digital business excellence

Risikomanagement

Der Risiko-Prozess für KMUs im pragmatischen Ansatz

Version:	1
Autor:	Dr. M. Wolfensberger und Joël Bühler
Klassifikaton:	Public

Dr. Pascal Sieber & Partners AG
Bern | Zürich | +41 31 566 93 00 | www.sieberpartners.com

sieber & partners

Inhalt

1 Risikomanagement – ein pragmatischer Ansatz für KMUs

Wir alle managen Risiken. Mehr oder weniger professionell, in Freizeit und Beruf, im Internet, beim Sport – überall. Nur gehen wir eher selten mit einem konkreten Prozess und einem geordneten Verfahren an unserer Risikomanagement heran.

KMUs wissen oft, dass sie mit ihrer IT ein Risiko eingehen. Bei der Vielzahl der Bedrohungen ist klar, dass man eigentlich etwas tun sollte, aber oft ist nicht klar, wie sie vorgehen sollen. Einerseits, weil es völlig überzogen wäre, jedes Risiko administrieren zu wollen und andererseits, weil so ein Prozess mit dahinterliegenden Methoden und Techniken immer so sperrig daherkommt und im Grunde schon bei erster Betrachtung zu umständlich und vor allem teuer erscheint.

Das muss nicht sein.

Im Folgenden wird der Risikoprozess kurz und knapp erläutert und aufgezeigt, wie man auch als KMU ein pragmatisches und wirksames Risikomanagement aufbauen und beständig verfolgen kann.

2 Der Risiko-Management-Prozess

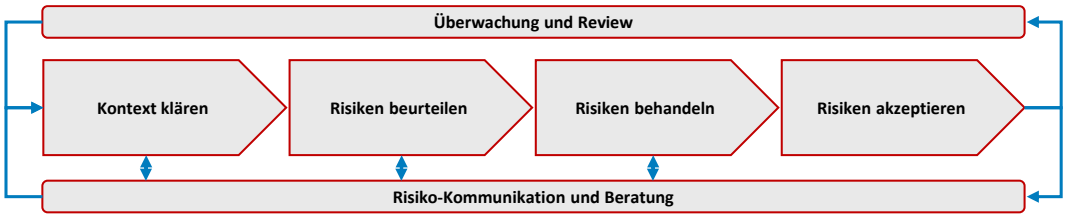


Abbildung 1: Risikoprozess nach ISO 27005

Der Kern des Risiko-Management-Prozesses besteht aus den vier aufeinanderfolgenden Phasen

- Situation und Anforderungen klären
- Risiken identifizieren und beurteilen
- Risiken behandeln
- (Rest-)Risiken akzeptieren und verfolgen

Damit ist der Durchlauf des Kernprozesses abgeschlossen. Aber natürlich sollte man es nicht bei einem Durchgang belassen. Der Prozess sollte in regelmässigen Abständen immer wieder durchlaufen werden, um den sich mit der Zeit ändernden Umständen oder Bedrohungen gerecht zu werden und neu auftauchenden Risiken zu begegnen. In welchen Abständen dies passieren soll, ist den Verantwortlichen der Organisation überlassen. Näheres hierzu im Abschnitt «Kontext und Anforderungen klären».

In der übergreifenden Phase «Überwachung und Review» wird dafür gesorgt, dass der Prozess richtig durchgeführt wird und Verbesserungen am Risiko-Management-Prozess dort eingeführt werden, wo sie tatsächlich Sinn machen.

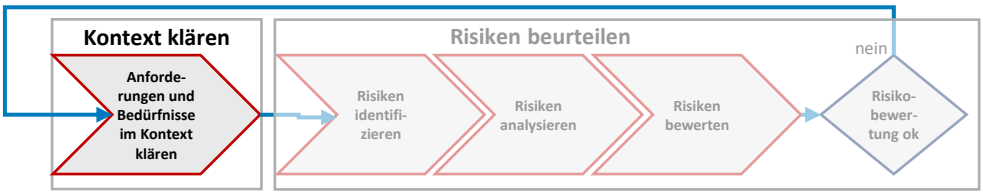
In der Basis-Phase «Kommunizieren, beraten und Bewusstsein schaffen» wird bei allen Betroffenen und Beteiligten anhaltend die Grundlage für das individuelle Mitwirken am Risikomanagement geschaffen und gepflegt: die Awareness. Hier wird der Awareness-Horizont der Organisation abgesteckt. Oft unterschätzt und nicht mit Technik aufzuwiegen: das Verhalten der Mitarbeiter:innen.

