ISMS-Risikomanagement in 45 Minuten[1]

[1] Mathias Dalheimer, November 2023

Das Risikomanagement ist ein zentraler Bestandteil eines *Informationssicherheitsmanagementsystems (ISMS)* — und ich hatte anfangs Schwierigkeiten, ein zusammenhängendes Bild im Kopf zu entwickeln. Rückblickend habe ich einfach nicht genug auf die Bedeutung einzelner Begriffe geachtet. Und ich hatte kein Beispiel, anhand dessen ich eine Variante eines Risikomanagementprozesses durchdenken konnte. Daher versuche ich im Folgenden, das Risikomanagement eines ISMS zwar kompakt, aber trotzdem verständlich darzustellen. Ein beispielhaftes Risikomanagement verdeutlicht die Konzepte.

Risikomanagement hat das Ziel, Informationssicherheits-Risiken[2] einer Organisation zu verstehen und angemessen zu behandeln. Die entsprechenden Normen[3] beschreiben Vorgehensweisen, die man nutzen kann, um Risiken systematisch zu erkennen, einzuordnen und angemessen zu behandeln. Auch wenn sich das Risikomanagement der einzelnen Normen leicht unterscheidet: Die grundlegenden Konzepte sind überall gleich.

[2] Risiko: Auswirkung von Unsicherheit auf Ziele

[3] *ISO/IEC 27005: Information security risk managment*. Beuth Verlag, 2022; and *BSI Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz*. Bundesamt für Sicherheit in der Informationstechnik, 2017

Hinweis: In einem Kasten wie diesem entsteht ein Risikomanagement-Beispiel. Das Beispiel stellt nicht alle Risiken dar, es soll lediglich die grundlegenden Konzepte verdeutlichen.

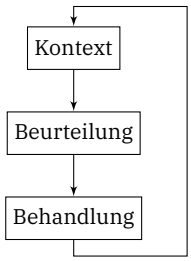

Abbildung 1: Fortlaufendes Risikomanagement

1 Begriffe & Konzepte

Im Bereich der Informationssicherheit sind Beeinträchtigungen der *Vertraulichkeit (C)*[4], der *Integrität (I)*[5] sowie der *Verfügbarkeit (A)*[6] die hauptsächlichen Risiken. Diese Risiken beziehen sich primär auf *Informationswerte*[7] und nur nachgelagert auf *Informationsträger*[8] wie Computersysteme oder auch Papier.

Generell können Risiken nicht komplett vermieden werden. Ziel ist daher, die Risiken durch geeignete *Maßnahmen*[9] auf ein akzeptables Maß zu reduzieren. Ein *Restrisiko*[10] verbleibt allerdings immer. Es soll jedoch unter dem *Risikohunger*[11] der Organisation liegen.

Der *Kontext*[12] der Organisation beeinflusst das Risikomanagement maßgeblich. Unterschiedliche Organisationen kommen daher zwangsläufig auch auf unterschiedliche Herangehensweisen im Umgang mit Informationssicherheitsrisiken.

Da sich der Kontext auch ständig ändert, wird der Risikomanagementprozess zu keinem fertigen Endergebnis führen. Stattdessen durchläuft der Risikomanagementprozess die Schritte *Evaluation des Kontexts*, *Risikobeurteilung* und *Risikobehandlung* fortlaufend (vgl. Abb. 1).

[4] Vertraulichkeit (confidentiality): Eigenschaft, dass Information unbefugten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder offengelegt wird

[5] Integrität (integrity): Eigenschaft der Richtigkeit und Vollständigkeit

[6] Verfügbarkeit (availability): Eigenschaft zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat

[7] Informationswert (primary asset): Informationen, die für die Organisation einen Wert besitzen

[8] Informationsträger (secondary asset): Medium, auf dem ein Informationswert gespeichert ist

[9] Maßnahme (Control): Mittel zur Veränderung von Risiken

[10] Restrisiko: Das verbleibende Risiko nach Maßnahmen

[11] Risikohunger: Das Risikoniveau, das die Organisation bereit ist, zu akzeptieren

