FinTec Consulting

Finance ■ Technology ■ Processes

RISIKOMANAGEMENT

MIT

Inhaltsverzeichnis Seite

Abbildungsverzeichnis Seite

1 EINLEITUNG

1.1 Zielsetzung

1.1.1 Praxisbezogen & geschäftsmäßig verwendbar

In meiner Eigenschaft als **Unternehmensberater →*11.1*** wollte ich eine sowohl für meine Kunden, als auch für mich verwendbare, einfach strukturierte und universell einsetzbare Softwarelösung schaffen um ein **unternehmensweites Risikocontrolling** zu ermöglichen.

1.1.2 Integration DSGVO

Integration in eine bereits von mir entworfene Lösung zur Erfassung des Risikos im Zusammenhang mit der **Datenschutzgrundverordnung** (DSGVO).
.

2 DEFINITIONEN

Jedes Unternehmen hat unterschiedliche Schmerzgrenzen und ertragbare Schadenssummen. Demzufolge müssen auch die Clusterungen der wichtigsten Parameter unternehmensspezifisch definiert werden können.

Während der Analysephase mit den Fachabteilungen des Kunden ist eine einfache Fragestellung notwendig. Daher empfiehlt sich statt „Wie hoch ist die Eintrittswahrscheinlichkeit in % bei technischen Ursachen?“ zu fragen, die Frage so zu formulieren: „Ist die Eintrittswahrscheinlichkeit von technischen Ursachen häufig, d.h. wöchentlich?“.

Ein weiterer Vorteil bei der Verwendung von globalen Parametern ist die rasche Neuberechnung aller Risiken, nur durch die Veränderung der Schadenspunkte, Eintrittswahrscheinlichkeiten oder Entdeckungswahrscheinlichkeit.

2.1 Unternehmensspezifische Einstellungen

2.1.1 Definition der Risikoursachen

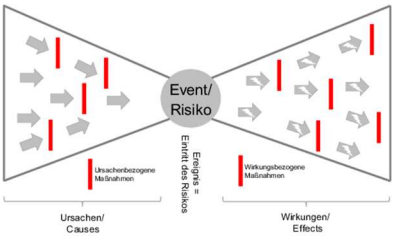
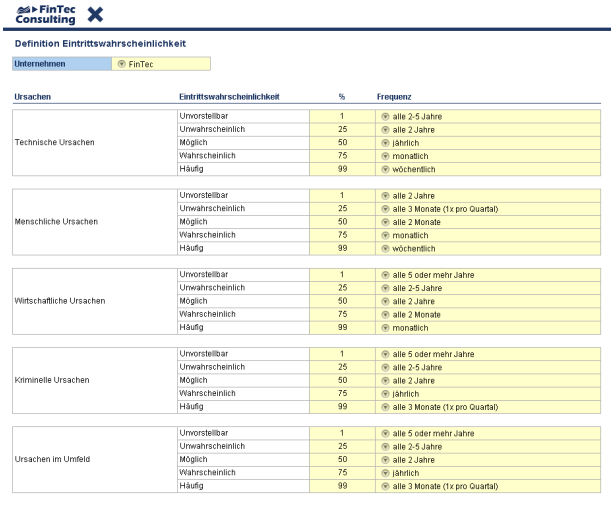


Abbildung 1 - Bow-Tie Diagramm zur Visualisierung von Ursachen und Wirkung

Die Ursachen können je nach Branche und Unternehmen unterschiedlich sein. Im wesentlichem wird es allerdings immer zumindest diese **5 Ursachen** geben:

- technische Ursachen
- menschliche Ursachen
- wirtschaftliche Ursachen
- kriminelle Ursachen
- Ursachen aus dem Umfeld (z.B. Naturereignisse)

2.1.2 Definition der Eintrittswahrscheinlichkeiten



Definition Eintrittswahrscheinlichkeit

Unternehmen: FinTec

Ursachen	Eintrittswahrscheinlichkeit	%	Frequenz
Technische Ursachen	Unvorstellbar	1	alle 2-5 Jahre
	Unwahrscheinlich	25	alle 2 Jahre
	Möglich	50	jährlich
	Wahrscheinlich	75	monatlich
	Häufig	99	wöchentlich
Menschliche Ursachen	Unvorstellbar	1	alle 2 Jahre
	Unwahrscheinlich	25	alle 3 Monate (1x pro Quartal)
	Möglich	50	alle 2 Monate
	Wahrscheinlich	75	monatlich
	Häufig	99	wöchentlich
Wirtschaftliche Ursachen	Unvorstellbar	1	alle 5 oder mehr Jahre
	Unwahrscheinlich	25	alle 2-5 Jahre
	Möglich	50	alle 2 Jahre
	Wahrscheinlich	75	alle 2 Monate
	Häufig	99	monatlich
Kriminelle Ursachen	Unvorstellbar	1	alle 5 oder mehr Jahre
	Unwahrscheinlich	25	alle 2-5 Jahre
	Möglich	50	alle 2 Jahre
	Wahrscheinlich	75	jährlich
	Häufig	99	alle 3 Monate (1x pro Quartal)
Ursachen im Umfeld	Unvorstellbar	1	alle 5 oder mehr Jahre
	Unwahrscheinlich	25	alle 2-5 Jahre
	Möglich	50	alle 2 Jahre
	Wahrscheinlich	75	jährlich
	Häufig	99	alle 3 Monate (1x pro Quartal)

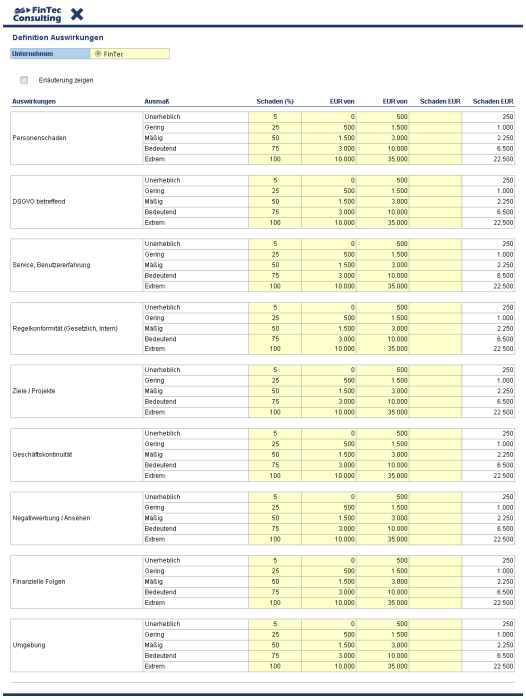
Abbildung 2 - Definition der Eintrittswahrscheinlichkeit

Die Clusterung der Eintrittswahrscheinlichkeiten erfolgt je Ursache.

Zu erfassen ist sowohl der Eintrittswahrscheinlichkeit in %, als auch die dahinterliegende Frequenz.

Die Verwendung der Frequenz ermöglicht es in den Analysengesprächen schneller und transparenter die Eintrittswahrscheinlichkeit zu besprechen: „Wie oft kommt dieser Fall vor - monatlich?“

2.1.3 Definition der Auswirkungsgrenzen



Definition Auswirkungen

Unternehmen: FinTec

Erläuterung zeigen

Auswirkungen	Ausmaß	Schaden (%)	EUR von	EUR von	Schaden EUR	Schaden EUR
Personenschaden	Unerheblich	5	0	500		250
	Gering	25	500	1.500		1.000
	Mäßig	50	1.500	3.000		2.250
	Bedeutend	75	3.000	10.000		6.500
	Extrem	100	10.000	35.000		22.500
DSGVO betreffend	Unerheblich	5	0	500		250
	Gering	25	500	1.500		1.000
	Mäßig	50	1.500	3.000		2.250
	Bedeutend	75	3.000	10.000		6.500
	Extrem	100	10.000	35.000		22.500
Service, Benutzererfahrung	Unerheblich	5	0	500		250
	Gering	25	500	1.500		1.000
	Mäßig	50	1.500	3.000		2.250
	Bedeutend	75	3.000	10.000		6.500
	Extrem	100	10.000	35.000		22.500
Regelkonformität (Gesetzlich, Intern)	Unerheblich	5	0	500		250
	Gering	25	500	1.500		1.000
	Mäßig	50	1.500	3.000		2.250
	Bedeutend	75	3.000	10.000		6.500
	Extrem	100	10.000	35.000		22.500
Ziele / Projekte	Unerheblich	5	0	500		250
	Gering	25	500	1.500		1.000
	Mäßig	50	1.500	3.000		2.250
	Bedeutend	75	3.000	10.000		6.500
	Extrem	100	10.000	35.000		22.500
Geschäftskontinuität	Unerheblich	5	0	500		250
	Gering	25	500	1.500		1.000
	Mäßig	50	1.500	3.000		2.250
	Bedeutend	75	3.000	10.000		6.500
	Extrem	100	10.000	35.000		22.500
Negativwerbung / Ansehen	Unerheblich	5	0	500		250
	Gering	25	500	1.500		1.000
	Mäßig	50	1.500	3.000		2.250
	Bedeutend	75	3.000	10.000		6.500
	Extrem	100	10.000	35.000		22.500
Finanzielle Folgen	Unerheblich	5	0	500		250
	Gering	25	500	1.500		1.000
	Mäßig	50	1.500	3.000		2.250
	Bedeutend	75	3.000	10.000		6.500
	Extrem	100	10.000	35.000		22.500
Umgebung	Unerheblich	5	0	500		250
	Gering	25	500	1.500		1.000
	Mäßig	50	1.500	3.000		2.250
	Bedeutend	75	3.000	10.000		6.500
	Extrem	100	10.000	35.000		22.500