Der Risiko-Prozess wird von der verantwortlichen Rolle für alle bestehenden Risiken in ihren verschiedenen Stadien iterativ vorangetrieben.

Im Allgemeinen werden die Informationssicherheits-Risiken an einem regelmässig abgehaltenen Meeting als Traktandum mit aufgenommen und mit den Betroffenen und/oder Beteiligten besprochen.

Es kostet schon etwas, sich zu schützen. Es werden einige FTE-Prozente benötigt, um die Risiken zu erkennen, zu managen und zu verfolgen. Zur Durchführung des Risiko-Management-Prozesses ist der Einsatz eines Tools empfehlenswert, um die Komplexität und Verschiedenheit der Risiken im Griff zu behalten. Dazu genügt aber durchaus eine XL-Liste oder etwas ähnliches. Es muss nicht sofort ein weiteres teures Tool sein, das Spezialwissen erfordert und Service- und Lizenzkosten verursacht. Auch Einfaches kann gut und wirksam sein.

2.1 Kontext und Anforderungen klären



Die Klärungsphase geht dem eigentlichen Risiko-Prozess voraus. Hier soll mit Blick auf die Bedürfnisse und Anforderungen der im Organisations-Kontext identifizierten Anspruchsträger durchge-

führt werden. Hier steht die Frage nach dem Charakter der Organisationsaufgaben und -tätigkeiten im Vordergrund. Dies umfasst Themen wie das Verständnis für das Businessmodell, die Standorte, Markt-Leistungen und Lösungen wie auch die innere Organisation der Firma selbst. Ziel ist, alle Stakeholder und deren Bedürfnisse zu erfassen.

Business-Kontext

Das allgemeine Business-Kontext-Modell dient dazu, die Risiken im Unternehmens-Kontext zu identifizieren. Es bietet mit der Aufteilung des Kontexts in die Bereiche Kund:in (Leistungsempfänger:in), Zulieferer:in (Leistungserbringer:in), Mitarbeiter:in, gegenwärtige Cyber-Crime Bedrohungslage, Markt und Technologie und regulatorische und gesetzliche Rahmenbedingungen klar abgegrenzte Themenfelder, in denen man gezielter nach möglichen Stakeholdern, deren Schutzobjekten und -bedürfnissen und somit nach Risiken suchen kann.

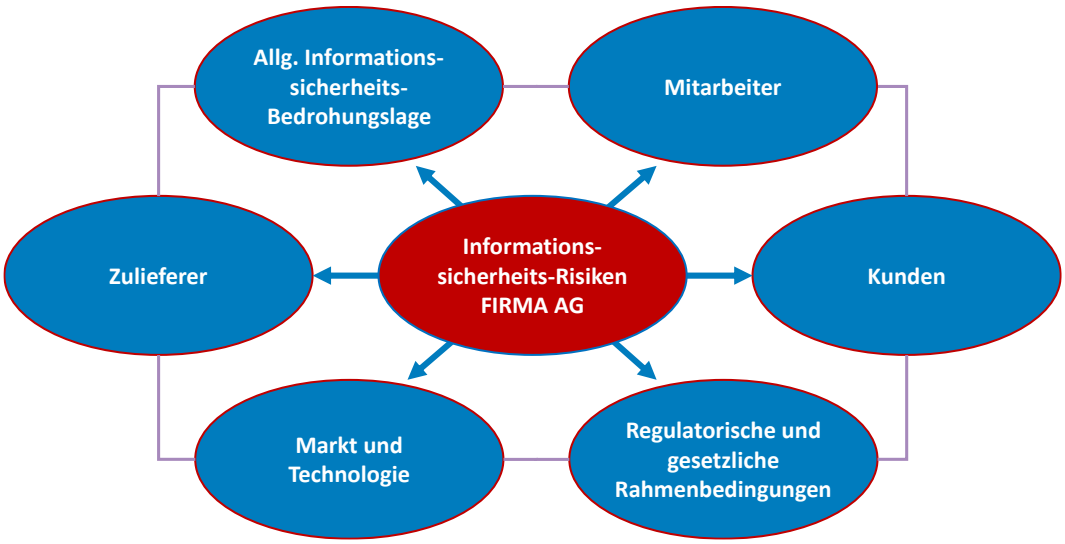
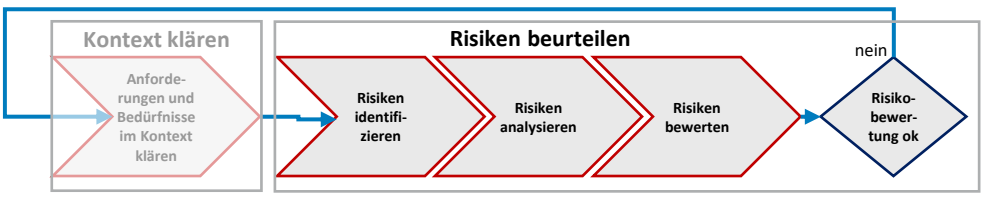