[12] Kontext: Das interne und externe Umfeld einer Organisation

Kontext: Die CyberMechanics gGmbH (kurz: CM) ist ein Forschungsdienstleister mit dem Schwerpunkt auf der Weiterentwicklung und Kundenanpassung des Rockwell Retro Encabulators. Sie ist bekannt für innovative Zusatzaggregate rund um den Retro Encabulator und hält mehrere Patente. Die CM geht davon aus, dass ihre gegenwärtigen Forschungstätigkeiten zu weiteren Patenten führen werden.
Als Forschungsdienstleister arbeitet sie weltweit mit Kunden aus der Automobil-, Luftfahrt- und Raumfahrtindustrie zusammen. Gleichzeitig bewirbt sie sich auf öffentlich geförderte Projekte und geht Forschungspartnerschaften mit Universitäten ein.
CM ist eine teils öffentlich finanzierte Gesellschaft mit einem Jahresumsatz von 50 Mio. Euro. Sie bietet ihren 400 Angestellten weitgehende Freiheit, denn: Kreative Problemlösungen erfordern freies Denken und Arbeiten. Die CM ist gewohnt, für innovative Forschung auch Risiken einzugehen.
Die Zunahme von Informationssicherheitsvorfällen sowie die gestiegenen Anforderungen aus Lieferantenaudits zwingen die Geschäftsleitung nun, ein ISMS einzuführen. Im Hinblick auf Managementsysteme (z.B. ISO 9001, ISO 27701, ...) hat die CM bislang keine Erfahrungen.

2 Risikobeurteilung

Die *Risikobeurteilung* bestimmt Informationswerte, identifiziert Bedrohungen und Schwachstellen, leitet mögliche Konsequenzen ab und bewertet diese. Die Risikobeurteilung durchläuft die Schritte Risikoidentifikation, Risikoanalyse und Risikobewertung, vgl. Abb. 2.

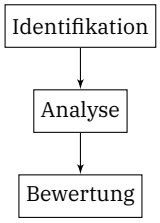

Abbildung 2: Schritte der Risiskobeurteilung

2.1 Risikoidentifikation

Die *Risikoidentifikation* soll zunächst die Informationssicherheitsrisiken identifizieren. Dabei finde ich es hilfreich, mit einem Verzeichnis der Informationswerte zu arbeiten[13]. In Gesprächen mit den *Risikoeignern*[14] können Risiken identifiziert und entsprechende Szenarien abgeleitet werden.

Ein Informationssicherheitsrisiko besteht immer aus einer *Schwachstelle*[15] und einer *Bedrohung*[16]. Ohne Bedrohung ist eine Schwachstelle ohne Bedeutung, daher werden diese Fälle üblicherweise nicht explizit betrachtet.

[13] Eine andere Herangehensweise ist, mit einem Verzeichnis der Informationsträger zu beginnen. Erscheint mir allerdings aufwändiger.

[14] Risikoeigner: Verantwortlichen für Informationswerte

[15] Schwachstelle (vulnerability): Schwäche eines Wertes.

[16] Bedrohung (threat): Ausnutzbarkeit einer Schwäche.

Risikoidentifikation: In Workshops mit den Führungskräften der Unternehmensbereiche wurden die wesentlichen Informationswerte identifiziert sowie Schwachstellen und Bedrohungen zugeordnet:

Nr.	Informationswert	Schwachstelle	Bedrohung	CIA?
1	Forschungsdaten vor Patentanmeldung	Speicherung auf internem Fileshare, jedem Mitarbeiter zugänglich	Exfiltration durch Innentäter	C
2		Nutzeradministrierte Laptops ohne Backup und Festplattenverschlüsselung	Verlust Laptop	C, A
3		Fehlende Backups	Ransomware, Irrtümliche Dateilöschung	I, A
4	Personaldaten	Papiergestützte Prozesse	Keine Vernichtung bei Entsorgung	C
5			Unterlagen nach Arbeitsende zugänglich	C
6	Projektdaten (vertraulich)	Offenlegung	Verlust von mobilen Datenträgern (z.B. USB-Stick)	C
7	Projektdaten (öffentlich)	Offenlegung	Verlust von mobilen Datenträgern	C
...				

Das Management bemerkt außerdem, dass viele Risiken projektbezogen unterschiedlich gehandhabt werden müssen (siehe Nr. 6 und 7). Zusätzlich zu obiger Risikoidentifikation wird daher eine verbindliche Projekt-Risikobeurteilung vor Abschluss eines Projektvertrags eingeführt. Diese soll im Projekt einerseits Flexibilität bewahren und andererseits auch entstehende Projektrisiken durch projektspezifische Maßnahmen sinnvoll behandeln.

