Richtlinie
Risikomanagement

Untertitel

Klassifikation:	Bitte klassifizieren!
Datum:	21.02.2019
Version:	**0.1**
Autor:	Reiner Schröppel
Dok.-Name:	RL_Risikomanagement_v0.10.docx
Seiten:	14

Dokumentenhistorie

Version	Datum	Bearbeiter	Status	Bemerkung/Änderung
0.10	06.12.2018	R. Schröppel	In Bearbeitung	Ersterstellung

Inhaltsverzeichnis

1 Einleitung, Zweck und Ziele

Ziel der Informationssicherheit ist es, sowohl die Informationen selbst als auch die Prozesse, Anwendungen, Systeme, Services, Kommunikation und Einrichtungen zu schützen, welche die Informationen enthalten, verarbeiten, speichern, transportieren oder liefern.

Zur Erfüllung der organisationsspezifischen Sicherheits- und Geschäftsziele müssen Sicherheitsmaßnahmen eingeführt, überwacht, überprüft und bei Bedarf verbessert werden. Im Zuge der Überprüfungen und des Betriebs kommt es immer wieder vor, dass Abweichungen oder Schwachstellen identifiziert werden. Dies Abweichungen oder Schwachstellen müssen in Bezug auf das damit verbundene Risiko analysiert, bewertet und angemessen behandelt werden. Dabei kann die Behandlung identifizierter Risiken von der Akzeptanz, über die Verlagerung, der Versicherung, der Minimierung bis hin zur Ergreifung von Maßnahmen bestehen.

Für die Einschätzung und die Behandlung von Informationsrisiken ist eine Methodik zur einheitlichen Ermittlung von Bedrohungen, Schwachstellen und Risiken sowie Maßnahmen zu deren Behandlung und Steuerung festzulegen sowie eine Aussage zu akzeptablen Risikoniveau zu treffen.

Für den Einsatzbereich im Geltungsbereichs des B3S für die Gesundheitsversorgung im Krankenhaus werden dabei zusätzlich zum Risikomanagement, welches sich aus den Anforderungen der DIN ISO/IEC 27001 (in der jeweilig gültigen Fassung) zusätzlich die Anforderungen an die Informationssicherheit von Medizingeräten in IT-Netzwerken, DIN EN 80001-1 „Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten“ berücksichtigt.

Die nachfolgend beschriebene Risikomethodik bildet die Grundlage für das Informationssicherheitsrisikomanagement (IS-RM). Es beschreibt die organisatorische und operative Umsetzung, die zur Risikoerkennung, -quantifizierung, -kommunikation, -steuerung und -kontrolle zu beachten sind. Zusätzlich liefert die Risikomethodik die Basis für die Prüfung des Risikomanagements und deren Kontrolle durch externe Institutionen als auch durch interne Gremien.

Die Risikomethodik definiert die Mittel und Begrifflichkeiten und beschreibt deren Gewichtung für die bestehenden operativen Informationssicherheitsrisiken (IS-Risiken).

Die Risikomethodik im Informationssicherheitsmanagement liefert Kennzahlen und Werte, die an das zentrale Riskmanagement des Unternehmens weitergegeben sind und dort in das unternehmerische Gesamtrisikomanagement einfließen müssen. Das IS-RM besteht aus der systematischen und kontinuierlichen Erfassung und Bewertung von Risiken, sowie der anschließenden Steuerung und Kommunikation der identifizierten Risiken.

Die sich aus dem IS-RM ergebenen Erkenntnisse und Handlungshinweisen bzw. -anreize werden von den entsprechenden Stellen bei ihrem wirtschaftlichen Handeln im Rahmen der jeweiligen Wirtschaftspläne adäquat berücksichtigt.

Das IS-Risikomanagementsystem versteht sich als ein dynamischer Prozess, der ständig weiterentwickelt wird. Hierbei dienen verschiedenste Risikoarten, die jeweils verschiedene Risikogruppen beinhalten, als Ausgangsbasis.

Vor diesem Hintergrund dient die hier beschriebene Risikomethodik zur Dokumentation dieses Prozesses und wird regelmäßig aktualisiert. Es wird durch den von der Geschäftsführung benannten Risikomanager erstellt, gepflegt und weiterentwickelt und steht allen Bereichen des Unternehmens zur Verfügung.