Abbildung 2: Risikobereiche im Unternehmens-Kontext

2.2 Risiken beurteilen



Diese Phase hat drei Schritte:

- Risiken identifizieren
- Risiken analysieren
- Risiken bewerten

2.2.1 Risiken identifizieren

Assets auf Bedrohungen prüfen

Im ersten Schritt werden bestehende Risiken identifiziert, indem bestimmte Asset-Kategorien (bzw. -Gruppen), Unterkategorien oder Assets, Prozesse, Personal, Leistungserbringerverträge, SLAs o.ä. im Rahmen von Risikoszenarien auf mögliche Bedrohungen oder bestehende Schwachstellen hin geprüft werden.

Risiko typisieren

Das Risiko sollte einem Kapitel oder Aspekt eines Gefährdungskatalogs oder einer Gefährdungsliste zugeordnet werden, damit eine Typisierung des Risikos und eine allfällige spätere Trendanalyse möglich ist.

Es bietet sich an, primär die aktuelle Gefährdungsliste G0 des BSI einzusetzen. Sie bietet eine breite Palette an Optionen zur Typisierung von Risiken. Es können auch weitere eigene Listen (Operative Gefährdungen, Projektgefährdungen o.ä.) zum Einsatz kommen.

Risiko-Eigentümer bestimmen

Wenn möglich wird bereits hier ein:e Risiko-Eigentümer:in bestimmt, die bzw. der bei der Analyse und Evaluation unterstützt und später die Verantwortung für die Risikovermeidungsaktivitäten übernimmt.

Bei Projektrisiken ist die bzw. der Projekteigentümer:in zumeist gleichzeitig auch die bzw. der Risikoeigentümer:in.

Projektrisiken

Im Rahmen von Projekten können durch Neuerschaffung, Abänderung, Ersatz oder Entfernung von Dienstleistungen und/oder infrastrukturellen Aspekten projektbezogene Risiken auftreten.

Jedes Projekt ist darauf zu prüfen, ob dessen Durchführung, Zwischen- oder Endergebnisse neue Risiken entstehen lassen oder Auswirkungen auf bestehende Risiken hat. Dies gilt auch für den voraussichtlichen Betriebsmodus des Projektergebnisses.

Vor Einführung des Projektergebnisses, sind die getroffenen Massnahmen nochmals zu kontrollieren. Eine Freigabe des Projekts sollte nur mit Freigabe der darin enthaltenen Risiken bzw. ihrer risikomitigierenden Massnahmen zulässig sein.

Überdies ist jedes Projekt auch darauf zu überprüfen, ob sich während der Bau- oder Umbauphase aus allfälligen Änderungen in der Infrastruktur, den Handlungsabläufen, Arbeitsverfahren

oder Prozessen, den genutzten Einsatzmitteln oder der einstweiligen Organisation neue, von den Betriebsrisiken abweichende Risiken ergeben.

Bei Projekten mit besonders hoher Risikobelastung oder bei Projekten, die länger als drei Monate dauern, sollte ein regelmässiges Reporting an das Risikomanagement festgelegt werden. Das Reporting sollte Gegenstand der Projektplanung sein.