2.2 Risikoanalyse

Die Risikoanalyse schätzt die Folgen bei Eintritt eines Risikos ab. Sie kann quantitativ[17] und qualitativ durchgeführt werden. Eine quantitative Analyse bewertet ein Risikoniveau monetär: Die Kosten für einen Vorfall werden unter Berücksichtigung der Eintrittswahrscheinlichkeit ermittelt[18]. Sind Risiken nur schwer monetär bewertbar, bietet sich eine qualitative Risikoanalyse an: Die Risiken werden in Klassen eingeordnet. Beide Verfahren können auch kombiniert werden: Beispielsweise kann bei hohen (qualitativen) Risiken zusätzlich eine quantitative Analyse durchgeführt werden, um die Kosten eines Vorfalls besser einschätzen zu können.

Die qualitative Risikoanalyse dominiert im Bereich der ISMS, da sie einfacher zu handhaben ist. Unabhängig von der Systematik der Risikoanalyse muss aber vor der ersten Risikoanalyse ein einheitlicher Bewertungsmaßstab sowie der Risikohunger der Organisation festgelegt werden. Im weiteren Verlauf der Risikoanalyse wird dann dieses Bewertungsschema verwendet, um unterschiedliche Risiken miteinander zu vergleichen und

[17] Ding Tan. Quantitative Risk Analysis Step-By-Step. `https://www.sans.org/white-papers/849/`. SANS Institute White Paper, Zugriff am 24.10.2023

[18] Die *jährliche Verlusterwartung* (anualized loss expectancy, ALE) ist eine oft genutzte Kennzahl quantitativer Risikoanalysen. Zur Berechnung siehe das SANS White Paper.

letztlich Maßnahmen zu priorisieren.

Bewertungsmaßstab: Die CM bevorzugt ein pragmatisches Schema zur Risikobewertung. In Abstimmung mit der Geschäftsleitung wird eine qualitative Risikoklassifizierung eingeführt: A für hohes Risiko, B für mittleres Risiko, C für niedriges Risiko. Eintrittswahrscheinlichkeit und potentielle Schadenshöhe werden zur Einschätzung von Risiken herangezogen. Die Zuordnung wird wie folgt festgelegt:

Schadenshöhe/ Anteil Jahresumsatz	Eintrittswahrscheinlichkeit selten	gelegentlich	häufig
>15 %	A	A	A
10–15 %	B	A	A
5–10 %	C	B	B
0–5 %	C	C	B

Für die Eintrittswahrscheinlichkeit gilt: Selten entspricht einem Vorfall alle zehn Jahre, gelegentlich alle zwei Jahre und häufig mindestens einmal im Jahr.
Die CM geht, gemessen am Jahresumsatz, eher hohe Risiken ein. Der Risikohunger wird in obigem Schema wie folgt festgelegt:

1. A-Risiken müssen vermieden werden.
2. B-Risiken sollen vermieden werden. Lässt sich ein B-Risiko nicht vermeiden, so muss die Geschäftsleitung das Risiko explizit akzeptieren.
3. C-Risiken gehören zum normalen Geschäft und werden in der Regel ohne weitere Maßnahmen akzeptiert.

2.3 Risikobewertung

In der Risikobewertung werden die Ergebnisse der Risikoanalyse mit dem Risikohunger der Organisation verglichen. Falls das ermittelte Risiko über dem Risikohunger liegt, müssen Maßnahmen zur Risikobehandlung (siehe Abschnitt 3) ergriffen werden.

Risikoanalyse und Risikobewertung: Die oben identifizierten Risiken werden durch Informationssicherheitsbeauftragte (ISB) und Führungskräfte der CM anhand des Bewertungsmaßstabs wie folgt eingeordnet:

Nr.	Anteil Jahresumsatz	Häufigkeit	Risikoklasse
1	>15 %	selten	A
2	>15 %	gelegentlich	A
3	>15 %	selten	A
4	0–5 %	selten	C
5	0–5 %	selten	C
6	5–10 %	gelegentlich	B
7	0–5 %	gelegentlich	C
...			

Aus der Klassifizierung kann direkt abgelesen werden, dass die Risiken im Zusammenhang mit noch nicht zum Patent angemeldeten Forschungsdaten erheblich sind (siehe Nr. 1–3). Entsprechende Maßnahmen müssen im Rahmen der Risikobehandlung priorisiert umgesetzt werden.
Außerdem sind Risiken aus dem Projektgeschäft (siehe Nr. 6+7) je nach Projekt unterschiedlich zu bewerten. Entsprechende Maßnahmen werden im Rahmen der Projektrisikobehandlung festgelegt. Zur besseren Einschätzung der Projektrisiken müssen die Projektleiter vor Angebotsabgabe einen Screening-Fragebogen beantworten. Anhand des Fragebogens analysiert der ISB die Risiken analog zu obiger Systematik und berät zu notwendigen Maßnahmen.