Inhalt der Risikomethodik sind die gesetzlichen Grundlagen, die Begriffsdefinitionen und die Prozesse zum IS-RM sowie der Aufbau- und die Ablauforganisation im Rahmen dieses Risikomanagementsystems.

2 Anwender

Anwender dieses Dokuments sind alle Mitarbeiter des Unternehmens die mit Risikoeinschätzung und Risikobehandlung befasst sind.

3 Geltungsbereich

xxx

Die Umsetzung der Risikoeinschätzung und Risikobehandlung gilt für den gesamten Anwendungsbereich des ISMS. Alle Werte die im Unternehmen genutzt werden oder die eine Auswirkung auf die Informationssicherheit im Rahmen des ISMS haben könnten, sind einer Risikobewertung zu unterziehen.

4 Definitionen und Begriffe (falls vorhanden)

Begriff	Beschreibung
Akzeptiertes Risiko	Risiko, das z. B. aus technischen, praktischen oder wirtschaftlichen Gründen nicht (weiter) reduziert werden soll und somit getragen wird.
Auswirkung	...
Chancen	...
Maßnahmenverantwortlicher	...
Restrisiko	...
Risiko	Ein Risiko ist per Definition ein mögliches zukünftiges Ereignis oder eine Handlung, die das Unternehmen daran hindert, seine geplanten Ziele zu erreichen. Zu Grunde liegen hier Ertrags-, Finanz- und Vermögenslage des Unternehmens sowie der Informations-sicherheitsstandard gegeben über dem Unternehmen selbst, seinen Mitarbeitern, Kunden und sonstiger Dritten. Ereignisse und Entwicklungen, die mit einer gewissen Wahrscheinlichkeit eintreten und wesentliche negative finanzielle und nichtfinanzielle Auswirkungen auf die Erreichung der Ziele und die Erfüllung der Aufgaben haben.
...	...
...	...
...	...
...	...
Risikoeigner	Person mit der Entscheidungskompetenz und Verantwortung, hinsichtlich eines Risikos zu handeln. Der Risikoeigentümer verfügt über entsprechende Entscheidungskompetenz bezüglich des konkreten Prozesses. Der Risikoeigentümer ist zuständig für den Risikoprozess eines bestimmten Risikos.
...	...
Risiko-Managementsystem	Das Risikomanagementsystem ist die Gesamtheit aller organisatorischen Regelungen und Maßnahmen, um eine Risikofrüherkennung wirkungsvoll zu realisieren und entsprechende Maßnahmen der Gegen-steuerung umzusetzen. Das Risikomanagementsystem dient dazu, die Risiken des Unternehmens systematisch zu steuern und zu überwachen, sowie alternative Maßnahmen vorzubereiten, um bedrohlichen Entwicklungen recht-zeitig entgegensteuern zu können, um die Realisierung der angestrebten Ziele zu ermöglichen. Das Risikomanagementsystem ist mithin ein Frühwarn- und Steuerungssystem. Da eine Vermeidung sämtlicher Risiken nicht realisierbar ist, ist es Ziel des Risikomanagementsystems, den kontrollierten und gesteuerten Umgang mit den Restrisiken des Unternehmens zu ermöglichen.

Begriff	Beschreibung
…	…
…	…
…	…
Wahrscheinlichkeit	Relative Häufigkeit des Eintritts zukünftiger Ereignisse oder Entwicklungen (objektive Definition). Unsicherheit von Aussagen bzw. Grad an persönlicher Überzeugung betreffend den Eintritt eines Ereignisses oder einer Entwicklung (subjektives Verständnis). Die Wahrscheinlichkeit eines Risikos kann sich auf eine Periode (z. B. Jahreswahrscheinlichkeit) oder auf eine Anzahl von Fällen (Fall-Wahrscheinlichkeit) beziehen.