2.2.2 Risiken analysieren

Im zweiten Schritt wird das Risiko analysiert. Zur Analyse des Risikos und zur Ermittlung des Risikowerts werden die Auswirkung wie auch die Eintretenswahrscheinlichkeit herangezogen.

Hierbei ist es wichtig, für jeden der beiden Aspekte mindestens zwei parallele Beschreibungsqualitäten zur Ermittlung des Risikos anzubieten, damit eine kontextorientierte realitätsnahe Beschreibung als Vergleichswert angeboten werden kann und die Beurteilenden nicht in einem abstrakten, von verschiedenen Personen verschiedenen eingeschätzten Wertefeld suchen muss.

Auswirkung

Die Abschätzung der Auswirkung sollte auf zwei unabhängige Weisen möglich sein. In unserem Beispiel ist einerseits eine finanzielle, andererseits eine beschreibende Referenzierung angegeben.

Die Schwere der Auswirkung wird auf einer Skala (z.B. A-E) beschrieben.

Wert	Auswirkung	Schadensausmass	Beschreibung
A	tief	CHF 0 – 50’000	kein Business Impact, geringe finanzielle Auswirkungen, kein Image-Verlust, kein Reputationsschaden
B	mittel	CHF 50'001 – 200’000	diskreter Business Impact, gemässigte finanzielle Auswirkungen, Sachschaden, Erwähnung in der Fachpresse
C	hoch	CHF 200'001 – 500’000	spürbarer Business Impact, deutliche finanzielle Auswirkungen, erheblicher Sachschaden, Datenverlust Compliance Vergehen, Reputationsschaden (Erwähnung in der nationalen Presse), Leistungsempfänger:inschäden

Wert	Auswirkung	Schadensausmass	Beschreibung
D	sehr hoch	CHF 500'001 – 800’000	invalidisierender Business Impact, weitreichender Datenverlust, Gesetzesverstoss, Compliance Verstoss, Reputationsschaden (internationale Pressekampagne) Leistungsempfängerschäden, bilanzwirksame finanzielle Auswirkungen
E	extrem hoch	> CHF 800’000	Komplettverlust des Business, Gesetzesverstösse, Compliance Verstösse, ruinöse finanzielle Schäden, Verlust von mehr als 90% der eigenen oder der Daten von Leistungsempfängern oder deren End-Kund:innendaten

Tabelle 1: Auswirkung

Eintretenswahrscheinlichkeit

Die Häufigkeit bzw. Eintretenswahrscheinlichkeit eines Risikoereignisses wird ebenfalls abgeschätzt und in einer Skala (z.B. 1-5) mit zwei entsprechenden Referenzbeschreibungen hinterlegt.

Wert	Eintretenswahrscheinlichkeit	Beschreibung
1	selten	einmal in 10 Jahren oder seltener
2	gelegentlich	einmal fünf bis 10 Jahren
3	oft	ein- bis fünf-jährlich wiederkehrend
4	häufig	einmal im Quartal bis jährlich
5	extrem häufig	monatlich bis quartalsweise

Tabelle 2: Eintretenswahrscheinlichkeit

2.2.3 Risiken bewerten

Die Multiplikation von Auswirkung und Eintretenswahrscheinlichkeit stellt die eigentliche Bewertung der identifizierten Risiken dar.

Die Eintretenswahrscheinlichkeit wird dabei gemäss ihrem Wert direkt in Punkten zur Kalkulation herangezogen.

In der Analyse sollten zur Bewertung der Auswirkung bewusst Buchstaben verwendet werden, um eine Verwechslung mit der Analyse der Eintretenswahrscheinlichkeit auszuschliessen.

Zur eigentlichen Berechnung des Risikowerts bzw. Risikopotentials könnten so die Werte A bis E folgendermassen in Zahlenwerte umgerechnet werden:

Auswirkung	Rechnerischer Wert
A	1
B	2
C	3
D	4
E	5

Tabelle 3: Punktewerte Auswirkung

Durch die Multiplikation von rechnerischem Wert der Auswirkung und dem Wert der Eintretenswahrscheinlichkeit wird das Risikopotential bzw. der Risikowert ermittelt.

Auswirkung	Eintretens-wahrscheinlichkeit	Risikowert (Risikopotential)
A	1	1
D	3	12
B	3	6
B	5	10
E	5	25

Tabelle 4: Beispiele Risikowert-Errechnung

Der Risikowert beschreibt das Gefährdungspotential des Risikos für die jeweilige Organisation oder Unternehmung. Je höher der Wert, desto mehr Gefahr geht von dem Risiko aus.