Abbildung 3 - Definition der Auswirkungen

Grundsätzlich habe ich das mögliche Ausmaß auf 5 Cluster definiert:

- Unerheblich
- Gering
- Mäßig
- Bedeutend
- Extrem

Ebenso wurden die möglichen Auswirkungen und Anlehnung an das *HSE Risk Assessment*[1] geclustert:

Abbildung 4 - Mögliche Auswirkungen lt. HSE

Nachdem für jedes Unternehmen die Schadenshöhe unterschiedliche Folgen haben kann, muss diese auch individuell festgelegt werden können.

In den Risikomodellen besteht durch Verwendung von Durchschnitten immer die Gefahr, dass Risiken nicht korrekt eingeschätzt werden. Aus diesem Grund gibt es die Möglichkeit, den durch die Schadensbandbreite berechneten Wert auf einen zu verwendenden Schadenswert zu korrigieren.

Die Bandbreite wird für die Analysegespräche benötigt, um das mögliche Ausmaß besser erklären zu können.

Je mögliche Auswirkung steht ein zusätzlicher beschreibender Text lt. HSE zur Verfügung:

Personenschaden	Unerheblich	Adverse event leading to minor injury not requiring first aid. No impaired Psychosocial functioning.	5	0	500		250
	Gering	Minor injury or illness, first aid treatment required <3 days absence < 3 days extended hospital stay Impaired psychosocial functioning greater than 3 days less than one month.	25	500	1.500		1.000
	Mäßig	Significant injury requiring medical treatment e.g. Fracture and/or counselling. Agency reportable, e.g. HSA, Gardaí (violent and aggressive acts). >3 Day 3-8 Days extended hospital Stay Impaired psychosocial functioning greater than one month less than six months	50	1.500	3.000		2.250
	Bedeutend	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling. Impaired psychosocial functioning greater than six months.	75	3.000	10.000		6.500
	Extrem	Incident leading to death or major permanent incapacity. Event which impacts on large number of service users or member of the public. Permanent psychosocial functioning incapacity.	100	10.000	35.000		22.500

Abbildung 5 - Detaillierte Beschreibung der Personenschaden

[1] HSE Risk Assessment; Risk Management der Health and Safety Executive, http://www.hse.gov.uk/risk/

2.1.4 Definition der Entdeckungswahrscheinlichkeit

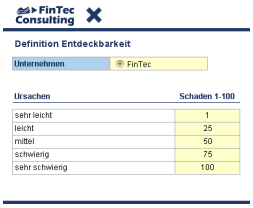


Abbildung 6 - Definition Entdeckbarkeit

Je nach Schwierigkeit der Entdeckbarkeit können Schadenspunkte vergeben werden um nach der *Failure Mode Effect Analysis (FMEA)*[2] die Risikoprioritätszahl zu ermitteln.

$$Risikoprioritätszahl = Eintrittswahrscheinlichkeit\ (\%) \times Auswirkung\ (\%) \times Entdeckungswahrscheinlichkeit\ (\%)$$

[2] WIFI/procon, Skriptum Modul 1: Risikomanagement erfassen & gestalten, Tag 2: Risikoidentifikation & -analyse, Seite 26ff

3 PHASEN IM RISIKOMANAGEMENT

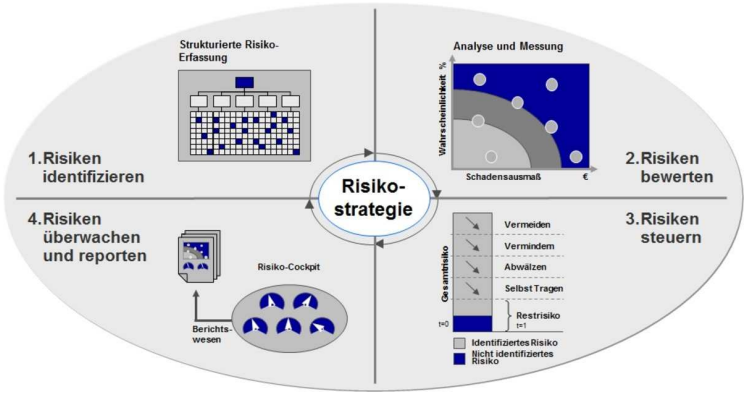


Abbildung 7 – Phasen im Risikomanagement

„[3]Das Strategische Risikomanagement bildet die integrative Klammer und das Fundament des gesamten Risk-Management-Prozesses.

Es beinhaltet vor allem die Formulierung von **Risk-Management-Zielen in Form einer "Risikostrategie"**. [..]