3 Risikobehandlung

Die Risikobehandlung baut auf den Ergebnissen der Risikobewertung auf und setzt Maßnahmen ein, um zu hohe Risiken zu reduzieren. Dabei können technische Maßnahmen[19], rechtliche Maßnahmen[20], administrative Maßnahmen[21] sowie Führungsmaßnahmen[22] eingesetzt werden. Die meisten ISMS-Rahmenwerke unterstützen durch umfangreiche Maßnahmenkataloge[23]. Je nach ISMS-Rahmenwerk müssen diese komplett umgesetzt werden (TISAX/VDA ISA) oder können in weiten Teilen an die Organisation angepasst werden (ISO 27001).

Es gibt vier grundlegende Möglichkeiten, Risiken zu behandeln (vgl. Abb. 3):

1. *Risikomodifikation*: Das Risiko wird durch geeignete Maßnahmen so verändert, dass das verbleibende Restrisiko unter dem Risikohunger liegt.

2. *Risikoakzeptanz*: Risiken, die unterhalb des Risikohungers der Organisation liegen, können einfach akzeptiert werden.

3. *Risikovermeidung*: Die dem Risiko zugrunde liegende Aktivi-

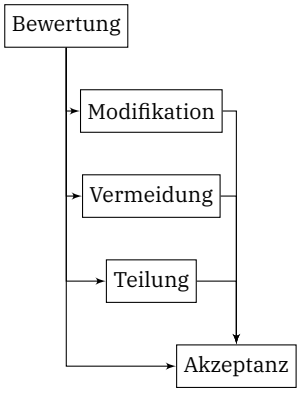

Abbildung 3: Optionen der Risikobehandlung

[19] z.B. Firewalls, Alarmanlagen

[20] z.B. Haftungsbegrenzung in AGB, Verpflichtung von Beschäftigten auf Geheimhaltung

[21] auf die Struktur der Organisation ausgerichtet, z.B. Aufgabentrennung oder Genehmigungsprozesse

[22] haben Personalbezug, z.B. Training, Coaching, Managementreviews und Audits

[23] *ISO/IEC 27002: Leitfaden für Informationssicherheitsmaßnahmen*. Beuth Verlag, 2022; *IT-Grundschutz-Bausteine*. Bundesamt für Sicherheit in der Informationstechnik, 2023; and *VDA ISA Katalog*. Verband deutscher Automobilindustrie, 2022

tät wird nicht durchgeführt, sodass das Risiko nicht weiter besteht.

4. *Risikoteilung*: Das Risiko wird mit einer dritten Partei geteilt. Dazu kann eine Versicherung abgeschlossen werden, oder ein Partnerunternehmen trägt einen Teil des Risikos.

Nach Abschluss der Risikobehandlung sollten alle identifizierten Risiken auf ein Maß unterhalb des Risikohungers begrenzt sein.

Risikobehandlung: Die CM orientiert sich bei der Behandlung der Risiken an vorhandenen ISMS-Rahmenwerken und allgemeinen Best Practices. Die folgenden Maßnahmen werden beschlossen:

Nr.	Risiko-veränderung	Maßnahmen
1	A → B	Rechtezuweisung nach Least Privilege-Prinzip, Richtlinien zu Kennworten und Informationsklassifizierung (Risikomodifikation)
2	A → C	Verpflichtende Vollverschlüsselung der Festplatten, verbindliches Backup, Passwortrichtlinie (Risikomodifikation)
3	A → C	Verbindliches, Ransomware-resistentes Backup (Modifikation), Versicherung (Teilung)
4	C	Risikoakzeptanz
5	C	Risikoakzeptanz, zusätzlich Einführung Clean Desk-Richtlinie, da auch an anderen Stellen sinnvoll
6	B → C	Haftungsbegrenzung in AGB (Risikoteilung), Richtlinie Informationsklassifizierung mit Hinweise zum Umgang mit mobilen Datenträgern (Risikomodifikation)
7	C	Risikoakzeptanz
...		

Das verbleibende B-Risiko (Nr. 1) wird von der Geschäftsleitung als akzeptabel angesehen, weil weitere Einschränkungen nicht praktikabel wären.

4 Hinweise zur praktischen Umsetzung

Generell gilt: Ein Risikomanagementprozess sollte die *wesentlichen* Risiken abdecken. Es ist nicht erforderlich, alle Risiken abzudecken. Wichtig ist aber, auf neue Risiken z.B. durch eine Änderung des Kontexts zu reagieren. Insofern sollte ein Risikomanagementprozess tendenziell eher schlank und agil als

umfassend und schwerfällig sein.