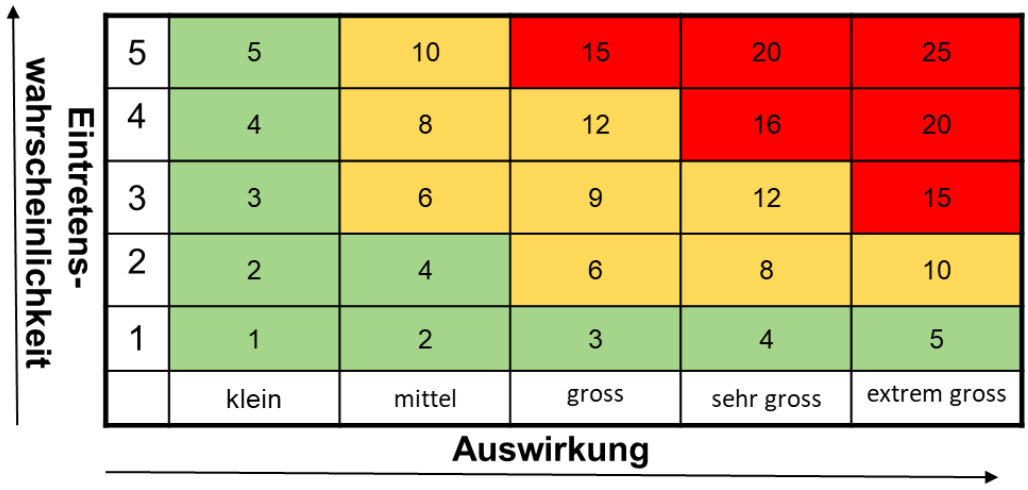


Abbildung 3: Risikomatrix mit Risikowerten

NETTO-Risikowert

Die Risikobewertung VOR der Identifikation und Umsetzung von mitigierenden Massnahmen ist eine BRUTTO-Bewertung. Nachdem Massnahmen zur Risikominderung umgesetzt wurden, sollte das Risiko neu bewertet werden und bekommt so eine NETTO-Bewertung. Damit ist abschätzbar, welchen Gegenwert die risikomindernden Massnahmen haben.

Im Weiteren sollte noch bestimmt werden, welche Bereiche von Vertraulichkeit, Integrität und Verfügbarkeit durch das Eintreten des Risikos betroffen wären, d.h. in welcher Art und Weise das jeweilige Risiko einen Schaden anrichten könnte.

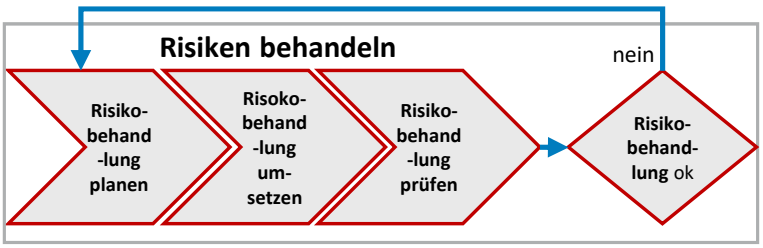
Hierbei ist es durch aus möglich, dass ein einzelnes Risiko auch mehrere der Bereiche trifft.

BRUTTO Eintretens-Wahr-schein-lichkeit	BRUTTO Auswir-kung	Vertraulichkeit (VT)	Verfügbarkeit (VF)	Integrität (I)
3	B		x	
3	B		x	

2	B	X	x	x
3	C	X	x	x
2	C	X		

Die Risikobewertung kann im Vier-Augen-Prinzip nochmals geprüft und allenfalls nochmals einer Klärung, Analyse und Neubewertung unterzogen werden.

2.3 Risiken behandeln



Generell werden die Risiken in einer Art Priorisierung vom höchsten Risikowert her behandelt.

