

IKS braucht Risikomanagement

Risikomanagement mit swissRM™

Wie Sie mit swissRM™ die Risiken im Griff
behalten



Inhalt

- 3 | Einführung
- 4 | Risiko-Dimensionen
- 7 | Risiko- und Chancenmatrix
(«Heatmap»)
- 9 | Erarbeitungsprozess

Einführung

Prinzip

Jedes Risiko wird

- in allen erforderlichen Dimensionen beschrieben und bewertet.
 - in einer Risikomatrix dargestellt und in Echtzeit nachgeführt.
 - den Bewertern automatisch rglm. zur Neubewertung vorgelegt.
- Das Controlling der Massnahmen erfolgt analog zum IKS.

Risikokarte¹

Jedes einzelne Risiko wird in einer Risikokarte beschrieben.

Rollen

- Riskowner¹
- Risikobewerter¹
- Massnahmenbeauftragte
- Administrator

Zugang

- Internet-Browser
- Google Chrome
 - Safari
 - Firefox
 - MS Edge

Sicherheit

- Hosting in der Schweiz, Schweizer Management der Daten Center
- 2 redundante Rechenzentren, ISO 9001 und 27001 in der Schweiz, 99.99 % Uptime
- Zusätzlich separates Backup Data Center, mit Zugriff auf Vorabend-Datenbestand bei Downtime
- 3-fache Georedundanz in der Schweiz
- Sichere Authentifizierung nach § 7 ZH IDG (Kant. Gesetz über die Information und den Datenschutz)
- SMS-Authentifizierung userspezifisch einstellbar
- SSL (Secure Sockets Layer)



¹Bei Chancen wird die Risikokarte zur Chancenkarte, die Riskowner sind Chancenowner und die Risikobewerter sind Chancenbewerter

Risiko¹-Dimensionen

1. Das Risiko



	Nummer	Bezeichnung	Geschäftsbereich	Owner	Periodenbeginn		
✎	1	Liquiditätsklemme	Finanzen	Berclaz Christian	01.09.2021 23:50:00	✎	👍
✎	2	Schneefall	Verkauf	Amrein Urs	16.01.2022 23:50:00	✎	👍
✎	3	Rohwarenpreis	Einkauf	Achermann Michael	16.01.2022 23:50:00	✎	👍

1

Risiko

Nummer:

Bezeichnung:

Geschäftsbereich:

Beschreibung Vorfall:

Beschreibung Schaden:

Beschreibung Ursache/Schwachstelle:

2

An...

Senden Cc...

Konto Bcc...

Betreff:

Sehr geehrte Frau Muster

Bitte bewerten Sie das Risiko. [Hier](#) bitte melden bis 31. März 2021.

3

An...

Senden Cc...

Konto Bcc...

Betreff:

Sehr geehrter Herr Weissnicht

Bitte ergreifen Sie folgende Massnahme/n:

- ...
- ...

Bitte [hier](#) melden bis 31. März 2021.

1. Beschreibung des Risikos
2. Bestimmen der Risikobewerter und Bewertungsperiodizität. Bei mehreren Risikobewertern wird der gerundete Durchschnitt verwendet.
3. Bestimmen der Massnahmenaufträge und der Massnahmenbeauftragten. Es kann eine unbeschränkte Anzahl von Massnahmen pro Risiko festgelegt werden.

¹Zur besseren Lesbarkeit ist nicht an jeder Stelle erwähnt, dass auch Chancen abgebildet und gemanagt werden können. Eine Chance ist im Grundsatz nichts anderes als ein negatives Risiko.

2. Risikozuteilung



1. Jedem Risiko können fünf Elemente zugeteilt werden: Geschäftsbereich, Risikogruppe, Risikoart, Unternehmensziel und Risikostrategie.
2. Die Einteilungen für jedes Element («Bezeichnung») ist frei wählbar, resp. erfassbar – ohne Feldebegrenzung und Anzahllimitierung.