5 Mitgeltende Unterlagen und Referenzdokumente

- ISO/IEC 27001 Standard, Abschnitte …
- ISO/IEC 27001 Standard, Abschnitte …
- Informationssicherheitsleitlinie des Unternehmens
- Liste rechtlicher, amtlicher, vertraglicher und anderer Anforderungen
- DIN 80001-1, Teil 1
- …
- …

6 Zuständigkeit

Für die Erstellung, Pflege und regelmäßige Überprüfung dieser Richtlinie ist xxx verantwortlich.

Zu den Aufgaben der Verantwortlichen des IS-RM gehört die Identifikation, Bewertung, Dokumentation von IS-Risiken, so wie die Durchführung entsprechender Abstimmungen mit der Unternehmensleitung und dem Gesamtrisikomanagement des Unternehmens. Weiterhin ist durch den Verantwortlichen für das IS-RM zu gewährleisten, dass Anpassungen/Änderungen, die Bewertung von Risiken, etc. nachvollziehbar und sicher erfolgt. Die IS-Risikomethodik unterliegt wie alle Prozesse und Verfahren einer regelmäßigen Kontrolle und er Verantwortliche für das IS-RM hat dafür Sorge zu tragen, dass Änderungen und Verbesserungen am IS-RM erfolgen und Veränderungen entsprechend freigegeben und veröffentlicht werden.

7 Umsetzung

7.1 Aufbau- und Ablauforganisation

7.1.1 *Aufgaben der Geschäftsführung/Risikomanagement*

Das Risikomanagement gehört zum Aufgabenbereich der Geschäftsführung. Sie übernimmt damit die Gesamtverantwortung für den Risikomanagementprozess im Unternehmen. Unterstützend und beratend wirkt hier in großem Maße die Funktion eines Risikomanagers.

Die Risikoberichterstattung erfolgt in regelmäßigen Abständen aber mindestens einmal jährlich. Falls Sicherheitsvorfälle bei einzelnen Risiken auftreten, werden diese umgehend zum Zeitpunkt des Auftretens an die Geschäftsführung berichtet neu bewertet und ausgerichtet.

7.1.2 *Risikomanager*

…

7.2 Inventar der Werte

Damit Risiken überhaupt bewertet werden können, muss im Unternehmen bekannt sein, über welche Werte das Unternehmen verfügt. Dies hat im Zuge der Umsetzung der ISO 27001, A.8.1.1 und A.8.1.2 zu erfolgen um im Rahmen des ISMS Anwendungsbereichs ermitteln zu können, welche Werte, Auswirkung auf die Vertraulichkeit, Integrität, Verfügbarkeit…

- Verfügbarkeit
- Vertraulichkeit
- Integrität

unterliegen.

7.3 Risikomanagementprozess

Der eigentliche Risikomanagementprozess gliedert sich in folgende Stufen:

- Risikoerfassung
- Risikobewertung
- Risikobehandlung
- …

Der Risikomanagement-Prozess ist ein Regelkreislauf, der sich laufend an die geänderten Bedingungen anpasst. Die einzelnen Schritte werden individuell ausgestaltet.

7.4 Risikoerfassung

Die Risikoerfassung dient der systematischen und regelmäßigen Ermittlung aller bestandsgefährdenden und wesentlichen Risiken des Unternehmens. Die Risikoerfassung erfolgt durch den Risikomanager. Bei der Risikoerfassung sollen alle Prozesse, Funktionsbereiche und Hierarchiestufen des gesamten Unternehmens in Bezug auf das Informationssicherheitsmanagement-System abgedeckt werden.

…

7.5 Risikobewertung

Die Risikobewertung erfolgt im Rahmen einer „Expertenbefragung". Als "Experten" kommen die Personen in Frage, die in dem jeweiligen Sachgebiet tätig sind, in dem das Risiko auftreten kann. Auch etwaige Erfahrungswerte der Geschäftsleitung und langjähriger Mitarbeiter sind bei der Befragung heranzuziehen.

…

7.5.1 *Auswirkungsbewertung*

In einem ersten Schritt werden für zuvor festgelegte Kategorien mögliche Auswirkungen zu ermitteln. Die Ermittlung der Auswirkungen erfolgt wie zuvor beschrieben durch „Experten“ bzw. durch die für die betroffenen Werte zuständigen und verantwortlichen Fachbereiche.