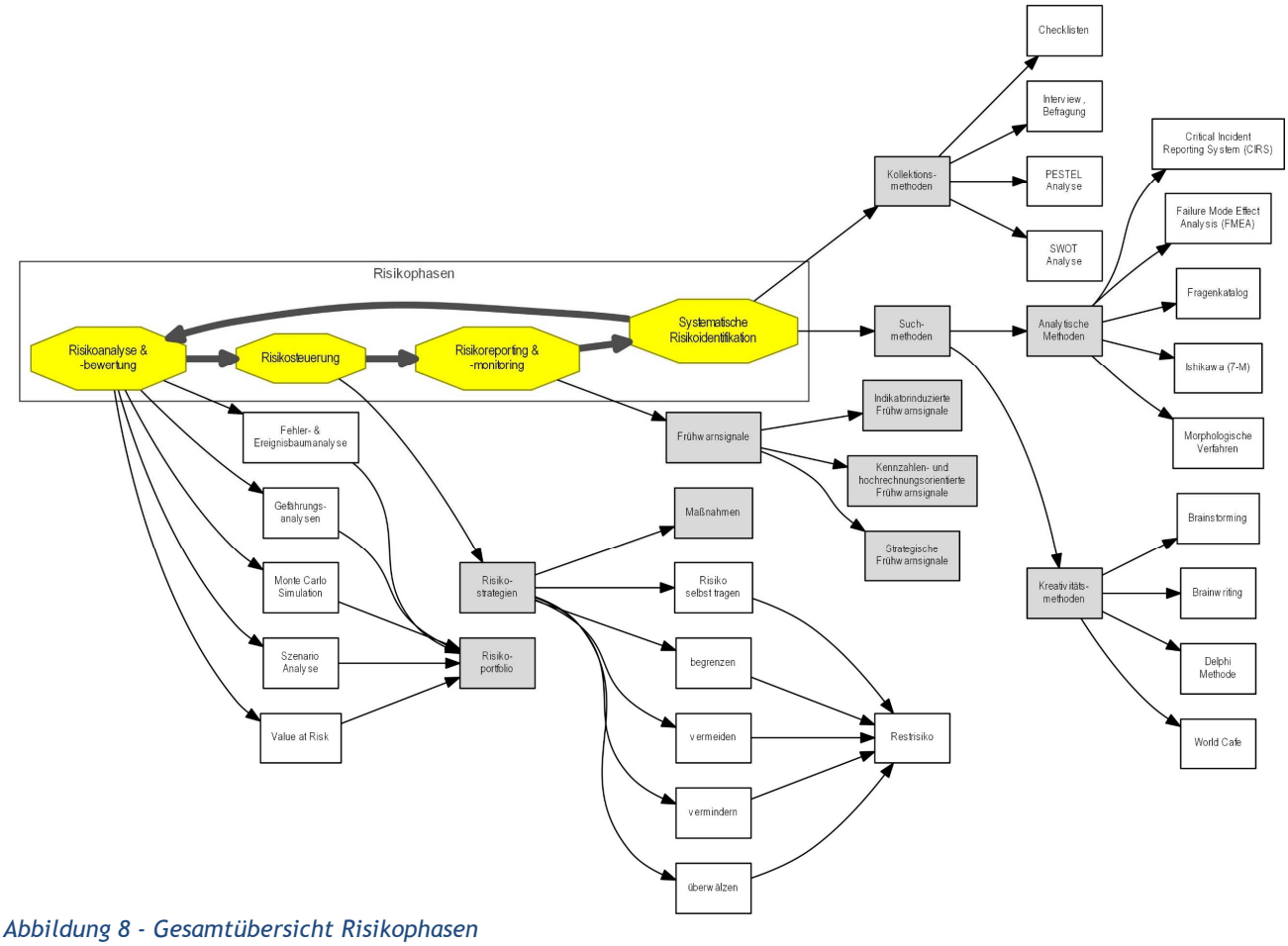


Abbildung 8 - Gesamtübersicht Risikophasen

Das operative Risikomanagement (vgl. Abbildung oben) beinhaltet den Prozess der **systematischen und laufenden Risikoanalyse** der Geschäftsabläufe. [..] Für einen effizienten Risk-Management-Prozess kommt es darauf an, dass dieser als kontinuierlicher Prozess – im Sinne eines Regelkreises – **in die Unternehmensprozesse integriert** wird.“

[3] Quelle: RiskNet – The Risk Management Network, https://www.risknet.de/wissen/risk-management-prozess/

Abbildung 9 - Übersicht Startseite Softwarelösung

Diesem Aufbau wurde auch bei der Implementierung der Lösung Rechnung getragen.

Sowohl in der Menüführung, als auch in der Integration.

Aufgrund der Prevero-Architektur kann das Risikomanagement leicht bei Neu- und Bestandskunden in das BI (Business Intelligence) bzw. CPM →***11.2*** (Corporate Performance Measurement) Modul von Prevero (und somit in die zentrale Stelle für das Reporting der Unternehmensprozesse) integriert werden.

4 RISIKOIDENTIFIKATION

Risiken können in dieser Lösung nach zwei grundsätzlichen Methoden erfasst, bzw. analysiert werden. Selbstverständlich ist auch eine Kombination der beiden Methoden möglich.

4.1 Baummethode

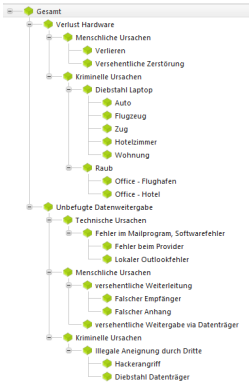


Abbildung 10 – Baumbasierte Risikodefinition

Es wurde eine „Baum“-basierende Lösung entwickelt, mit der beliebige Baumstrukturen dargestellt werden können. Mit dieser Lösung ist eine grundsätzliche Abbildung u.a. der folgenden Methoden möglich:

- Ishikawa Methode
- FMEA Analyse
- Ursache – Ereignis – Wirkung

4.2 Listenbasierte Methode

4.2.1 Risikoauswahl

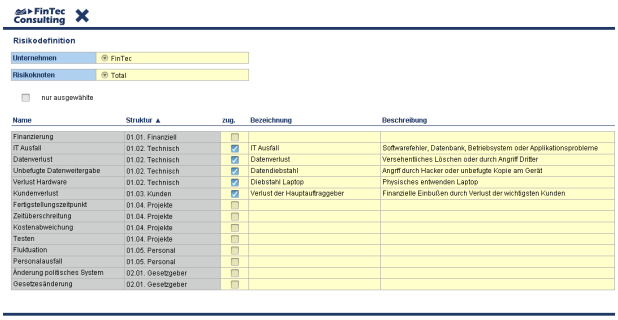


Abbildung 11 - Listenbasierte Risikodefinition

Aus einer vorgegebenen Liste von möglichen Risiken können für das Unternehmen zutreffende ausgewählt werden.

Die Liste ist in Kategorien zusammengefasst und kann beliebig ergänzt werden.

Zusätzlich kann eine unternehmensinterne Bezeichnung vergeben werden, sowie eine genaue Beschreibung für das Unternehmen

Der Detailgrad der vorgegeben möglichen Risiken ist beliebig anpassbar. Sehr zu empfehlen im Bereich IT-Riskmanagement ist der *IT-Grundschutz-Katalog*[4] der Gefährdungskataloge aller möglichen Risiken mit Beschreibung, sowie Maßnahmenkataloge enthält.

Im Falle meiner Risikoanalyse z.B. die Gefährdung **G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten**

[5]„Durch den Diebstahl von Datenträgern, IT-Systemen, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen

[4] IT-Grundschutz-Katalog des Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[5] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g00/g00016.html?nn=6604996

Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Wenn durch den Diebstahl vertrauliche Informationen offengelegt werden, kann dies weitere Schäden nach sich ziehen. Neben Servern und anderen teuren IT-Systemen werden auch mobile IT-Systeme, die unauffällig und leicht zu transportieren sind, häufig gestohlen. Es gibt aber auch Fälle, in denen gezielt Datenträger, wie Dokumente oder USB-Sticks, entwendet wurden, um an die darauf gespeicherten vertraulichen Informationen zu gelangen."

Durch die listenbasierte Methode können auch anonymisierte Vergleiche zwischen unterschiedlichen Unternehmen, bzw. Unternehmen innerhalb eines Konzerns angestellt werden.

4.2.2 Ursachenzuordnung

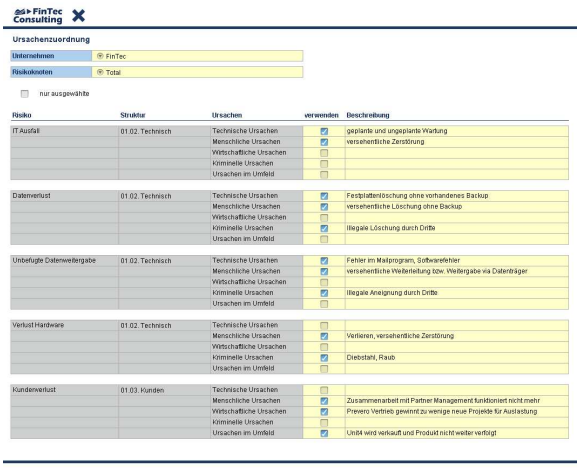


Abbildung 12 - Ursachenzuordnung

Für jede der ausgewählten Risiken kann entschieden werden, welche der definierten Ursachen Bedeutung haben können.

Für die ausgewählten Ursachen ist jedenfalls eine genauere Beschreibung anzuführen, da diese je Unternehmen unterschiedlich sein kann.

4.2.3 Auswirkungszuordnung

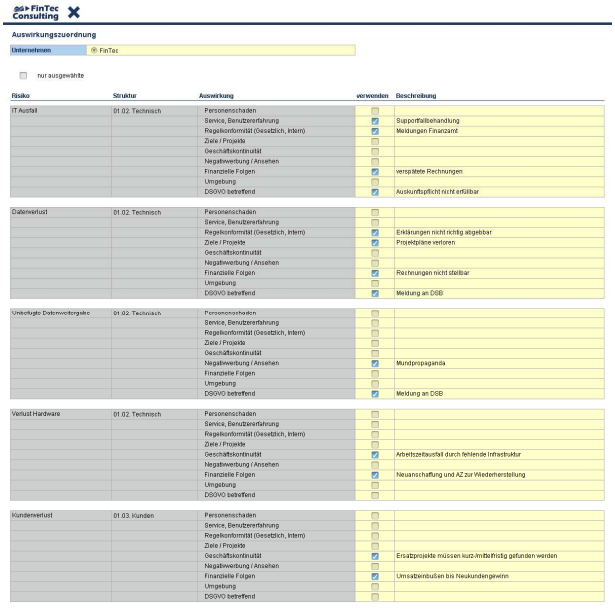


Abbildung 13 - Auswirkungszuordnung

Für jede der ausgewählten Risiken kann angegeben werden, welche der Auswirkungskategorien (z.B. nach HSE) zutreffen und wie genau die Auswirkung im konkreten Unternehmen aussieht.