Dies geschieht in drei Phasen:

- Planung
- Umsetzung
- Prüfung

2.3.1 Risikobehandlung planen

Gemäss der Art und Schwere des Risikos werden Behandlungsoptionen entworfen und die ausgewählte Option in ihrer Umsetzung als einzelne Massnahme oder als Projekt geplant. Da eine individuelle Massnahme oder ein Projekt auch mehrere Risiken adressieren kann, sollte die Risikobehandlungsplanung im Sinne von Aufwand und Ertrag, wo immer möglich integrativ mehrere Risiken einbeziehen. Spätestens zu diesem Zeitpunkt wird ein: Risikoeigentümer:in festgelegt, die bzw. der die Beauftragung und allenfalls Führung in der eigentlichen Umsetzung der Risikobehandlung innehat. Die Behandlungsmassnahme wird beschrieben und erfasst.

Bei der Planung von Massnahmen wie Schutz- und Rettungsszenarien, die Brandschutzeinrichtungen, Alarmierungstechnik, Alarmierungsabläufe u.Ä. zum Schutz von Leib und Leben von Mitarbeiter:innen und Personen beinhalten, sind regelmässige Übungen zur physischen Durchführung der Notfallszenarien zu planen.

Es gibt verschiedene Optionen, ein Risiko anzugehen:

Behandlungsoption	**Erläuterung**
Risiko transferieren	Transfer bedeutet die Abwälzung des Risikos auf eine andere Partei, d.h. in der Praxis auf eine:n Versicher:in oder eine:n Geschäftspartner:in in einem anderen Teil der Lieferkette (z. B. eine:n Leistungserbringer:in oder eine:n Leistungsempfänger:in). Es könnte auch eine Option zum Aufteilen des Risikos zwischen zwei Partner:innen zum Zuge kommen.
Risiko akzeptieren	Die Option, ein Risiko zu akzeptieren, schliesst im Wesentlichen zwei Fälle ein: 1. Restrisiken, die mit keiner anderen praktikablen Massnahme weiter im Risikowert reduziert werden können 2. Risiken, bei denen die Risikomerkmale klar bekannt sind (Auswirkung, Eintretenswahrscheinlichkeit) und a. der erwartete Ertrag, der sich aus der Übernahme des Risikos ergibt, höher ist als die potenziellen Risiko-Kosten oder b. die Kosten der Risiko-Massnahmen das potenzielle Risiko klar übersteigen
Risiko reduzieren	Wenn entschieden wird, dass das Risiko weder übertragen noch vermieden werden kann, stellt sich die Frage, ob etwas unternommen werden kann, um das Risiko zu verringern oder abzuschwächen. Dies könnte z. B. bedeuten, dass technische oder organisatorische Massnahmen (TOM) zur Risikoverringerung getroffen werden. Dies könnte aber auch bedeuten, dass eine erwartete Rendite verringert wird, um das Risiko zu diversifizieren, oder dass ein Prozess umgestaltet wird, um die Verringerung zu erreichen.

Behandlungsoption	Erläuterung
Risiko vermeiden	Vermeidung bedeutet, dass man sich fragt, ob die Organisation die Tätigkeit oder den Bereich, in dem das Risiko auftritt, überhaupt ausüben muss oder diese Tätigkeit ganz unterlassen kann. Hier bieten sich beispielsweise Anpassungen in den Geschäftsprozessen oder Abgrenzungen in der Lieferkette an.

Tabelle 5: Risikobehandlungsoptionen

Die Optionen sind für ein jeweiliges Risiko nicht exklusiv. Es kann eine Massnahme ergriffen werden, bei der zwei oder mehr Arten dieser Optionen zum Tragen kommen.

Zur Gewährleistung der Auditierbarkeit bezüglich ISO 27001 kann jeder gewählten Massnahme ein Kapitel des Annex A der Norm zugeordnet werden.

Die Massnahmen sollen mit einem geplanten Datum zur Fertigstellung der Umsetzung der Massnahme und ein Massnahmen-Status erfasst werden. Status können sein:

Status	Erläuterung
Offen	Das Risiko ist bekannt und erfasst, aber die zu ergreifenden Massnahmen sind noch nicht endgültig bestimmt oder Die konkrete Durchführungsplanung der eigentlichen technischen oder organisatorischen Massnahmen ist noch nicht abgeschlossen
geplant	Die konkrete Durchführungsplanung der eigentlichen technischen oder organisatorischen Massnahme(n) ist klar oder weitestgehend festgelegt
in Arbeit	Die Risikomassnahmen befinden sich in Umsetzung

Status	Erläuterung
erledigt	Die Risikomassnahmen sind abgeschlossen
geschlossen	Das Risiko wird geschlossen, weil der Grund dafür in Kürze entfällt oder bereits entfallen ist, bzw. die Bedrohung oder Schwachstelle nicht mehr vorhanden ist.
fortlaufend	Das Risiko muss engmaschig verfolgt bzw. mit anhaltenden Massnahmen eingegrenzt werden.

