



Parasol Island

Risikomanagement Richtlinie

Dateiname:	02_12_PSL_ISMS_Risikomanagement_v00.10_jH
Dokumentenebene:	02_Richtlinie
Erstellt von:	Philip Hansen
Version:	00.10
Status:	Freigegeben
Letzte Aktualisierung am/von:	07.11.2017 Justus Heinser
Exportiert am:	07.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	07.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	1.2

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	18.09.2017	Justus Heinser	Anpassungen
00.10	07.11.2017	Justus Heinser	Finalisierung



Parasol Island

Inhaltsverzeichnis

1. Einleitung	3
2. Geltungsbereich	3
3. Häufigkeit und Zeitpunkt der Risikoanalyse	3
4. Durchführung der Risikoanalyse	4
Identifikation von Risiken	4
Analyse von Risiken (Wahrscheinlichkeit)	5
Erfassung der Auswirkungen	5
Festsetzung der Akzeptanzkriterien	5
Erarbeitung einer Risikostrategie	5
Umsetzung und Kontrolle	5
5. Dokumentation	6
Weiterführende Dokumente	6



Parasol Island

1. Einleitung

Der Risikomanagement-Prozess umfasst die systematische Vorgehensweise, um alle potentiellen Risiken zu identifizieren und zu bewerten, sowie hierauf aufbauend entsprechende Maßnahmen zur Risikohandhabung und Chancennutzung auszuwählen und umzusetzen. Die Risiken sollen bewusst erfasst, analysiert und auf ein erträgliches Maß gemindert werden. Ebenso soll das Risiko permanent kontrolliert und weiter gemindert werden.

Neben der Vermeidung messbarer Auswirkungen wie finanzielle Schäden, Reputationsschäden oder strafrechtlichen Auswirkungen soll auch das Bewusstsein der Geschäftsleitung und der Mitarbeiter geschärft werden, um Risiken im Alltag frühzeitig zu erkennen.

2. Geltungsbereich

Die Regelungen dieser Richtlinie gelten uneingeschränkt. Sie sind verbindlich und dürfen nicht umgangen werden. Ausnahmen von der Richtlinie sind nicht zulässig, es sei denn, sie sind in dieser ausdrücklich aufgeführt.

Mit Erscheinen einer neuen Version werden vorangegangene Versionen automatisch ungültig.

3. Häufigkeit und Zeitpunkt der Risikoanalyse

Die Risikoanalyse ist jährlich zu wiederholen, um den Sicherheitsstandard aufrecht zu erhalten oder zu verbessern. Immer, wenn erhebliche Änderungen vorgeschlagen werden oder auftreten, ist ebenfalls eine Risikoanalyse durchzuführen.

Bei Änderungen für Systeme mit hohem Schutzbedarf ist sowohl bei der Planung als auch nach der Umsetzung eine Risikoanalyse durchzuführen.

- Siehe auch: Change-Management (02_05)

Vor Projekten ist ebenfalls eine Risikoanalyse durchzuführen, um die erforderlichen Maßnahmen innerhalb eines Projektes zu erörtern.

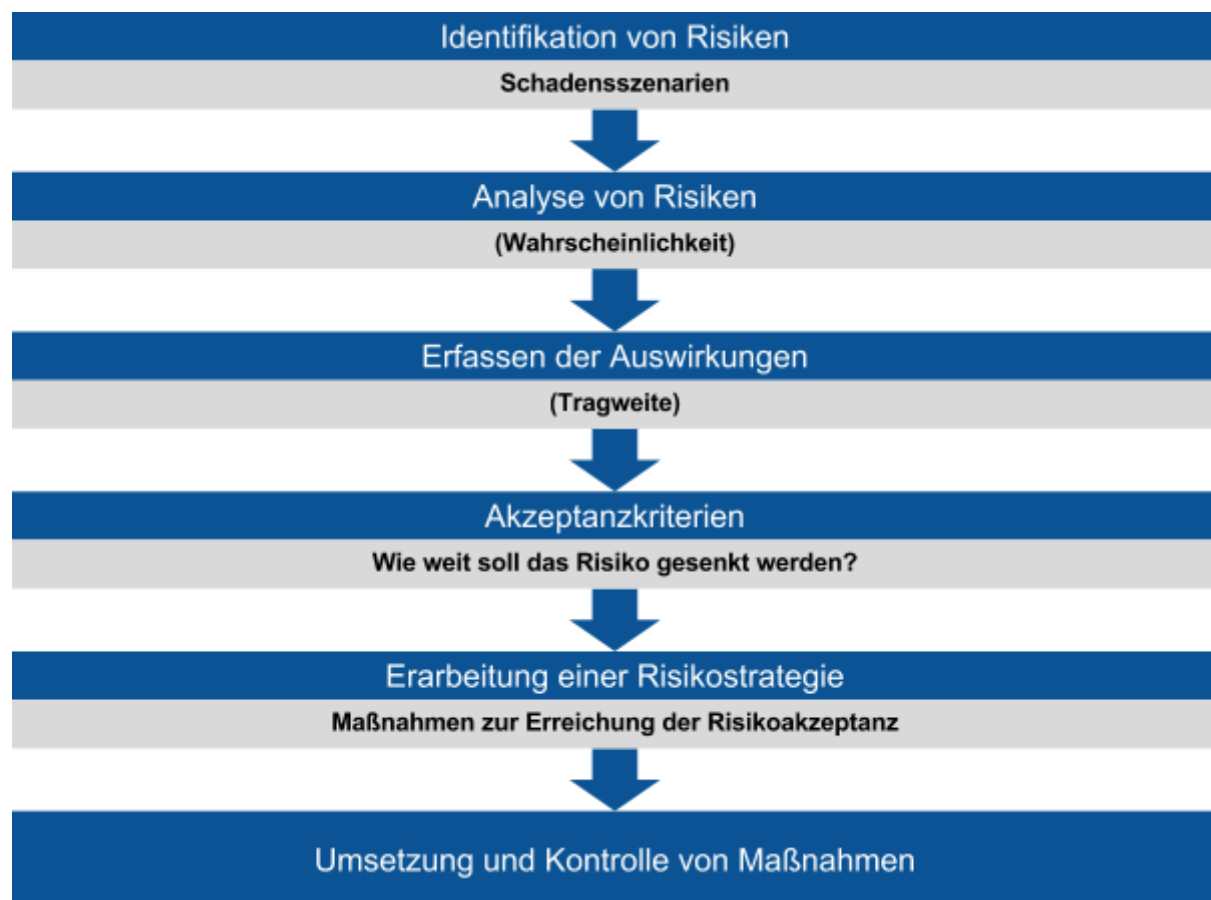
Bei Projekten mit vertraulichen oder streng vertraulichen Informationen ist das Risiko während des laufenden Projektes vom Projektleiter wiederholt zu kontrollieren.