Folgende Auswirkungskategorien werden betrachtet:

- wirtschaftliche Auswirkungen
- Verstoß gegen Gesetzte, Verträge
- Reputationsschäden
- …
- …

Ausgehend von den Auswirkungskategorien ergibt sich folgende Matrix für ein Schadenspotential:

[Matrix hier]

Für jedes Risiko ist anhand der Matrix das Schadenspotential zu ermitteln. Für den Fall, dass keines der qualitativen Merkmale für eine Schadensbewertung herangezogen werden kann, ist das quantitative Merkmal zu schätzen. Für den Fall, dass ein eventueller Schaden zwar geringe finanzielle Schäden zur Folge haben kann, aber dadurch ggf. der Ruf des Unternehmens erheblich in Mitleidenschaft gezogen werden kann, hat das Kriterium „Reputationsschaden“ Vorrang vor den quantitativen oder anderen qualitativen Schadenspotentialen.

Grundsätzlich ist die höchste Kategorie, die für ein Risiko identifiziert wurde, ausschlaggebend.

7.5.2 *Eintrittswahrscheinlichkeit*

Für jedes identifizierte Risiko ist, bezogen auf die entsprechende Auswirkungsbewertung, die mögliche Eintrittswahrscheinlichkeit zu bestimmen. Zur Bestimmung der Eintrittswahrscheinlichkeit können Erfahrungswerte aus der Vergangenheit, Erfahrungen aus Studien oder eigene Einschätzungen herangezogen werden.

Die Abschätzung der Eintrittswahrscheinlichkeit wird gemeinsam vom Werteeigentümer, dem Risikoeigentümer und mit Unterstützung des ISMS-Teams durchgeführt.

Nachfolgend sind die Stufen für die Eintrittswahrscheinlichkeit aufgeführt:

Eintrittswahr-scheinlichkeit	%	Kriterien
Sehr hoch (7)	ab 50%	•
Hoch (5)	25% bis 50%	•
Mittel (3)	10% bis 25%	•
Gering (1)	< 10%	•

7.5.3 *Risikobewertung*

Die Identifikation, Bewertung und Behandlung von Risiken ist ein kontinuierlicher Prozess. Risiken sind mindestes einmal jährlich zu bewerten. Darüber hinaus sind, sobald Risiken erkannt werden, z. B. bei neuen Technologien, neuen Anwendungen, veränderten Situationen, etc. auch unterjährig zu bewerten und zu behandeln.

…

Mit der Definition der vier Stufen des Schadenspotentials (von «gering» bis «sehr hoch») in der Bewertungsmatrix wird eine grobe Einstufung der Risiken nach ihrer Bedeutung vorgenommen. Die konkrete Bedeutung im Einzelfall hängt u. a. vom Risikokontext und der Grösse des untersuchten Bereiches (Umfangs) ab und sollte individuell festgelegt werden.

[Tabelle mit Risikoklassen hier]

7.5.4 *Risikotoleranz*

Ausgehend von den Risikoklassen sind durch das Unternehmen Risikotoleranzstufen festzulegen. Die Risikotoleranzstufen geben grob vor, wie mit einem identifizierten Risiko zu verfahren ist. Die Festlegung der Risikotoleranzstufen ist in Absprache und mit Zustimmung der Geschäftsführung festzulegen.

Die Toleranzstufen sind dabei eine Hilfsmittel, um eine grobe Idee zu entwickeln, wie mit einem Risiko umgegangen werden soll. Letztendlich muss für jede Bewältigungsmassnahme vor ihrer Umsetzung einzeln beurteilt werden, ob die Kosten der Umsetzung in einem sinnvollen Verhältnis zur Risikoverminderung stehen.

Aus den Risikotoleranzstufen ergeben sich die nachfolgenden Handlungsoptionen:

[Tabelle der Risikotoleranzstufen hier]

7.6 ...

...

7.7 ...

...

7.8 Überwachung

Die Überwachung der Risiken und der eingeleiteten Maßnahmen ist ein wichtiger Prozessschritt im Risikomanagement, der die Effektivität des Risikomanagements sicherstellt.