Tabelle 6: Risikostatus

2.3.2 Risikobehandlung umsetzen

Die Risikomassnahmen werden wie geplant umgesetzt.

Der Fortschritt, die Umsetzung, Erledigung oder allfällige Probleme sollten im Risiko-Teil z.B. eines IT-Monthly Meetings, wöchentlichen Betriebs-Meetings oder sonst einem regelmässigen operativen Treffen reviewed und fortgeschrieben werden.

Die Fertigstellung der Umsetzung wird mit Datum und einem Nachweis festgehalten und dokumentiert.

2.3.3 Risikobehandlung prüfen

Zur Abnahme prüft die bzw. der Risikoeigentümer:in oder ein:e entsprechende:r relevante:r Anspruchsträger:in die Fertigstellung, den Nachweis und die Wirkung der Massnahme. Die Abnahme wird dokumentiert.

Zur Prüfung von Massnahmen wie Schutz- und Rettungsszenarien, die Brandschutzeinrichtungen, Alarmierungstechnik, Alarmierungsabläufe u.Ä. zum Schutz von Leib und Leben von Mitarbeiter:innen und Personen beinhalten, sind regelmässige Übungen zu den Notfallszenarien einzurichten bzw. durchzuführen.

BRUTTO-Risikowert

Nachdem Massnahmen zur Risikominderung umgesetzt wurden, sollte das Risiko neu bewertet werden und bekommt so eine NETTO-Bewertung. Damit ist abschätzbar, welchen Gegenwert die risikomindernden Massnahmen gegenüber dem Brutto-Risiko haben.

Bei Mängeln in der Umsetzung oder Wirkung der Massnahme sollte der Status des Risikos zurückgesetzt und die Planung einer neuen Risikobehandlung begonnen werden.

2.4 Risiken akzeptieren

Risiken, die nach der Behandlung immer noch ein geringeres Restrisiko darstellen, können in einem neuerlichen Prozess-Zyklus weiter behandelt werden oder als Restrisiko akzeptiert und einer anhaltenden Überwachung unterstellt und so verfolgt werden.

Manche Risiken werden zwar erkannt, eine aktive Behandlung kann aber möglicherweise nicht oder noch nicht angezeigt sein. Diese Risiken können ebenfalls erfasst und einfach in einen Nachverfolgungszyklus eingebunden und so «unter Beobachtung» gestellt werden.

Zur Nachverfolgung der Massnahme(n) und ihrer Wirkung wird ein Überwachungsintervall für das Risiko festgelegt. Das Risiko und die entsprechenden Massnahmen werden mindestens mit der vorgegebenen Periodizität überprüft. Hierbei werden das Risiko selbst, die Risikofaktoren und die Aspekte «Eintretenswahrscheinlichkeit» und «Auswirkung» jeweils neu erwägt.

Jeder Überprüfungspunkt sollte mit seinem Datum festgehalten werden.

Nach jeder Überprüfung kann die Periodizität sinnvoll angepasst werden oder das Risiko kann erneut eröffnet und der Risikoprozess neu gestartet werden.

Ist ein Risiko nach Durchführung der Massnahmen und angemessener Überprüfungsperiode nicht mehr als relevant zu klassieren, kann es im Risikokatalog bzw. der Risikoliste auf den Status «geschlossen» gesetzt werden.

Der Risikokatalog bzw. der Status des Tools mit seinen Inhalten sollte periodisch zu gespeichert und für Auditzwecke aufbewahrt werden.

2.5 Risiko-Kommunikation und -Beratung

Um den Risiken im Geschäftsumfeld bestmöglich begegnen zu können, sollten die relevanten, von den jeweilig identifizierten Risiken betroffenen Personen initial darüber informiert und beraten werden, wie dem Risiko bis zur Umsetzung der Risikomassnahmen begegnet werden kann.

