment plans
P.10	Approval of action plan	0,5	5.5.3 Preparing and implementing risk treatment plans; 5.6 Monitoring and Review; 5.7 Recording the risk management process
P.11	Implementation of action plan	1,0	5.5.3 Preparing and implementing risk treatment plans
P.12	Identification of residual risks	0,5	5.5 Risk treatment; addressing non- treated risks only
Stage D - Risk Acceptance			
#	Process Name	Score	ISO 31000 Step(s)
P.13	Risk acceptance	0,5	Touched on by 5.5 Risk treatment 5.5.3 Preparing and implementing risk treatment plans
Stage E - Risk Monitoring and Review			
#	Process Name	Score	ISO 31000 Step(s)
P.14	Risk monitoring and reporting	1,5	Risk Management Process: 5.6 Monitoring and review; Framework: 4.5 Monitoring and review of the framework
Stage F - Risk communication, Awareness and Consulting			
#	Process Name	Score	ISO 31000 Step(s)
P.15	Risk communication, awareness and consulting	1,5	5.2 Communication and consultation; 4.2 Mandate and commitment

Die Punktevergabe erfolgte durch die ExpertInneneinschätzungen, wenngleich die ENISA-Methodik hier keine Handhabung von Zwischenergebnissen vorgibt. Die Gleichförmigkeit der

Ergebnisse wurde dadurch sichergestellt, dass die untersuchten Frameworks durch dieselben ExpertInnen bewertet wurden. Durch die sehr weiche Formulierung der Bewertungskriterien (siehe Tabelle 1) ergibt sich ein evidentes Kritikpotential, das im Abschnitt 0 diskutiert wird. Die Einzelergebnisse wurden dann in einem Netzdiagramm visualisiert (vgl. Abbildungen 4 bis 9), da hier zusätzlich Vergleiche in den einzelnen Prozess-Schritten möglich sind.

3.2 Gesamtvergleich der Methoden

Betrachtet man die Auswertungen der einzelnen in Abschnitt 2 beschriebenen Risikomanagementmethoden (Abbildungen 4 bis 9), so erkennt man, dass alle Methoden in den Bereichen der Risikobewertung (P.5 bis P.7 im ENISA-Prozess) durchwegs gut abschneiden. Allein die ISO 31000 hat aufgrund des sehr generischen Charakters hier keine markante Ausprägung (siehe Abbildung 4). Obwohl die jeweiligen Teile der ISO 31000 recht allgemein gehalten sind, beschreiben sie hinreichend detailliert die Hauptmerkmale der vorbereitenden Tätigkeiten für den Risikomanagementprozess und wie die Risikobewertung durchgeführt werden muss. Damit legt die ISO 31000 eine gute Basis für die Einführung eines Risikomanagementprozesses in einer Organisation.

Durch ihren Fokus auf IT-Risiken beschreibt die ISO/IEC 27005 (Abbildung 5) die Phasen der Bereichsbestimmung, Risikobewertung, sowie Risikokommunikation und -überwachung präziser als etwa die ISO 31000 und erreicht bei diesen Aspekten sogar die maximale Punkteanzahl. Ähnlich steht es hierbei um die NIST SP800-30 (Abbildung 6), wo ebenfalls diese Phasen besonders ausgeprägt sind. Hingegen fehlt die Phase der Risikobehandlung und -akzeptanz (P.8 bis P.13 im ENISA-Prozess) in der NIST SP800-30 jedoch vollständig. Der Grund hierfür ist die Aufteilung des Risikomanagement-Prozesses der NIST auf die Special Publications SP800-30 und SP800-39. Die jeweiligen Komponenten sind in der SP800-39 genauer beschrieben.