- Siehe auch: Arbeitsanweisung zur Klassifizierung von Projekten (03_02)



4. Durchführung der Risikoanalyse

Eine Risikoanalyse im Kontext der Informationssicherheit hat die Aufgabe, relevante Gefährdungen für den Informationsverbund zu identifizieren und die daraus möglicherweise resultierenden Risiken abzuschätzen. Das Ziel ist es, die Risiken durch angemessene Gegenmaßnahmen auf ein akzeptables Maß zu reduzieren, die Restrisiken transparent zu machen und dadurch das Gesamtrisiko systematisch zu steuern.



Identifikation von Risiken

Maßgebend für die Einschätzung des Risikos sind die Informationssicherheitsziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

In der Regel ist eines der Sicherheitsziele deutlicher ausgeprägt, die Anforderungen sind jedoch übergreifend. Das Risiko muss für jedes dieser Ziele berücksichtigt werden und die Auswirkungen müssen in einem Schadensfall eingeschätzt werden.



Parasol Island

Analyse von Risiken (Wahrscheinlichkeit)

Nach Erfassung der möglichen Schadensszenarien ist die Wahrscheinlichkeit zu ermitteln. Hierfür können je nach Fall Statistiken herangezogen werden oder Erfahrung und Expertise erörtert werden. Für Erfahrungswerte sind objektiv zukünftige Ereignisse zu berücksichtigen. Nur weil ein Schaden bisher nie eingetreten ist, mindert das nicht das Risiko für die Zukunft.

Erfassung der Auswirkungen

Auswirkungen können in Form von finanzielle Schäden, Reputationsschäden oder strafrechtlichen Auswirkungen auftreten.

Der mögliche entstandene Schaden kann direkte finanzielle Auswirkungen haben oder aber indirekte, wenn zum Beispiel ein wichtiger Kunde oder Lieferant verloren geht.

Festsetzung der Akzeptanzkriterien

Risiken lassen sich selten ganz beseitigen, daher ist es wichtig, ein akzeptables Maß zu definieren, auf welches das Risiko minimiert werden soll, oder wie die Voraussetzungen aussehen, unter denen ein Risiko akzeptiert werden kann.

Erarbeitung einer Risikostrategie

Risiken lassen sich auf unterschiedlichste Art und Weise bearbeiten. Die gängigsten Strategien sind:

- Risikovermeidung (z.B. Pläne über Änderung verwerfen)
- Risikobegrenzung (z.B. durch geregelten Umgang mit dem Risiko)
- Risikoabwälzung (z.B. durch Versicherung)
- Risikoakzeptanz (Übernahme von Risiken)

Die Risikostrategie muss das Risiko auf das vorher definierte Akzeptanzmaß reduzieren. Ist dies nicht der Fall, sind andere Maßnahmen zu treffen. Risikostrategien lassen sich auch kombinieren, ein Restrisiko lässt sich versichern oder akzeptieren.

Die Risikostrategie ist in Form einer Auflistung konkreter Maßnahmen festzuhalten und in einem zeitlich vertretbaren Rahmen zu planen.

Risikoakzeptanz, also das Ignorieren eines Risikos, empfiehlt sich nur, wenn der Aufwand der Maßnahmen den potenziellen Schaden übersteigen. Eine Risikoakzeptanz muss in jedem Fall von der Geschäftsführung genehmigt und unterzeichnet werden.

Umsetzung und Kontrolle

Die Entwicklung der Risikostrategie ist fortlaufend zu beobachten und zu kontrollieren. Bei Änderung der Ausgangssituation, aber spätestens nach einem Jahr, ist eine erneute Analyse der bestehenden Risiken durchzuführen.



5. Dokumentation

Durchgeführte Risikoanalysen sind für die stabile Entwicklung eines Unternehmens von entscheidender Bedeutung. Daher sind getroffene Einschätzungen für eine Vielzahl von Entscheidungen von Bedeutung.

Daher sind die durchgeführten Risikoanalysen in übersichtlicher und nachvollziehbarer Form aufzubewahren. Risikoeinschätzungen für bestehende

- Assets werden in einem Ampelsystem (1. Grün, 2. Gelb, 3. Rot) in der Assetliste festgehalten.
- Risikoanalysen für Projekte werden in den Projektunterlagen festgehalten

Weiterführende Dokumente

- Arbeitsanweisung zur Klassifizierung von Projekten (03_02)
- Changemanagement Richtlinie (02_05)
- Assetliste (zum Festhalten der getroffenen Asset-Risikoeinschätzungen)