Es gibt im Markt viele Softwarewerkzeuge zur Verwaltung eines ISMS, und diese haben auch ein Modul zum Risikomanagement integriert. Gerade bei Einführung eines ISMS empfiehlt es sich jedoch, auf derartige Werkzeuge zu verzichten und die ISMS-Prozesse möglichst einfach und flexibel abzubilden. Andernfalls besteht die Gefahr, dass man das ISMS am Werkzeug orientiert — und nicht an den Anforderungen der Organisation.

Beispielsweise findet man in den wenigsten Risiskomanagement-Softwareprodukten eine Möglichkeit, projektbezogene Risiken zu verwalten. Oder aber das Risikomanagement wird auf der Basis der Informationsträger aufgebaut und nicht, wie oben, auf der Basis der Informationswerte. Die grundlegenden Designentscheidungen dieser Softwareprodukte sind nicht notwendigerweise falsch, allerdings schränken sie die Möglichkeiten für die Umsetzung eines ISMS zumeist unnötig ein.

Das oben gezeigte Risikomanagement kann problemlos in einem Excel-Dokument abgebildet werden. Eine mögliche Dokumentenstruktur besteht aus den folgenden Arbeitsblättern:

1. *Deckblatt* ggf. mit Hilfetexten, Dokumentenlenkung
2. *Definition* des Risikohungers sowie des Risikobewertungsmaßstabs. Dieser kann in Excel als 2D-Lookup-Tabelle angelegt werden, auf welche dann innerhalb der Risikobeurteilung zugegriffen wird. Somit ist durch den Aufbau der Tabelle sichergestellt, dass alle Risiken gleich behandelt werden.
3. *Verzeichnis* der Informationsträger. Auch hier empfehle ich aus Gründen der Wartbarkeit und Übersichtlichkeit die Verwendung von Klassen von Informationsträgern. Im Hinblick auf die Risikobehandlung bietet eine gerätescharfe Auflistung in den meisten Fällen keine Vorteile. Denn: Die Maßnahmen wie „Datenträgerverschlüsselung" beziehen sich ja auch auf komplette Geräteklassen und nicht nur auf einzelne Laptops.
4. *Risikobeurteilung*: Verzeichnis der Informationswerte mit ihren Risikoeignern inklusive Risikobeurteilung und Risikobehandlung. Das Verzeichnis verweist üblicherweise auf den Maßnahmenplan (s.u.). Innerhalb der Risikobeurteilung kann man auch mit „Klassen" von Risiken arbeiten, welche dann in einem separaten Prozess genauer bewertet werden (vgl. Nr. 6 & 7 im Beispiel).
5. *Risikobehandlung*: Dokumentation der Risikobehandlung (oft Maßnahmenplan genannt): Hier werden Maßnahmen gelistet, die für die Behandlung der vorher identifizierten Risiken notwendig sind. Die Maßnahmen können sich auch an Maßnahmenkatalogen aus den ISMS-Normen orientieren.

Ein Screening-Fragebogen für projektbezogene Risiken muss sich immer an den Anforderungen der Organisation orientieren. Erfahrungsgemäß unterscheiden sich die Kenntnisstände von ISB, IT-Mitarbeitenden und Projektleitern sehr stark, sodass eine möglichst einfache Sprache sowie Hilfetexte vorteilhaft sind. Leitfragen für einen Fragebogen können sein:

1. Werden personenbezogene Daten verarbeitet? Falls ja: Welche?
2. Können durch Missbrauch von Daten ungewöhnlich hohe Schäden entstehen?
3. Gibt es Abweichungen der Projektverträge von den risikomindernden Regelungen der AGBs, beispielsweise Wegfall der Haftungsbegrenzung? Gibt es projektspezifische Geheimhaltungsvereinbarungen?
4. Wird besondere/unübliche Hard- oder Software eingesetzt? Werden die Systeme durch die IT oder die Projektmitarbeitenden administriert?
5. Gibt es besondere Vorgaben zum Datenschutz oder der IT-Sicherheit, beispielsweise TISAX?

Die obigen Leitfragen sollen Projekte schnell auf ungewöhnliche Risiken hin untersuchen. Können alle Fragen mit „Nein" beantwortet werden, so ist mit hoher Wahrscheinlichkeit keine weitere Risikobeurteilung und -behandlung notwendig. Andernfalls können projektspezifische Maßnahmen zur Risikoreduktion in Absprache mit dem Projektleiter umgesetzt werden.