Bei OCTAVE Allegro (siehe Abbildung 9) – ebenso wie bei der ISO/IEC 27005 (siehe Abbildung 5) – sind die ersten Schritte der Risikobehandlung stärker implementiert als die übrigen. Bei OCTAVE Allegro ist anzumerken, dass die Methode generell stark auf die Schritte P.4 bis P.9 fokussiert, wodurch Teile der Risikobehandlung sowie die Risikokommunikation, -überprüfung und die Bereichsbestimmung nur marginal oder gar nicht behandelt werden.

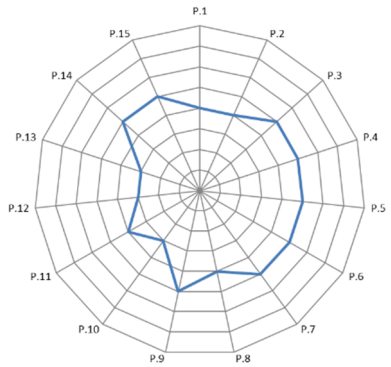

Abb. 4: Evaluierungsergebnis ISO 31000

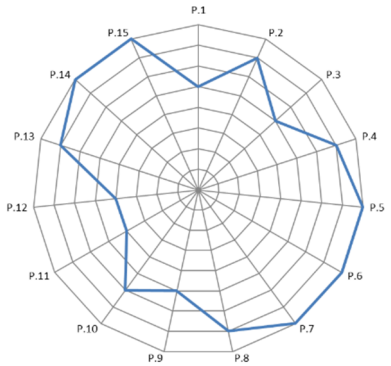

Abb. 5: Evaluierungsergebnis ISO/IEC 27005

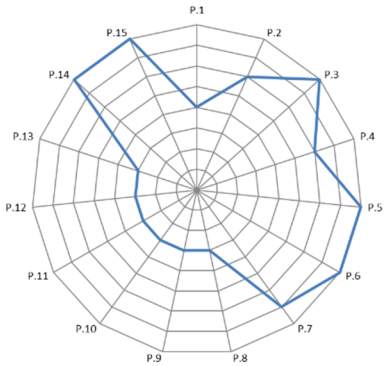

Abb. 6: Evaluierungsergebnis NIST SP800-30

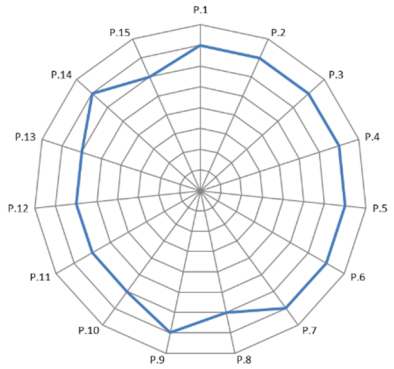

Abb. 7: Evaluierungsergebnis COBIT 5 for Risk

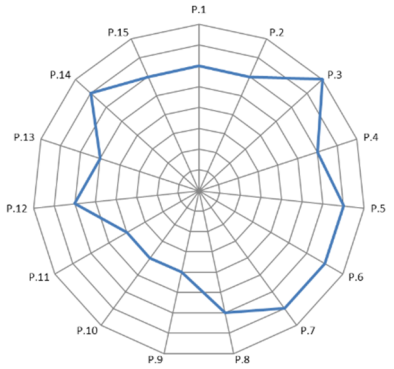

Abb. 8: Evaluierungsergebnis COSO ERM 2017

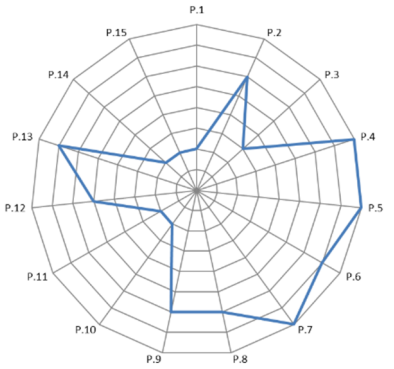

Abb. 9: Evaluierungsergebnis OCTAVE Allegro

Als Vertreter eines typischen Top-Down-Ansatzes hat COSO ERM 2017 (Abbildung 9) als das neueste Framework einen starken Fokus auf Strategie, Geschäftsziele sowie Leistungsvermögen und betont sehr stark die Integration in die bestehende Organisationsstruktur als auch die Risikoidentifikation. Etwas rudimentärer sind dann die Phasen hinsichtlich der Umsetzung der Response-Maßnahmen gestaltet, was die signifikant geringere Punkteanzahl bei den Schritten P.9 bis P.11 erklärt.