Beispiele für die Einteilung, Bezeichnung der einzelnen Elemente der Risikozuteilungen

1

2

Geschäftsbereich	
	Bezeichnung
	Einkauf
	Finanzen
	Produktion
	Verkauf

Risikogruppe	
	Bezeichnung
	keine Prio
	Prio 1
	Prio 2
	Prio 3

Risikoart	
	Bezeichnung
	IKS
	Personalmanagement
	Prozesse
	Sicherheitskonzepte
	Strategie VR

Unternehmensziel	
	Bezeichnung
	IPO
	Maximale Dividende
	Reputation
	Stabilität
	Wachstum
	Zero CO2

Risikostrategie	
	Bezeichnung
	Abwälzen
	Akzeptieren
	Begrenzen
	Vermeiden
	Vermindern

3. Risikobewertung :P :i :R

P = Eintretenswahrscheinlichkeit

i = Schadenhöhe/Auswirkung

R = Reputationsschaden

1

Nummer:

Bezeichnung:





2

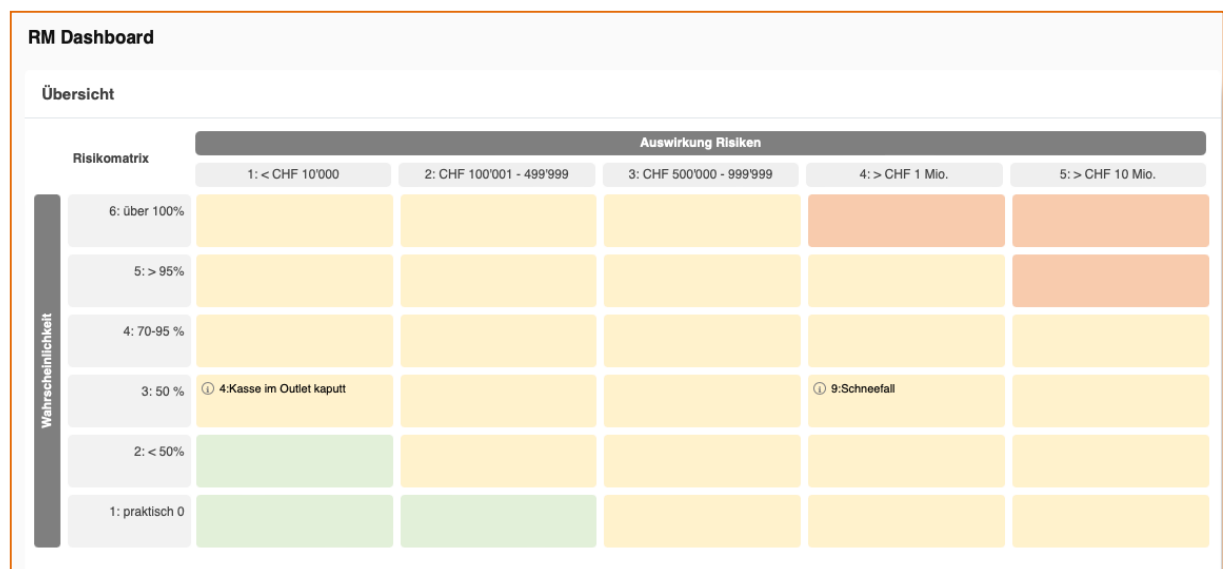
Beispiel für die Kategorisierung der Schadenshöhe:

i-Kategorie		
	Nummer	Bezeichnung
	1	< CHF 10'000
	2	CHF 10'0001 - 499'999
	3	CHF 500'000 - 999'999
	4	> CHF 1 Mio.

1. Die Skalierung von Eintretenswahrscheinlichkeit, Schadenhöhe und Reputationsschaden erfolgt durch Vergabe einer Anzahl von Nummern oder Zahlen. Die Zahlen bestimmen die Positionierung, den Ausweis des Risikos in der «Heatmap». Es kann mit bis zu vierstelligen positiven Zahlen nummeriert werden. Um eine **Chance** zu «kreieren», reicht es die Schadenhöhe/Auswirkung mit negativen Zahlen zu bewerten.
2. «Bezeichnung» ist ein alphanummerisches Feld ohne Zeichenbegrenzung und dient der Beschreibung der numerischen Einteilung von Eintretenswahrscheinlichkeit, Schadenhöhe und Reputationsschaden.