5 RISIKOBEWERTUNG

5.1 Baummethode

	Measure		
BAUM_Ereignisbaum	Eintrittswahscheinlichkeit (1..100)	Schaden (1..100)	Entdeckungswahrscheinlichkeit (1..100)
Gesamt	6,88	67,19	72,25
Verlust Hardware	4,25	100,00	100,00
Menschliche Ursachen	5,50	100,00	100,00
Verlieren	1,00	100,00	100,00
Versehentliche Zerstörung	10,00	100,00	100,00
Kriminelle Ursachen	3,00	100,00	100,00
Diebstahl Laptop	4,40	100,00	100,00
Auto	1,00	100,00	100,00
Flugzeug	1,00	100,00	100,00
Zug	5,00	100,00	100,00
Hotelzimmer	10,00	100,00	100,00
Wohnung	5,00	100,00	100,00
Raub	3,00	100,00	100,00
Office - Flughafen	1,00	100,00	100,00
Office - Hotel	5,00	100,00	100,00
Unbefugte Datenweitergabe	10,14	25,00	36,57
Technische Ursachen	5,00	25,00	3,00
Fehler im Mailprogram, Softwarefehler	5,00	25,00	3,00
Fehler beim Provider	5,00	25,00	1,00
Lokaler Outlookfehler	5,00	25,00	5,00
Menschliche Ursachen	17,00	25,00	66,67
versehentliche Weiterleitung	25,00	25,00	75,00
Falscher Empfänger	25,00	25,00	75,00
Falscher Anhang	25,00	25,00	75,00
versehentliche Weitergabe via Datenträger	1,00	25,00	50,00
Kriminelle Ursachen	5,00	25,00	25,00
Illegale Aneignung durch Dritte	5,00	25,00	25,00
Hackerangriff	5,00	25,00	25,00
Diebstahl Datenträger	5,00	25,00	25,00

Abbildung 14 - Risikobewertung mittels Baummethode

Jede der festgelegt Baumelemente wird einzeln nach

- Eintrittswahrscheinlichkeit
- Schaden
- Entdeckungswahrscheinlichkeit

bewertet.

Alle Knotenelement des Baumes werden automatisch aggregiert und gewichtet.

Bei der Verwendung ist immer zu bedenken, dass eine Berechnung zwar mathematisch richtig sein kann, aber das Resultat trotzdem keinen Sinn ergeben kann, bzw. das Risiko falsch darstellt.

Der gewichtete Schaden von Eintrittswahrscheinlichkeit = 1 und Schaden = 100 ist 1%, aber tatsächlich ist der Schaden 100 wenn er eintritt.

5.2 Listenbasierte Methode

5.2.1 Eintrittswahrscheinlichkeiten

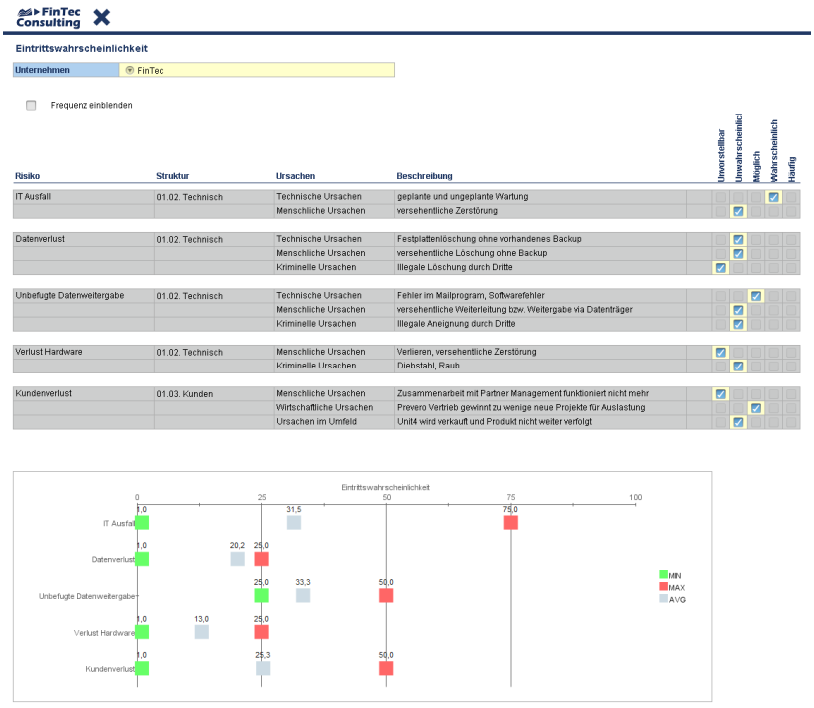


Abbildung 15 - Eintrittswahrscheinlichkeit

Bei der listenbasierten Methode wird die Eintrittswahrscheinlichkeit auch nach den einzelnen Ursachen erfasst, aber nicht nur als Durchschnittswert dargestellt.

Die Erfassung erfolgt nicht mehr mit % Eingaben, sondern mit den leichter verständlichen verbalen Bezeichnungen.

Es wird auch eine Bandbreite gezeigt, in der sich die Eintrittswahrscheinlichkeit bewegt.

So ist beim IT Ausfall der Durchschnittswert zwar 31,5%, aber es ist auch eine Ursache dabei, die 75% beinhaltet.

Dies ist für die Erstellung des Maßnahmenkataloges unbedingt zu berücksichtigen.

5.2.2 Auswirkungen

Abbildung 16 - Auswirkungen

Hier werden pro Risiko und Auswirkung das zur erwartende Schadensausmaß ausgewählt.

Es wird auch eine Bandbreite gezeigt, in der sich der Schaden, bzw. die Schadenssumme bewegt.

Mit dieser Methode bleiben auch immer die maximalen Schadensgrößen (unabhängig von der Eintrittswahrscheinlichkeit) im Blick.

5.2.3 Entdeckungswahrscheinlichkeit

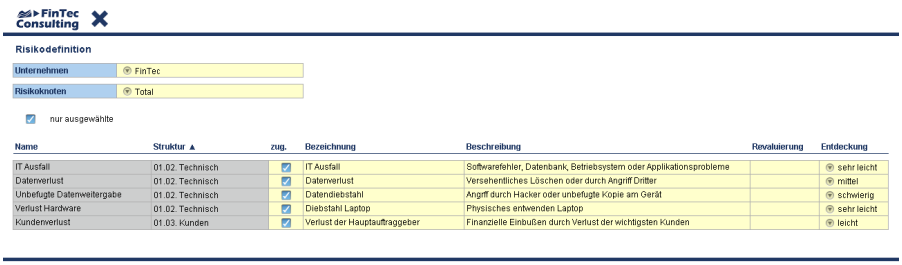


Abbildung 17 - Entdeckungswahrscheinlichkeit

Durch die Eingabe der Entdeckungswahrscheinlichkeit ist auch die Berechnung der Risikoprioritätszahl möglich.

Dieser erfolgt in der bereits bekannten Eingabemaske für die Risikodefinition

5.2.4 Ergebnisse / Reports

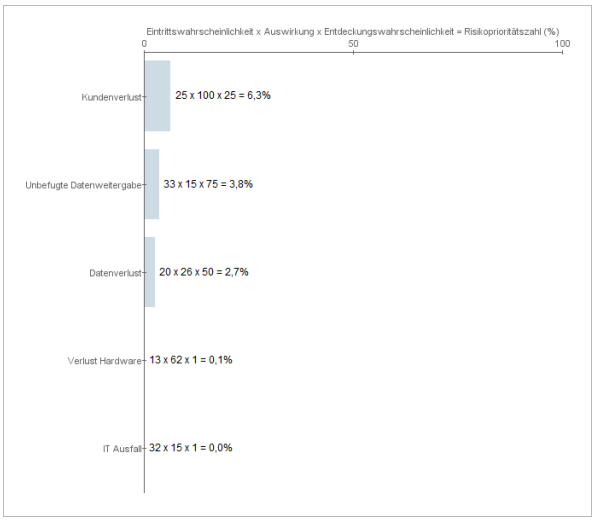


Abbildung 18 - Prioritätenliste aufgrund Risikopriorität-szahl

Alle Risiken können nach den Clustern oder einzeln ausgewertet werden.

Eine Übersicht der Risikopriorität-szahl ermöglichst eine erste Priorisierung der Risiken.

Wie bereits erwähnt bieten Durchschnittsberechnungen immer die Gefahr gewisse Risiken zu unterschätzen.