7.8.1 *Risikoüberwachung*

Mit einer regelmäßigen Überwachung der Risiken wird sichergestellt, dass das Wissen bezüglich der vorhandenen Risiken des Unternehmens auf dem aktuellsten Stand gehalten wird. Ziel ist es, einerseits Veränderungen im Umfeld zu erkennen, die zu einer Neueinschätzung von bereits erfassten Risiken führen. Andererseits geht es auch darum, neu entstehende Risiken frühzeitig zu erkennen.

Bereits erfasste Risiken müssen zusätzlich zum jährlichen Risikomanagementprozess laufend überwacht werden, damit bei einer Verschlechterung der Situation frühzeitig eingegriffen werden kann.

Für die Identifikation, Bewertung und Überwachung einzelner Risiken ist in erster Linie der Risikoeigentümer zuständig und verantwortlich. Veränderungen bei der Umsetzung von Maßnahmen, der Bewertung von Risiken, etc. sind dem Risikomanager umgehend mitzuteilen, so dass er diese in seinem Risikoregister nachführen kann.

7.8.2 *Maßnahmenüberwachung*

Die Umsetzung von Maßnahmen zur Risikoreduktion muss überwacht werden. Dies ist Aufgabe des Risikoeigentümers, der die Verantwortung für das Risiko trägt. Der Maßnahmenverantwortliche setzt die beschlossene Maßnahme um und meldet dem Risikoeigentümer über den Fortschritt und auftretende Probleme bei der Maßnahmenumsetzung.

7.8.3 ...

...

7.9 Risikobericht

...

7.9.1 *Häufigkeit*

Grundsätzlich ist mindestens jährlich ein Gesamtrisikobericht durch den Risikomanager zu erstellen und der Geschäftsführung zur Kenntnis zu geben. Darüber hinaus steht es dem Risikomanager frei, bei gravierenden neuen Risiken oder bei veränderter Risikolage der Geschäftsführung einen neuen bzw. einen Teilrisikobericht zur Kenntnis zu geben.

7.9.2 *Umfang*

- ...

8 Freigabe

Ort, Datum	Name in Druckbuchstaben	Unterschrift

Anhang 1 – Risikoerfassungsbogen

[Risikoerfassung hier]

Freigabe:

Datum: _____ Geschäftsführung: _____

Anhang 2 – Risikobericht

Inhaltsverzeichnis

1 Einleitung

Hier eine kurze Beschreibung zum Risikobericht

2 Management-Zusammenfassung

Kurze Zusammenfassung über die Risikosituation im Unternehmen, z.B.:

- Behandelte Risiken seit dem letzten Risikobericht
- Status von Maßnahmen
- …

3 Gesamtrisikosituation

Darstellung aller identifizierten Risiken und deren Einstufung

[Tabelle mit der Gesamtrisikosituation hier]

4 Detailergebnisse

Nachfolgend sind Details zu Risiken ab einem Risikotoleranzwert von <eigene Vorgabe einfügen> (Hoch/Rot/ab 14, Mittel/Gelb/4-12, Niedrig/Grün/1-3) im Detail aufgeführt und beschrieben. Die aufgeführten Risiken können der jeweiligen Risikoerfassung entnommen werden.

4.1 R1 - <Risikotitel>

4.2 R2 - <Risikotitel>

5 Risikoregister

Bestandteil des Risikoberichtes ist die Darstellung aller im Unternehmen identifizierten, bewerteten und dokumentierten Risiken.

6 Freigabe

Mit der nachfolgenden Unterschrift nimmt die Geschäftsführung die ihr bekanntgegebenen und zur Kenntnis gegeben Risiken zur Kenntnis. Die vom Risikomanager vorgestellten Risiken und Maßnahmen werden durch die Geschäftsführung befürwortet.

Das Risikoregister vom <Datum>, <Version> (ggf. Hashwert der gültigen Version, falls das Risikoregister als Excel-Tabelle eingesehen wurde, alternativ eine PDF-Version) wurde der Geschäftsführung zur Einsicht gegeben. Die im Risikoregister aufgeführten Risiken, Maßnahmen und Behandlungsoptionen werden durch die Geschäftsführung bestätigt.

Datum: _____ Geschäftsführung: _____