Mit einer durchwegs hohen Punktzahl schneidet COBIT 5 for Risk (Abbildung 8) am besten ab. Dies ergibt sich vor allem durch die praxisnahe Gestaltung des Rahmenwerks. Wie in Abschnitt 2.4 bereits kurz angemerkt, legt COBIT 5 for Risk einen starken Fokus darauf, Informationen aus verschiedenen Funktionsbereichen einer Organisation sowie aus unterschiedlichen Organisationssichten zu sammeln und diese Informationen in die Kontextbildung, Risikobewertung sowie die kontinuierliche Überwachung und Kommunikation mit den Entscheidungsträgern zu integrieren. Dadurch werden alle 15 Schritte in den sechs Phasen des ENISA-Prozesses gleichermaßen detailliert beschrieben und ermöglichen so eine direkte Umsetzung in einer Organisation.

3.3 Kritische Betrachtungen

Wesentliche Zielsetzung bei der Anwendung des Methodenvergleichs ist die Hilfestellung in der Praxis, also als tatsächliche Entscheidungshilfe für eine Organisation, welches Risikomanagementframework am besten für die konkrete Situation und dem Reifegrad passt, um diese aufzusetzen und zu implementieren. Ebenfalls wäre eine Erneuerung des Methodenvergleichs aus dieser Argumentation heraus zu rechtfertigen. Wie sich bei der simplen Wiederdurchführung anhand der ENISA-Kriterien aus dem Jahr 2006 zeigt, liegt ein starker Fokus des ENISA-Methodenvergleichs insbesondere in der Abschwächung (Mitigation) der Risiken. Im Umkehrschluss stellt sich die Frage, ob die anderen Phasen im Risikomanagementlebenszyklus nach aktuellem Forschungsstand noch repräsentativ sind, da sich im Laufe der Zeit auch der Fokus hin zur Prävention verändert hat. Somit müssen auch ex-post die Bewertungskriterien auf ihre Praxistauglichkeit hin hinterfragt werden, ob diese das in der bestehenden Form auch leisten und eine entsprechende Treffsicherheit auch gegeben ist.

Grundsätzlich hängt die Auswahl aus Sicht einer Organisation basierend auf den argumentativ-deduktiven Erkenntnissen der Autoren nach der erfolgten Wiederdurchführung des Methodenvergleichs von folgenden möglichen Entscheidungskriterien ab:

- **Ausgestaltungsdetaillierungsgrad**. Dieser reicht von sehr generisch (z.B. ISO 31000) bis sehr restriktiv und konkret (z.B. OCTAVE). Einerseits ist ein generischer Zugang zwar flexibel, lässt allerdings auch viel offen und gibt keine Antworten auf konkrete Praxisfragen. Die dominierende Frage, die sich einem Risikoverantwortlichen eines kleinen oder mittleren Unternehmens (KMU) stellt („Welche typischen Risiken sind zu betrachten?“) wird von den Frameworks nur unzureichend beantwortet. Zusätzlich konkrete Anwendungsmodule zu generischen Frameworks wären aus Praxissicht sinnvoll.
- **Organisationsgröße und -komplexität**. Es ist sowohl bei Planung und Implementierung von Risikomanagementstrukturen ein signifikanter Unterschied gegeben, ob dabei auf eine Konzernstruktur zurückgegriffen werden kann oder ein KMU adressiert wird. Der Ausgestaltungsbedarf für KMUs kann bei generischen Frameworks immens sein. Es fehlen konkrete auf die Unternehmensgröße hin justierte Risikomanagementvorgaben, die einfach und rasch umgesetzt werden können und welche die Kapazität der Organisation nicht überfordern.
- **Branchenrisiken**. Allein bei der jeweiligen Branchenumgebung entstehen mehr oder weniger Risiken (z.B. Handelsbetrieb im Gegensatz zu einer Bank oder Versicherung), die durch das Risikomanagementframework möglichst vorab erkannt und adressiert werden müssen. Die Anforderung auf entsprechende Vorbereitung wird in den einzelnen Branchen unterschiedlich formuliert. Auch hier fehlen hilfreiche Sammlungen typischer Branchenrisiken, die rasch in Form von Checklisten in die Risikomanagementüberlegungen einfließen könnten. COBIT for Risk bietet beispielsweise Hilfestellung bei der Szenarienauswahl, um mögliche Risiken zu identifizieren.
- **Risikomanagement-Knowhow**. Größere Unternehmen können sich dezidierte Rollen in ihrer Organisation leisten, welche das Risikomanagementsystem aktiv ausgestaltet. Kleinere Organisationen haben die Zeit, Energie und mitunter auch das Fachwissen hierfür nicht, da die wenigen Mitarbeiter primär auf das Kerngeschäft ausgerichtet sind. KMUs brauchen praktikable Lösungen, also ganz konkrete Vorgaben, wie sie aus Prozess-Sicht z.B. OCTAVE bietet, und weniger generische Frameworks, die vorbereitend erst ausgestaltet werden müssen.
- **Ressourceneinsatz**. Ausgehend von der Notwendigkeit und der beabsichtigten Intensität, Risikomanagement in der Organisation zu betreiben, sind die zur Verfügung stehenden Mittel in Form von Zeit und Geld ebenso formgebend.

Die Entscheidungskriterien müssten aus Sicht der Autoren demnach auf diese Anwendungsaspekte und Zielsetzungen hin effektiver fokussiert werden, um die Praktikabilität in der Praxis besser beurteilen zu können. In dem Zusammenhang muss auch diskutiert werden, ob die jeweiligen Bewertungen der Frameworks anhand der 15 Kriterien exakter an spezifischen Aussagen, möglichst in Form von Entscheidungsfragen, formuliert werden können. Die aktuellen ENISA-Bewertungsskalen lassen – dies ist wohl das eklatanteste Manko der Einzelbewertung – zu viel Interpretationsspielraum, was möglicherweise der angestrebten Objektivität zuwiderläuft. Die einzelnen Detailergebnisse der Bewertung können durchaus in berechtigter Kritik stehen und sind somit angreifbar.

Es wären z.B. gewichtete Fragenkombinationen in überschaubarer Anzahl denkbar, um das analysierte Framework eindeutig, zweifelsfrei und klar bewerten zu können, wobei auch die Formulierung von Kriterien für Zwischenwerte sinnvoll erscheinen.