Daher gibt es auch eine Prioritätenliste nach Bandbreiten und Schadenssumme.

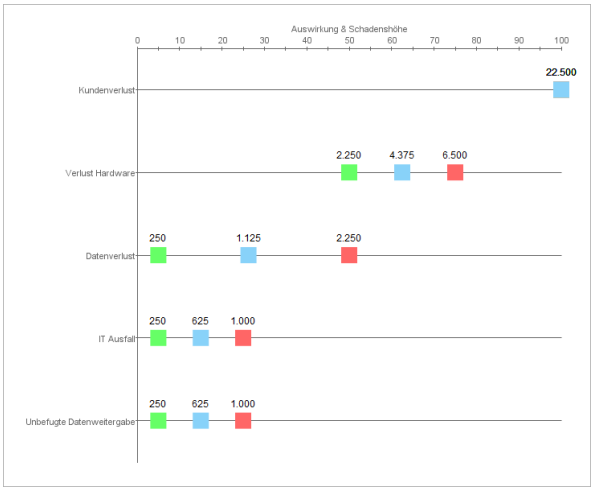


Abbildung 19 - Prioritätenliste aufgrund Auswirkung & Schadenshöhe

Im Falle von FinTec Consulting ist das größte Risiko der Verlust des größten Kunden *Unit4/Prevero*.

An zweiter Stelle liegt der Verlust der Hardware, da somit mittel- und langfristig die Arbeit an den Projekten nicht mehr möglich wäre.

Hingegen rangiert ein IT-Ausfall oder eine unbefugte Datenweitergabe an unterster Stelle.

Dies ist gerade aufgrund der DSGVO besonders erfreulich.

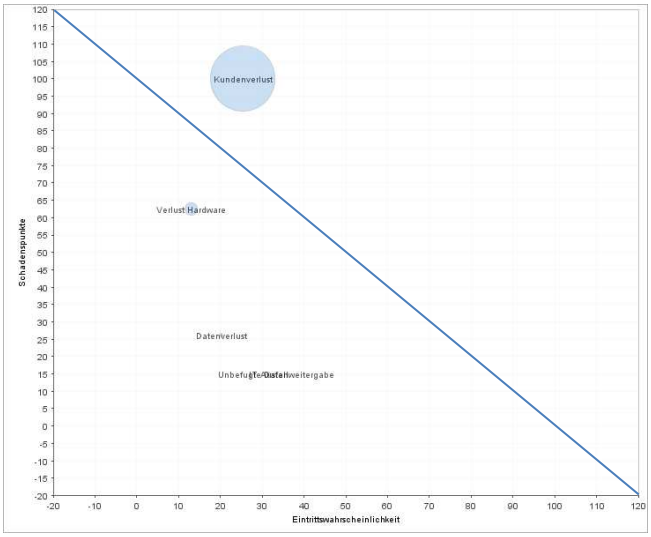


Abbildung 20 - Risikoportfolio nach Risiken

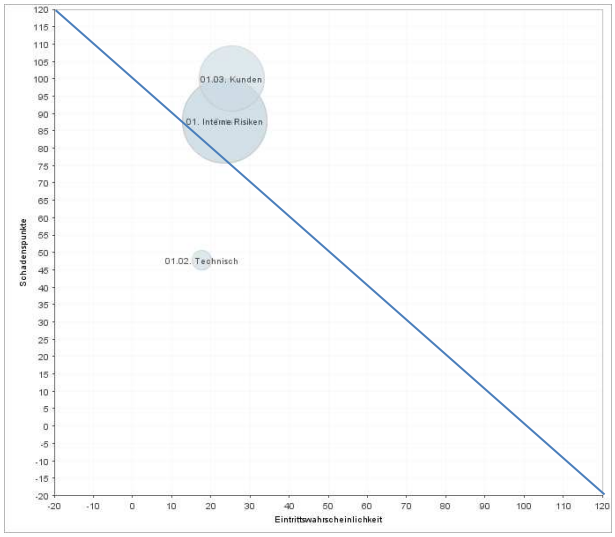


Abbildung 21 - Risikoportfolio nach Cluster

6 RISIKOSTEUERUNG

6.1 Baummethode

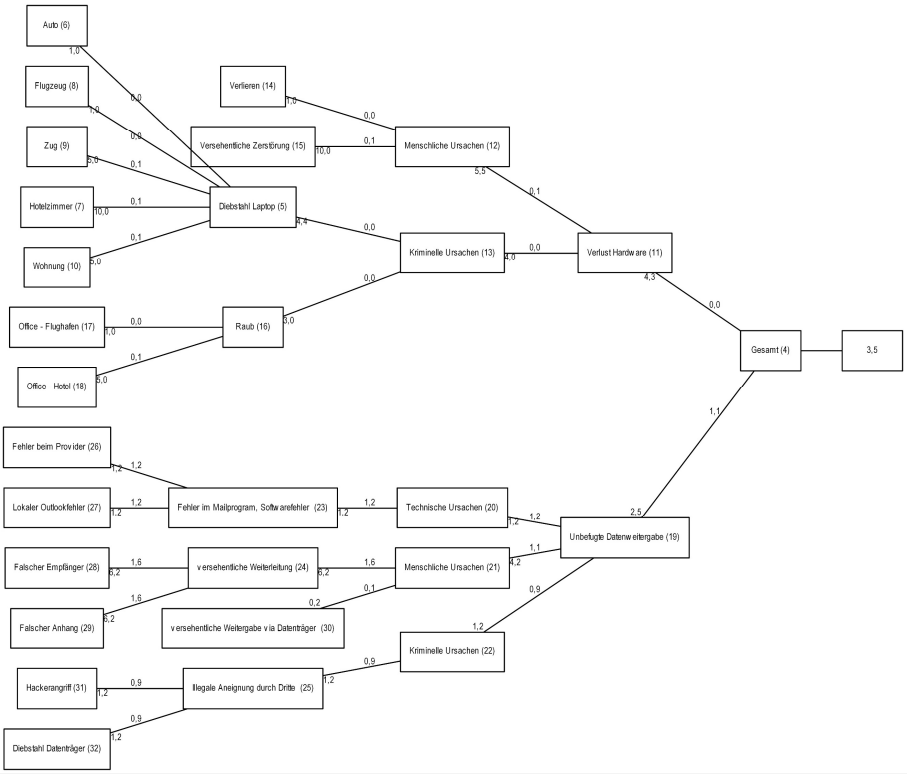


Abbildung 22 - Risikosteuerung Baummethode

Die vorher erfassten Daten können mittels grafischer Aufbereitung dargestellt werden.

Direkt am abgebenden Kästchen befindet sich die Schadenspunkte (0..100).

Auf dem Linien werden die Risikoprioritätszahlen dargestellt.

Durch Rückwärtsanalyse kann schnell der kritische Grund ermittelt werden.

In meinem Fall: Verlust Hardware → Kriminelle Ursachen → Diebstahl Laptop → Hotelzimmer

6.2 Listenbasierte Methode

6.2.1 Risikomatrix

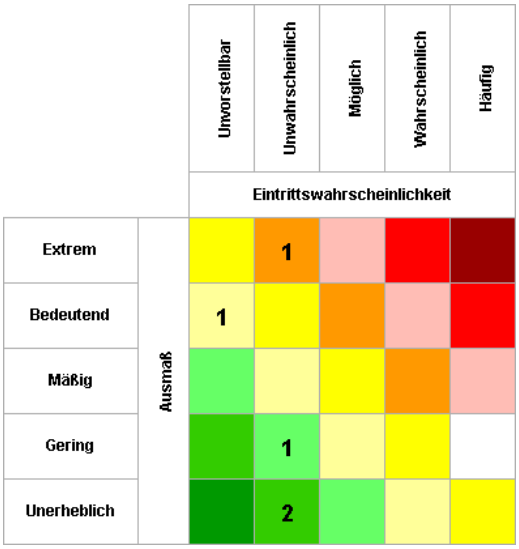


Abbildung 23 - Risikomatrix

Eines der Ergebnisse der listenbasierten Eingaben ist eine Risikomatrix nach Eintrittswahrscheinlichkeit und Ausmaß unter Angabe der Anzahl der Risiken.

In der Lösung kann direkt auf die gewünschte Kombination geklickt werden, um weitere Details zu erhalten.

Bei FinTec ist das größte Ausmaß der *Kundenverlust*, auch wenn die Eintrittswahrscheinlichkeit sehr gering ist.