Risiko- und Chancenmatrix («Heatmap»)

1. RM Dashboard



1. Die einzelnen Risiken werden anhand der Bewertung von Eintretenswahrscheinlichkeit und Schadenhöhe/-ausmass in der Echtzeit-Risikomatrix ausgewiesen. Mit Klick auf die einzelnen Risiken gelangt man zur Risikokarte.

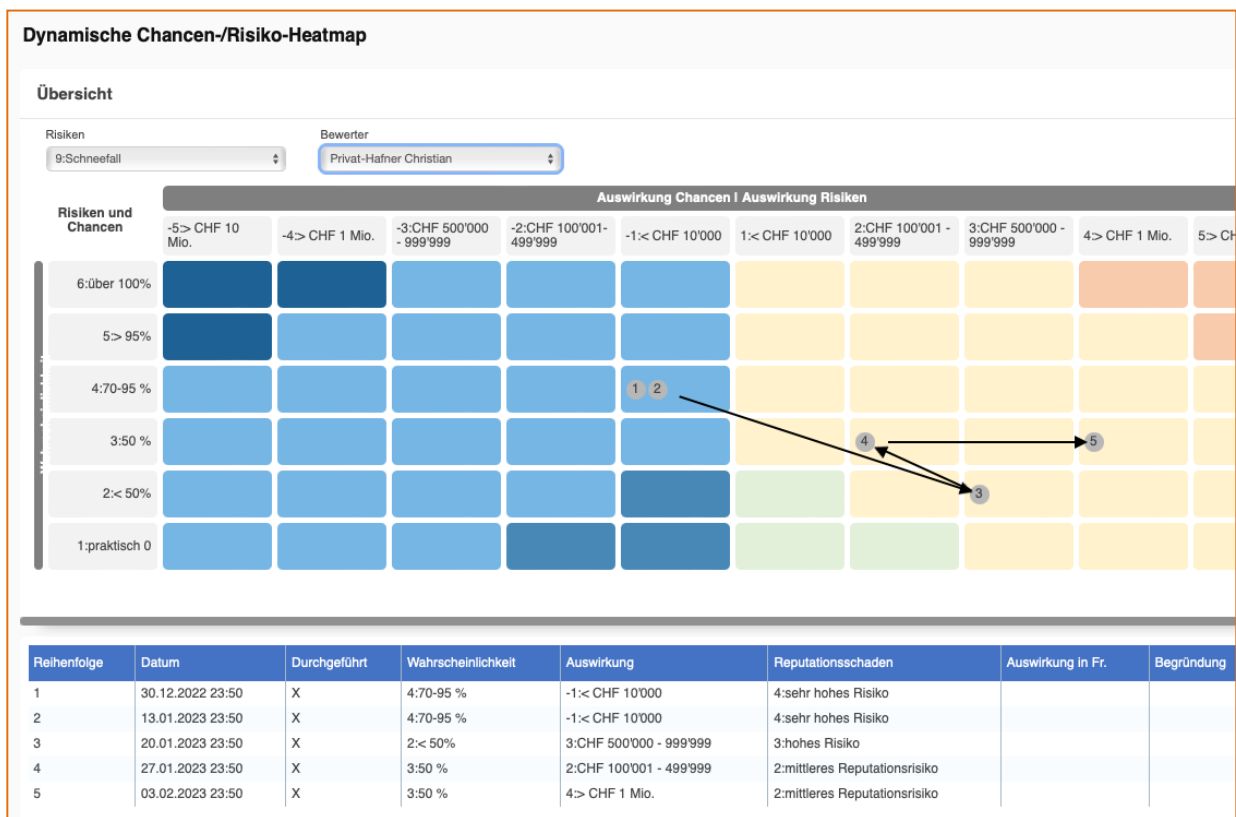
2. Reputationsrisiko

Damit die Informationen in den grafischen Darstellungen schneller erkennbar und einfacher verständlich sind, wird das Reputationsrisiko in einer separaten Matrix ausgewiesen. Auf der x-Achse wird das Reputationsrisiko abgetragen und auf der y-Achse die Multiplikation der gerateten Eintretenswahrscheinlichkeit und Schadenhöhe.