4 Conclusio

Risikomanagement ist geprägt durch verschiedene Frameworks mit unterschiedlichen Ausrichtungen, die eine Vielzahl von Methoden und ihrerseits jeweils eigenständigen Modellen propagieren, sowie jeweils spezifische Werkzeuge für die Umsetzung vorschlagen. Deren Stoßrichtungen sind durchaus ähnlich gelagert, jedoch in weiterer Folge unterschiedlich ausgestaltet und demnach wird auch deren Anwendungsaspekt mehr oder weniger betont. Nichtsdestotrotz stellen sie allesamt unter anderem rasch anwendbare Risikomanagement-Methoden vor. Eine Überführung der Daten bei einem Wechsel ist momentan nicht ohne weiteres umsetzbar, somit sind keine interorganisatorischen Vergleiche möglich. Ein Metamodell gibt es momentan nicht, diesbezügliche Ansätze und Überlegungen sind aber Gegenstand der aktuellen Forschung der Autoren [LaQu17] [Latz16]. In der Praxis bleiben in den Organisationen im wirtschaftlichen Umfeld die einmal eingesetzten Methoden aus Praktikabilitätsüberlegungen heraus nachhaltig bestehen und der eingeschlagene Weg wird prolongiert, auch wenn sich später mitunter die Rahmenbedingungen für eine bestimmte Auswahl verändern. Eine „One-Solution-fits-it-all"-Eigenschaft eines Risikomanagement-frameworks kann erwartungsgemäß mit dem Methodenvergleich nicht erfüllt werden. Auch eine Exzerpierung nach dem Baukastenprinzip, also je nach Komponente das Auswählen des jeweils optimalen Frameworkteils, führt nicht zum gewünschten Effekt, da die Bausteine nicht kompatibel zueinander sind und beliebig ausgetauscht werden können. Dem widerspricht nicht zuletzt das jeweilige Begriffskonzept, das mitunter gleichlautend, jedoch substantiell durchaus unterschiedliche Semantik aufweist und somit untereinander nicht konsistent ist. Diese fundamentalen Differenzen beeinflussen dann auch die übergeordnete Vergleichbarkeit der Risikomanagementframeworks selbst. In dieser Hinsicht sind die Frameworks atomar, also nicht teil- und beliebig kombinierbar. Letztlich ist die Entscheidung für die Anwendung eines bestimmten Risikomanagementmodells eine fundamentale Unternehmensentscheidung, die man bewusst setzen soll. In dieser Phase benötigt man probate Auswahlmechanismen.

Sämtliche Methoden weisen Mankos auf, die der Methodenvergleich in dieser Form nicht thematisiert. Beispielsweise sind Kaskadeneffekte, also Auswirkungen von Vorfällen, die andere Risiken auslösen und sich kumulieren, derzeit gar nicht oder nur schwer abbildbar, wenngleich sehr wünschenswert. Naturgemäß liegt dies an der Komplexität durch den impliziten Permutationsfaktor, der rasch in Unübersichtlichkeit mündet. Ein fundamentales Problem im Risikomanagement ist der notgedrungene Umgang mit Unsicherheit. Dieser erfordert eine qualitative Einschätzung, da quantitative Bewertungen (Häufungszahlen) zumeist nicht vorliegen. Die gewählte Risikomanagementmethode muss eine Ex-post-Justierung durch eine vorgegebene Feedbackschleife zulassen, um die Erfahrung aus dem Risikoereignis zur Anpassung der Risikofaktoren aktiv nutzen zu können. Neuere Methoden bei der Bewertung von Risikofaktoren, z.B. durch Anwendung von Spieltheorie – helfen die Vorhersagequalität sukzessive zu verbessern [RaSc18]. Daher muss der Methodenvergleich in aktualisierter Form diese neueren Aspekte berücksichtigen, um den neueren Anforderungen aus akademischer und praktischer Welt Rechnung zu tragen.

Der hier durchgeführte, aktualisierte Vergleich des ENISA-Methodenvergleichs aus dem Jahr 2006 vergleicht die objektivierten Schlüsselaspekte der Prozess-Schritte und gibt insofern eine gute Auskunft über die Schwerpunkte der jeweils untersuchten Risikomanagement-frameworks. Je nach Erfordernis der Organisation kann so das am besten passende Framework auf Basis der Prozessunterstützung ausgewählt werden. In dieser Detailtiefe lässt sich