6.2.2 Risikostrategie

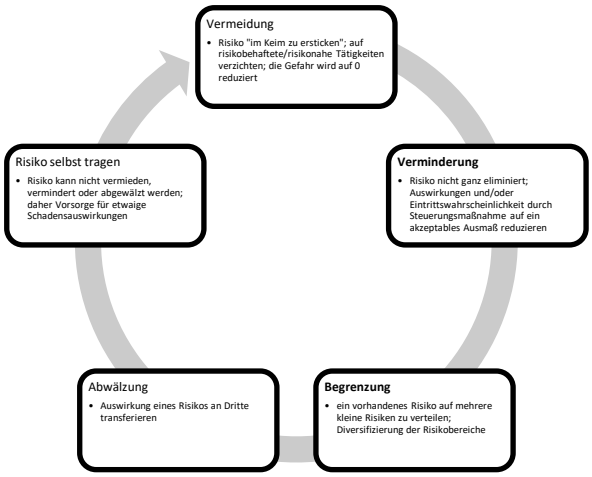
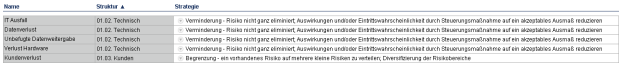


Abbildung 24 - Risikostrategie

Die Auswahlmöglichkeit der Risikostrategie wurde aus den Seminarunterlagen übernommen[6].

In der Softwarelösung kann für jedes Risiko eine Risikostrategie gewählt werden.

Im Falle meines Unternehmens sieht die Risikostrategie wie folgt aus:

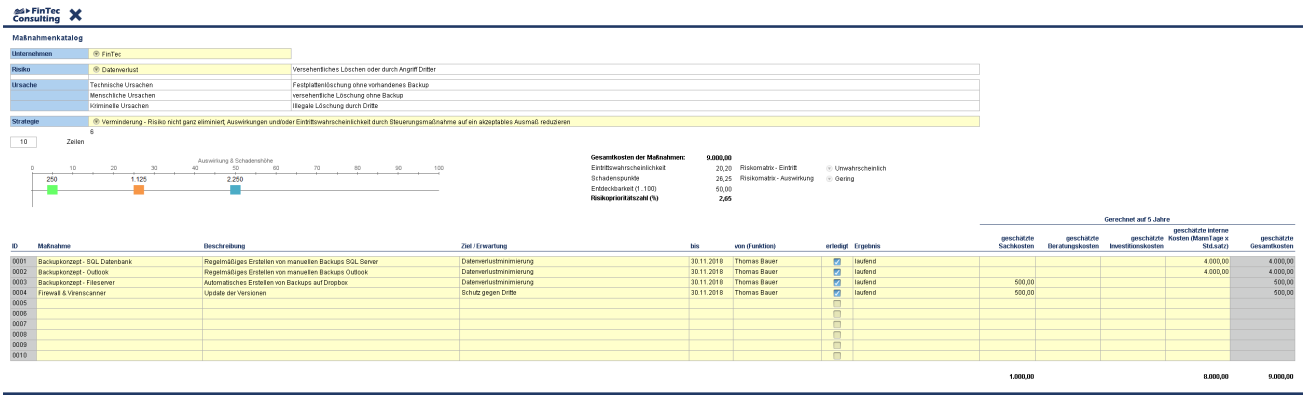


Name	Struktur ▲	Strategie
IT Ausfall	01.02. Technisch	Verminderung - Risiko nicht ganz eliminiert, Auswirkungen und/oder Eintrittswahrscheinlichkeit durch Steuerungsmaßnahme auf ein akzeptables Ausmaß reduzieren
Datenverlust	01.02. Technisch	Verminderung - Risiko nicht ganz eliminiert, Auswirkungen und/oder Eintrittswahrscheinlichkeit durch Steuerungsmaßnahme auf ein akzeptables Ausmaß reduzieren
Unbefugte Datenweitergabe	01.02. Technisch	Verminderung - Risiko nicht ganz eliminiert, Auswirkungen und/oder Eintrittswahrscheinlichkeit durch Steuerungsmaßnahme auf ein akzeptables Ausmaß reduzieren
Verlust Hardware	01.02. Technisch	Verminderung - Risiko nicht ganz eliminiert, Auswirkungen und/oder Eintrittswahrscheinlichkeit durch Steuerungsmaßnahme auf ein akzeptables Ausmaß reduzieren
Kundenverlust	01.03. Kunden	Begrenzung - ein vorhandenes Risiko auf mehrere kleine Risiken zu verteilen; Diversifizierung der Risikobereiche

Abbildung 25 - Risikostrategie FinTec

Unter Berücksichtigung der Risikostrategie ergibt sich der Maßnahmenkatalog.

6.2.3 Maßnahmenkatalog



Maßnahmenkatalog

Unternehmen	FinTec	
Risiko	Datenverlust	Versehentliches Löschen oder durch Angriff Dritter
Ursache	Technische Ursachen	Festplattenlöschung ohne vorhandenes Backup
	Menschliche Ursachen	versehentliche Löschung ohne Backup
	Kriminelle Ursachen	Illegale Löschung durch Dritte
Strategie	Verminderung - Risiko nicht ganz eliminiert, Auswirkungen und/oder Eintrittswahrscheinlichkeit durch Steuerungsmaßnahme auf ein akzeptables Ausmaß reduzieren	

Gesamtkosten der Maßnahmen: 9.000,00
Eintrittswahrscheinlichkeit 20,20 Risikomatrix - Eintritt: Unwahrscheinlich
Schadenspunkte 26,25 Risikomatrix - Auswirkung: Gering
Entdeckbarkeit (1..100) 50,00
Risikoprioritätszahl (%) 2,65

ID	Maßnahme	Beschreibung	Ziel / Erwartung	bis	von (Funktion)	erledigt	Ergebnis	Gerechnet auf 5 Jahre: geschätzte Sachkosten	geschätzte Beratungskosten	geschätzte Investitionskosten	geschätzte interne Kosten (Mann-Tage x Std.satz)	geschätzte Gesamtkosten
0001	Backupkonzept - SQL Datenbank	Regelmäßiges Erstellen von manuellen Backups SQL Server	Datenverlustminimierung	30.11.2018	Thomas Bauer	☑	laufend				4.000,00	4.000,00
0002	Backupkonzept - Outlook	Regelmäßiges Erstellen von manuellen Backups Outlook	Datenverlustminimierung	30.11.2018	Thomas Bauer	☑	laufend				4.000,00	4.000,00
0003	Backupkonzept - Fileserver	Automatisches Erstellen von Backups auf Dropbox	Datenverlustminimierung	30.11.2018	Thomas Bauer	☑	laufend	500,00				500,00
0004	Firewall & Virenscanner	Update der Versionen	Schutz gegen Dritte	30.11.2018	Thomas Bauer	☑	laufend	500,00				500,00
0005						☐						
0006						☐						
0007						☐						
0008						☐						
0009						☐						
0010						☐						
								1.000,00			8.000,00	9.000,00

Abbildung 26 - Maßnahmenkatalog

Zu jedem Risiko ist über diese Eingabemaske sowohl die *Risikostrategie*, als auch die daraus resultierten Maßnahmen zu erfassen.

[6] WIFI/procon, Skriptum Modul 1: Risikomanagement erfassen & gestalten, Tag 3: Risikosteuerung, Monitoring & Reporting, Seite 13ff

7 RISIKOÜBERWACHUNG

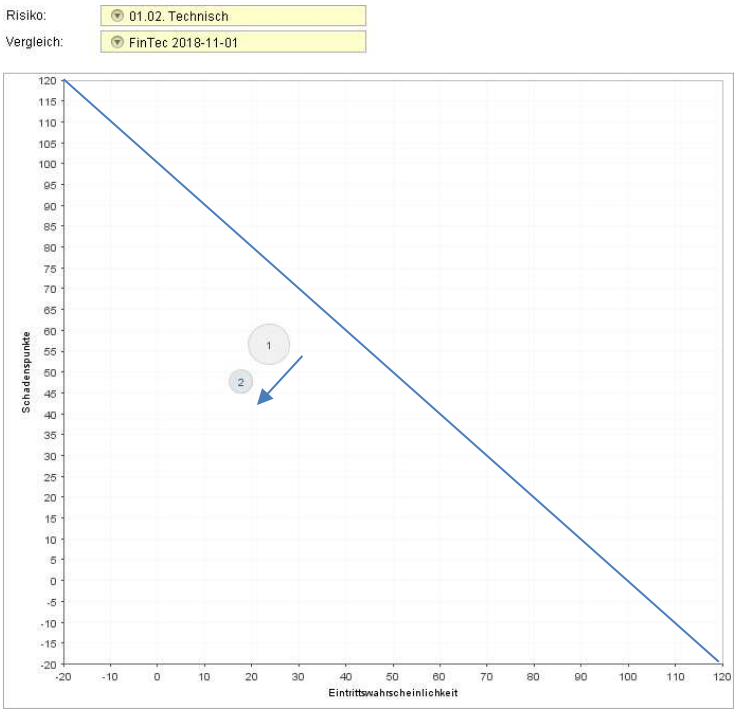


Abbildung 27 - Risikoüberwachung

Prevero bietet eine integrierte Funktionalität zur Historisierung von Daten. Mittels der Kopie eines Dimensionelementes (hier zB. das Element CO_Company, können alle Daten dieses Elementes mit kopiert werden.