3. Dynamische Chancen-/Risiko-Heatmap

1

2



1. Die Chancen werden auf der X-Achse der Matrix in die negative Richtung abgetragen und inhaltlich wie die Risiken dargestellt.
Diese Darstellung wird durch die Bewertung des Potenzials der Chancen mit negativer Schadenhöhe erreicht.
2. Die Bewertungsergebnisse werden in ihrer zeitlichen Reihenfolge in der Matrix abgebildet und in der Legende erscheinen die Details zu jedem Bewertungsereignis.

Erarbeitungsprozess

1. Voraussetzungen

Alle Entscheidungen und Aktivitäten einer Organisation sind mit Risiken verbunden, angefangen bei der Strategie. Deshalb muss Risikomanagement (RM) als integrativer Bestandteil der Unternehmensstrategie verstanden werden.

Erst die Integration von Risiko und Strategie ermöglicht es dem Management, die besten Strategien auszuwählen und relevante Risiken zu managen.¹

Engagement der Führung

Die oberste Führungsebene will ein wirksames Risikomanagement, damit die «richtigen» Risiken eingegangen werden.

Rollen und Verantwortlichkeiten

Wille zur klaren Formulierung von Verantwortlichkeiten für das Risikomanagement auf allen Ebenen.

Geeignete personelle Ressourcen zur Übernahme der Rollen und Verantwortlichkeiten.



¹A practical guide to ISO 31000:2018 S. 15

2. Festlegen von Umfang und Kontext der Risikobeurteilung



Der erste Schritt des Risikomanagementprozesses besteht darin, den Umfang, die Grenzen und den Kontext festzulegen. Dies gewährleistet eine bessere Nutzung von Zeit, Aufwand und Ressourcen der Organisation.

Bei allen Risikomanagementaktivitäten müssen die Ziele und Werte der Organisation sowie die spezifischen Ziele des Risikobeurteilungsprozesses berücksichtigt werden.¹

3. Festlegung von Risikokriterien



Risikokriterien sind eine Reihe von Regeln oder Aussagen, die eine einheitliche Entscheidungsfindung im gesamten Unternehmen ermöglichen. Die Verwendung von Risikokriterien unterstützt eine bessere Entscheidungsfindung, wie z.B.:

- ▶ Wie wird entschieden, ob ein Risiko ausreichend kontrolliert wurde?
- ▶ Wann ist das Risiko nicht akzeptabel, so dass die Arbeit ungeachtet des Nutzens eingestellt werden muss.
- ▶ Wann ist der potenzielle Nutzen ausreichend, um das Risiko akzeptabel zu machen.
- ▶ Wie ist die relative Bedeutung von Risiken für die Ressourcenzuweisung zu beurteilen.
- ▶ Wann ist das Vorhandensein von Risiken zu bewerten?
- ▶ Wie werden Absprachen getroffen, wenn mehrere Ziele betroffen sind?

Die Risikokriterien können für verschiedene Risikoarten unterschiedlich sein und sollten mit dem maximalen Risiko, das die Organisation einzugehen bereit ist, vereinbar sein. Eine Organisation kann Kriterien festlegen, die ihre Prioritäten berücksichtigen, zum Beispiel die drei Dimensionen der Nachhaltigkeit (ökologisch, sozial und wirtschaftlich).²

¹A practical guide to ISO 31000:2018 S. 38

²A practical guide to ISO 31000:2018 S. 39

4. Risikobeurteilung

Jede Organisation muss laufend Entscheide in Ungewissheit fällen. Sie können positive, negative oder neutrale Auswirkungen haben. Risiken sollen identifiziert werden, damit sie bei Entscheidungen berücksichtigt und Massnahmen entwickelt werden können, um positive Ergebnisse zu unterstützen und negative Ergebnisse zu reduzieren.

Die Risikobeurteilung umfasst drei Schritte:

1. Risikoidentifizierung (Erkennen von Risiken)
2. Risikoanalyse (Verstehen des Risikos) und
3. Risikobewertung (Bedeutung des Risikos).¹



Umfrage + Workshop 3



¹A practical guide to ISO 31000:2018 S. 41



Risikomanagement mit swissRMTM **swissaxis**

christian.hafner@swissaxis – www.swissrm.ch – Dezember 2021