zumindest die Intensität der Hilfestellung bei der Implementierung der einzelnen Schritte gut abschätzen. Für einen Praxisanwendungsbezug, insbesondere für KMUs, müssten jedoch in einem folgenden Schritt zusätzlich die Bewertungskriterien punktuell angepasst werden, auch im Hinblick auf zukünftige Erfordernisse, denen das Risikomanagement zukünftig ausgesetzt sein wird, um eine nachhaltig valide Auswahl für die Organisation treffen zu können. Zur Erhöhung der Aussagekraft der Bewertungen können zusätzlich die Bewertungspunkte anhand klarer Fragestellungen in Form von Entscheidungsfragen oder gewichteten Kombinationen davon entwickelt werden. Somit wäre der strukturelle Rahmen des ENISA-Methodenvergleichs ebenso aktualisiert und bietet dann zusätzlich auch einen echten Praxisnutzen bei der Entscheidungsfindung für das optimale Risikomanagement-Framework.

Danksagung

Dieser Beitrag wurde durch das FFG/KIRAS Projekt „GENESIS - Guideline für Behörden und KMU-Anbieter strategischer Services zur risiko-orientierten Implementierung der NIS-Richtlinie ” (Projekt-Nr. 860636) finanziert.

Literatur

[ADSW05] C. Alberts, A. Dorofee, J. Stevens, C. Woody: OCTAVE-S Implementation Guide (Technical Report CMU/SEI-2003-HB-003). Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA, 2005.

[AlDo01a] C. Alberts, A. Dorofee: OCTAVE Method Implementation Guide Version 2.0 Volume 1: Introduction.Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA, 2001.

[AlDo01b] C. Alberts, A. Dorofee: OCTAVE Method Implementation Guide Version 2.0 Volume 2: Preliminary Activities. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA, 2001.

[Bund13] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz Catalogue, English Version (2013).

[CoPw17] COSO, PwC: Enterprise Risk Management – Aligning Risk with Strategy and Performance (2017).

[Enis06] ENISA ad hoc working group on risk assessment and risk management: Inventory of Risk Assessment and Risk Management Methods (2006).

[Info12a] Information Systems Audit and Control Association: COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, USA, 2012.

[Info12b] Information Systems Audit and Control Association: COBIT 5 – Enabling Proccesses. Rolling Meadows, USA, 2012.

[Info13] Information Systems Audit and Control Association: COBIT 5 for Risk. Rolling Meadows, USA, 2013.

[Inte00] International Organization for Standardization: ISO/IEC 17799: Information technology – Code of practice for information security management (2000).

[Inte04] International Organization for Standardization: ISO/IEC 13335-1: Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management (2004).

[Inte09] International Organization for Standardization: ISO 31000: Risk Management – Principles and Guidelines (2009).

[Inte11] International Organization for Standardization: ISO/IEC 27005: Information technology – Security techniques – Information security risk management (2011).

[Iso13] International Organization for Standardization: ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. 2nd Ed. (2013)

[LaQu17] M. Latzenhofer, G. Quirchmayr: RMDM – A Conceptual ICT Risk-Meta-Data-Model – Applied to COBIT for Risk as underlying Risk Model. In: SECUREWARE 2017 117-124.

[Latz16] M. Latzenhofer: Ein Meta-Risiko-Datenmodell für IKT. P. Schartner (Hrsg.): DACH Security 2016, 161-173.

[Nati10] National Institute of Standards and Technology: NIST SP800-37 Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach (2010).

[Nati11] NIST SP800-39 Managing Information Security Risk: Organization, Mission, and Information System View (2011).

[Nati12] NIST 800-30: Guide for Conducting Risk Assessments. In: National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Joint Task Force Transformation Initiative Information Security (Hrsg.) , Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, USA (2012).

[RJLW07] Richard A., Caralli ; James F., Stevens ; Lisa R., Young ; William R., Wilson: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process (Technical Report CMU/SEI-2007-TR-012). Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA, 2007.

[StGF02] G. Stoneburner, A. Goguen, A. Feringa: NIST SP800-30 Risk Management Guide for Information Technology Systems (2002).

[Tech08] Technical Department of ENISA Section Risk Management and BOC Information Technology GmbH: Integration of Risk Management / Risk Assessment into Business Governance (2008).