Das heißt, mit dieser Funktionalität können „Zwischenstände“ des Risikocontrolling erstellt und natürlich auch vergleicht werden. Damit sind z.B. Verschiebungen in der Risikoanalyse nach einer Revaluierung schön darstellbar.

In diesem Fall haben sich durch die Maßnahmen die *technischen Risiken* in Eintrittswahrscheinlichkeit, Schadensausmaß und Kosten (Umfang) verändert/verschoben.

8 INTEGRATION IN DIE DATENSCHUTZGRUNDVERORDNUNG

8.1 Zusammenhang Risikomanagement und Datenschutzgrundverordnung

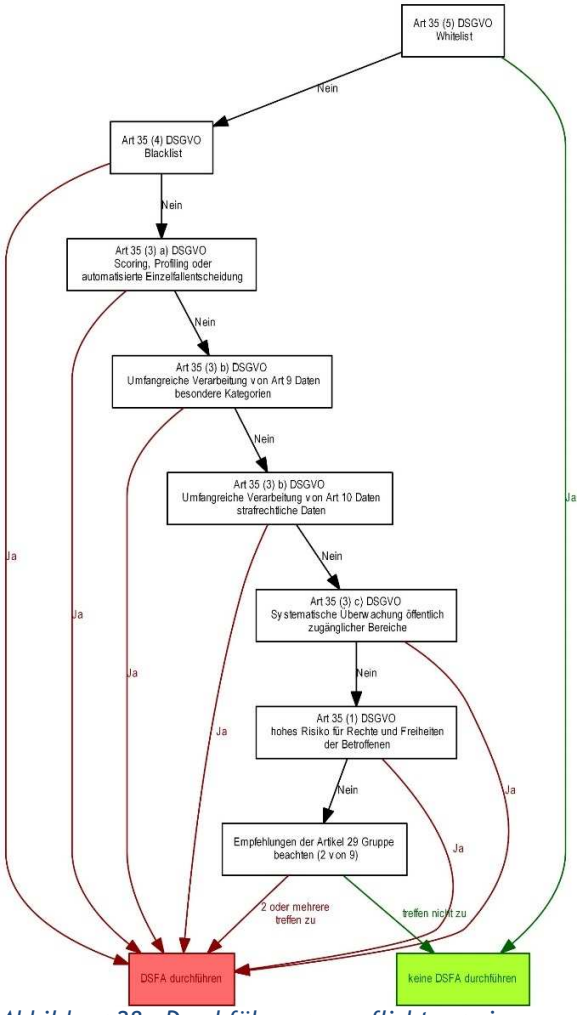


Abbildung 28 - Durchführungsverpflichtung einer Datenschutzfolgenabschätzung

Die rechtliche Grundlage bietet hier der **Artikel 24 der Datenschutzgrundverordnung**. **→*11.3***, dieser verpflichtet den Verantwortlichen zum:

- Feststellen der **Eintrittswahrscheinlichkeit** und Schwere der **Risiken** (= risikoangemessen) und
- Implementieren geeigneter technischer und organisatorischer Maßnahmen (TOM)
- Überprüfung der Maßnahmen und
- Auditierung der Maßnahmen

Also defacto einem klassischen Risikomanagementsystem.

Des weiteren greift **Artikel 35 Datenschutz-Folgenabschätzung**. **→*11.4*** Wann eine Datenschutz-Folgenabschätzung durchgeführt werden muss, kann dem Schaubild links entnommen werden.

Das bedeutet zwangsläufig, dass aus Sicht der DSGVO vermehrt Risikoanalysen durchgeführt werden müssen.

Das erfordert auch ein besonderes Qualifaktionsprofil für den Datenschutzbeauftragten:

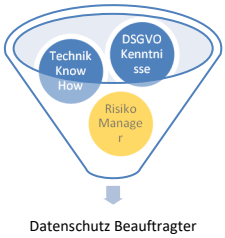


Abbildung 29 - Qualifikationsprofil Datenschutzbeauftragter

8.2 Integration in meine bereits entwickelte DSGVO Lösung

Abbildung 30 - IT Risikoanalyse

Insbesondere das IT Riskmanagement erfährt durch die DSGVO eine zusätzliche Bedeutung. In der DSGVO Lösung wurde der links skizzierte Ansatz verfolgt.

Die Integration der Lösung erfolgt einfach durch Ergänzung der Softwarelösung in der vorhandenen Risikostruktur.

9 ZUSAMMENFASSUNG UND ABSCHLIESSENDE BEMERKUNGEN

9.1 Zur Softwarelösung

Die *Baummethode* bietet sich an, wenn schnell eine Analyse durchgeführt werden soll, da ohne vorhergehende Definitionen gearbeitet werden kann. Ebenso ist die Zusammenhangsdarstellung ein mächtiges Instrument. Allerdings sind Vergleiche zwischen Themen nicht möglich und eine Integration in bestehende CPM-Module nicht leicht machbar.

Die *Listenbasierte Methode* bietet eine rasche Auswahl an bekannten Risiken, aber verhindert eventuell aus Bequemlichkeit das „eigene Denken“ und somit die Sicht auf das eigene Unternehmen.

Großer Vorteil ist die Integration in bestehende Modelle und auch BSC →*11.5* Balanced Scorecards.

9.2 Zur Integration / Einbindung in bestehende Modelle

Wie ein Risikocontrolling in die BSC integriert werden kann zeigt folgende Darstellung. Ausgangslage war der klassische BSC Ablauf[7]