Themen, die sich aus den behandelten Risiken ergeben, sollten von einer bzw. einem Sicherheits-Verantwortlichen oder einer bzw. einem Delegierten monatlich im Sinne einer Awareness- und Verhaltens-Information an die Mitarbeiter:innen kommuniziert werden. Tagesaktuelle Risiken sollten umgehend über einen etablierten Kommunikationskanal bekanntgegeben werden und dann in die monatliche Kommunikation einfliessen.

2.6 Überwachung und Review

Der Prozess des Risikomanagements an sich und die damit verbundenen Aktivitäten sollten kontinuierlich überwacht, überprüft und bei Bedarf und Bedarf verbessert werden. Beispielsweise könnte im Rahmen eines Auditplans periodisch eine Überprüfung dahingehend geplant werden, dass das Risiko-Management-Verfahren den aktuellen Umständen angemessen bleibt und korrekt befolgt wird. Der Auditbericht selbst dient dann der Verbesserung und könnte zuhanden des Sicherheits-Verantwortlichen der jeweiligen Organisation gehen.

2.6.1 Kontextsensitivität

Zur Erhaltung der Prozessqualität und -wirksamkeit sollte sichergestellt werden, dass der für die Identifikation, Bewertung und Behandlung notwendige Kontext, die Ergebnisse der Risikobewertung und Risikobehandlung sowie die Managementpläne relevant und den aktuellen Umständen angemessen bleiben. Ein zum Selbstzweck gewordenes Risikomanagement hilft niemandem und führt nur zu Widerständen, Kosten und mangelnder Compliance in der Organisation. Das regelmässige Sizing des Risikomanagements ist ein wesentlicher Erfolgsfaktor.

2.6.2 Prozessverbesserung

Der Prozess des Informationssicherheits-Risikomanagements sollte kontinuierlich überwacht, überprüft und bei Bedarf und Bedarf verbessert werden.

Alle vereinbarten Verbesserungen des Prozesses oder der Massnahmen, die zur besseren Einhaltung des Prozesses notwendig sind, können dann den zuständigen Führungskräften mitgeteilt werden, um sicherzustellen, dass:

- ein realistisches Risikoverständnis gewährleistet bleibt
- kein Risiko oder Risikoelement übersehen oder unterschätzt wird
- Entscheidungen getroffen und die notwendigen Massnahmen ergriffen werden
- die Fähigkeit erhalten bleibt, angemessen zu reagieren
- das Risiko-Verfahren up-to-date und wirksam bleibt

Schliesslich sollte auch hier die Umsetzung der entsprechenden Massnahmen überwacht und ebenfalls im Rahmen des kontinuierlichen Verbesserungsprozesses (KVP) des rapportiert werden.

2.7 Risiko-Cockpit und -Bericht

Es sollte ein Cockpit mit Risikokennzahlen geführt werden.

Dies sollte zur kontinuierlichen Risikoverfolgung durch eine:n Risikomanager:in an einem regelmässigen operativen Treffen und zur Kommunikation mit dem Management genutzt werden.

Jährlich sollte ein Risikobericht an das Management verfasst werden, dessen Inhalt offiziell vom Management zur Kenntnis genommen wird.

3 Fazit

So umfassend dieser Prozess und seine Beschreibung hier erscheinen mag, es lohnt sich, ihn in jeder Organisation, jedem KMU, jedem Ort anzuwenden. Und wir alle tun es. Wann immer wir entscheiden, für irgendetwas eine Versicherung abzuschliessen, das Auto vor dem Gewitter in die Garage zu nehmen, das Fahrrad abzuschliessen oder die Informatik mit einer Datensicherung abzusichern. Wir erkennen Risken, schätzen sie für uns ab, ergreifen angemessene Massnahmen und prüfen, ob sie greifen.

Dieser Artikel zeigt einfach auf, an was KMUs denken müssen, wenn sie ihre IT oder andere Werte schützen möchten. Wenn sie die oben aufgezeigten Schritte befolgen, dann kann das Risikomanagement auch gut sogar mit einem einfachen Excel gelingen.

Sicherheit ist die Abwesenheit intolerabler Risiken. Mit diesem Risiko-Prozess kann man sich ziemlich gut und einfach schützen.