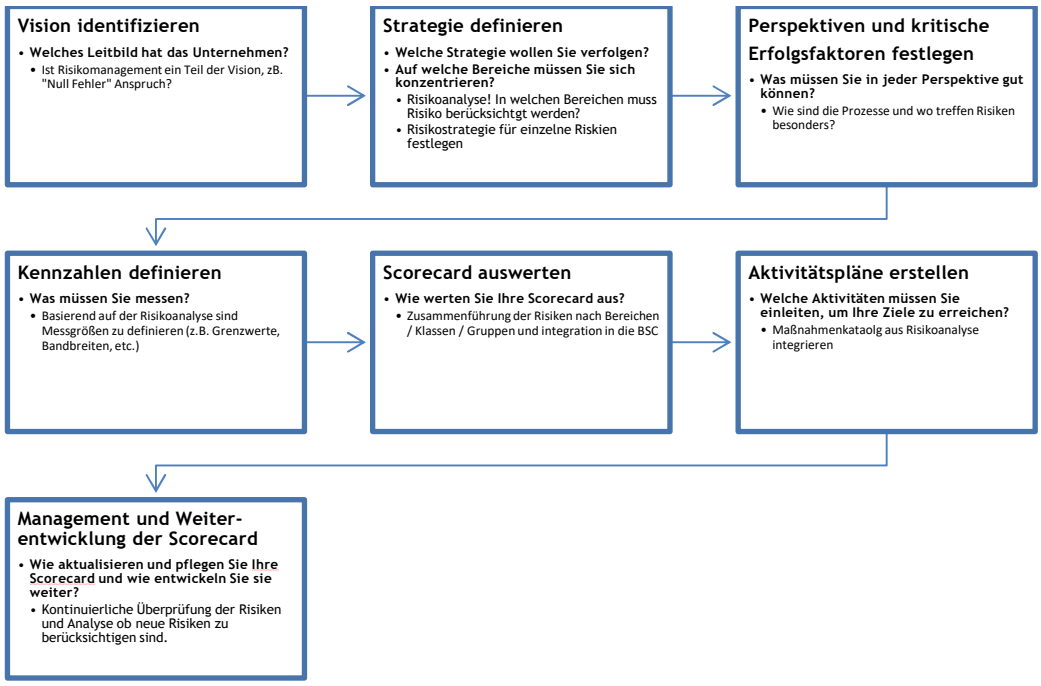


Abbildung 31 - Balance Scorecard Integration

[7] Quelle: Blanced-Scorecard.de, http://www.balanced-scorecard.de/konzept.htm

10 THEORIE ZUSAMMENFASSUNG

10.1 Risiko, Begriffsdefinitionen

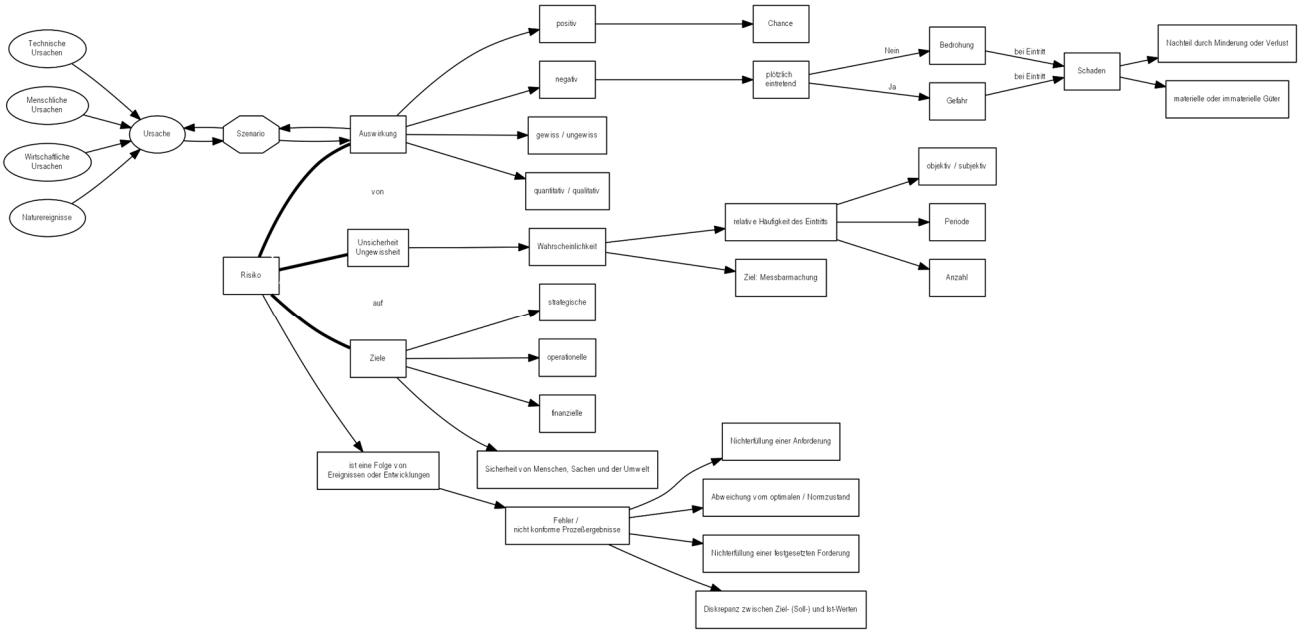


Abbildung 32 - Darstellung Begriffszusammenhänge[8]

10.2 DEMING-Kreis, PDCA-Zyklus

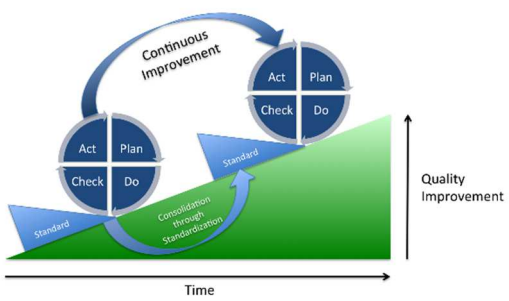


Abbildung 33 - Continuous Improvement

„Der PDCA-Zyklus beschreibt die Phasen im kontinuierlichen Verbesserungsprozess (KVP). KVP ist die Grundlage aller Qualitätsmanagement-Systeme. Damit wird im Unternehmen eine stetige Verbesserung der Prozesse und Abläufe verfolgt“[9]

[8] WIFI/procon, Skriptum Modul 1: Risikomanagement erfassen & gestalten, Tag 1: Risikoidentifikation & -analyse, Seite 10ff
[9] Quelle: Wikipedia, https://de.wikipedia.org/wiki/Demingkreis

11 ANHANG UND ANLAGEN

11.1 Informationen über Finance & Technology Consulting e.U.

Die seit 2015 bestehende Finance & Technology Consulting e.U. (FinTec) sieht ihren Schwerpunkt in der Analyse von Finanzabteilungen in Unternehmen. FinTec bietet Beratung und Verbesserungsmaßnahmen zu Organisationsstrukturen, Prozessen und IT Landschaft an. Weiters implementieren bzw. unterstützen wir bei der Implementierung von Softwarelösungen.
Gewerbescheine:

- Unternehmensberatung einschließlich der Unternehmensorganisation
- Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik

www.fintec-consulting.com

11.2 Corporate Performance Management (CPM)

Corporate Performance Management (CPM) ist ein Bereich von Business Intelligence (BI), der sich mit dem Monitoring und der Verwaltung der Leistung einer Organisation beschäftigt. Zur Bewertung dienen Leistungskennzahlen (Key Performance Indicators, KPIs) wie Umsatz, Return on Investment (ROI) sowie Gemein- und Betriebskosten. CPM wird häufig auch als Business Performance Management (BPM) oder Enterprise Performance Management (EPM) bezeichnet.

In der Vergangenheit nur innerhalb von Finanzabteilungen genutzt, ist CPM-Software inzwischen für den Einsatz im gesamten Unternehmen konzipiert, oft als Ergänzung zu Business-Intelligence-Systemen. CPM-Software enthält Funktionen für Prognosen, Budgetierung und Planung, außerdem grafische Scorecards und Dashboards, um Unternehmensinformationen anzuzeigen und bereitzustellen. Eine CPM-Oberfläche zeigt in der Regel Angaben zu Leistungskennzahlen an, sodass die Mitarbeiter ihre individuelle und die Projektleistung bezüglich der Unternehmensziele und -strategien verfolgen können. Einige Firmen verwenden zusammen mit ihren CPM-Systemen etablierte Managementinstrumente, zum Beispiel Balanced Scorecard oder Six Sigma.

Quelle: Techtarget, SearchEnterpriseSoftware.de, https://www.searchenterprisesoftware.de/definition/Corporate-Performance-Management-CPM

11.3 Datenschutzgrundverordnung Artikel 24

Art. 24 DSGVO
Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risi-ken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbei-tung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maß-nahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortli-chen umfassen.

(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizie-rungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

11.4 Datenschutzgrundverordnung Artikel 35

Art. 35 DSGVO
Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezo-gener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Daten-schutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a. systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grund-lage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten o-der diese in ähnlich erheblicher Weise beeinträchtigen;
b. umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
c. systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Daten-schutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. 2Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
b. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
c. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
d. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Si-cherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sicherge-stellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rech-nung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durch-geführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Uni-onsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge re-geln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass die-ser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkei-ten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbei-tung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsicht-lich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

11.5 Balanced Scorecard (BSC)

„Die Balanced Scorecard(BSC) ist ein Konzept zur Umsetzung einer Unternehmensstrategie. Eine BSC beginnt bei der Vision und Strategie des Unternehmens und definiert auf dieser Basis kritischen Erfolgsfaktoren (KEF). Kenn-zahlen werden dann so aufgebaut, dass sie die Zielsetzung und Leistungsfähigkeit in kritischen Bereichen der Strategie fördern. Die BSC ist daher ein aus Vision und Strategie abgeleitetes Management-System, welches die wichtigsten Aspekte eines Unternehmens-widerspiegelt. Das BSC-Konzept unterstützt strategische Planung und Implementierung durch eine Bündelung der Maßnahmen aller Einheiten eines Unternehmens auf der Basis eines gemeinsamen Verständnisses seiner Ziele und durch einen leichteren Zugang zur Bewertung und Fortschreibung der Strategie.“

Quelle: Blanced-Scorecard.de, http://www.balanced-scorecard.de/konzept.htm