DOKUMENTENTITEL	Quartalsbericht Risikomanagement 1. Quartal 2023
DOKUMENTENTYP	Bericht
DOKUMENTENVERANTWORTLICHER	Max Mustermann
VERTRAULICHKEITSKLASSE	Vertraulich
BEARBEITUNGSSTAND	Freigegeben
VERSION / GÜLTIG AB	v1 / 23.04.2023
VERTEILERKREIS	DIST und Geschäftsleitung

Inhaltsverzeichnis

1. Management-Summary

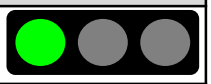
Dieser Bericht beschreibt den Status des Risikomanagements bestehend aus verschiedenen Teilen:

1. Business Impact Analyse (BIA) zur Bewertung der Folgen bei Ausfall von Geschäftsprozessen
2. Beschreibung des Umsetzungsstandes des Sollmaßnahmenkatalogs je Schutzziel
3. Schutzbedarfsanalyse zur Bewertung der Einhaltung von Schutzzielen
4. Status des Risikomanagements

Die nachfolgende Tabelle fasst alle Aktivitäten innerhalb des Berichtszeitraums mit Bezug zum Risikomanagement zusammen. Bei den Risiken gilt das Maximumprinzip, d.h. der Status des höchsten Risikos in einer Kategorie bestimmt den Status der gesamten Kategorie. Der detaillierte Status zu den jeweiligen Themen kann den entsprechenden Unterkapiteln entnommen werden. Die Ampelfarben haben folgende Bedeutung:

• Grün: Die Anforderungen sind zu mindestens 90% erfüllt oder es bestehen nur geringe Risiken.
• Gelb: Die Anforderungen sind zu mindestens 70% erfüllt oder es bestehen nur mittlere Risiken.
• Rot: Die Anforderungen sind zu weniger als 70% erfüllt oder es bestehen hohe Risiken.

Als Vorsorge für potentiell eintretende Risiken empfiehlt es sich, ein Risikokapital in angemessener Höhe als Rücklage zu bilden, siehe Seite 12.

Nr.	Themenbereich		Status
1	Business Impact Analyse (BIA)		
2a	Schutzbedarfsanalyse (Geschäftsprozesse)		
2b	Schutzbedarfsanalyse (Ressourcen)		
3a	Umsetzungsstand Sollmaßnahmenkatalog für Schutzziel	Normal	
3b	Umsetzungsstand Sollmaßnahmenkatalog für Schutzziel	Hoch	
3c	Umsetzungsstand Sollmaßnahmenkatalog für Schutzziel	Sehr hoch	
4a	Risiken der Kategorie	Technisch (IKT)	
4b	Risiken der Kategorie	Organisatorisch	
4c	Risiken der Kategorie	Projektmanagement	
4d	Risiken der Kategorie	Datenschutz	
4e	Risiken der Kategorie	Informationssicherheit	
4f	Risiken der Kategorie	Nachhaltigkeit	
4g	Risiken der Kategorie	Geschäftskontinuität	

2. Einleitung

Für den nachhaltigen wirtschaftlichen Erfolg unseres Unternehmens und das Erreichen unserer strategischen Ziele, ist ein erfolgreiches Management bestehender und neu auftretender Risiken entscheidend. Um Marktchancen nutzen und die hierin liegenden Erfolgspotenziale ausschöpfen zu können, müssen in angemessenem Umfang auch Risiken getragen werden. Daher bildet das Risikomanagement einen wesentlichen Bestandteil einer verantwortungsbewussten und guten Unternehmensführung.

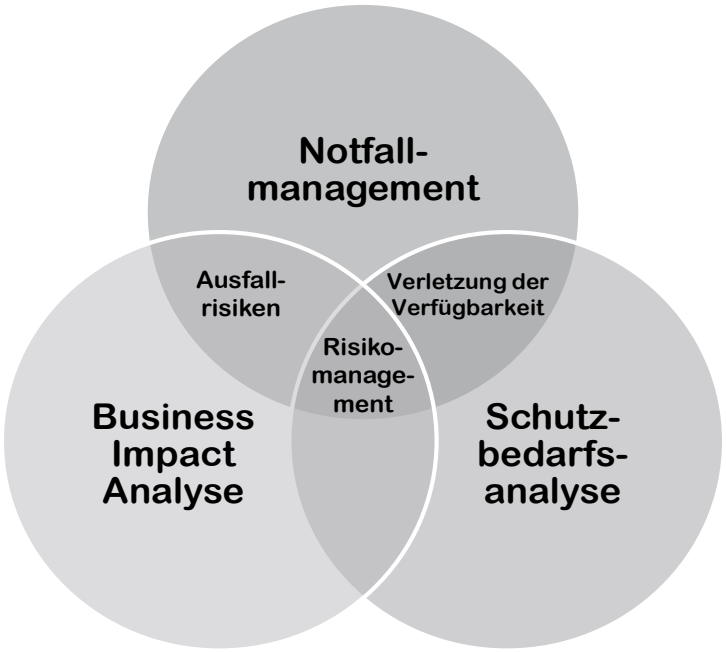
Dieser Bericht fasst die aktuelle Risikosituation des Unternehmens zusammen und besteht aus den folgenden Teilen:

• Business Impact Analyse (BIA)	zuletzt aktualisiert am:	12.04.2023
• Schutzbedarfsanalyse (SBA)	zuletzt aktualisiert am:	20.04.2023
• Umsetzungsstand des Sollmaßnahmenkatalogs	zuletzt aktualisiert am:	17.04.2023
• Status des Risikomanagement	zuletzt aktualisiert am:	17.04.2023
• Auszug Risikomatrix Notfallmanagement	zuletzt aktualisiert am:	17.04.2023

Die Business Impact Analyse betrachtet die möglichen Konsequenzen beim Ausfall von Geschäftsprozessen. Beim Notfallmanagement werden Maßnahmen beschrieben, um auf Ausfälle und Notfälle geeignet reagieren zu können. Die Schnittmenge beider Disziplinen ist die Behandlung von Ausfallrisiken.

Bei der Schutzbedarfsanalyse wird der Schutzbedarf von Geschäftsprozessen und IT-Ressourcen ermittelt hinsichtlich der VIVA-Schutzziele "Vertraulichkeit", "Integrität", "Verfügbarkeit" und "Authentizität". Die Verletzung des Schutzziels "Verfügbarkeit" hat daher eine Schnittmenge mit dem Notfallmanagement.

In allen Disziplinen werden Risiken identifiziert, die im Rahmen des Risikomanagements behandelt werden. Die nachfolgende Abbildung veranschaulicht das Zusammenspiel dieser 3 Disziplinen.



3. Business Impact Analyse

Die Business Impact Analyse (BIA) bewertet die Konsequenzen von ausfallenden Geschäftsprozessen. Je länger ein Geschäftsprozess ausfällt, desto spürbarer sind die Folgen. Als Konsequenzen wurden sowohl finanzielle, operationelle und juristische Folgen betrachtet, als auch potentielle Image-Schäden für das Unternehmen und die persönliche Unversehrtheit der Beschäftigten.

Als Ausfallzeiten wurden die Zeitintervalle "4 Stunden", "24 Stunden", "3 Tage" und 7 Tage" betrachtet. Das nachfolgende Diagramm zeigt das Ergebnis der BIA an. Bei Geschäftsprozessen, die eine längere Ausfallzeit nicht tolerieren, wurde das Risiko bewertet und mit geeigneten Maßnahmen in die Risikoliste aufgenommen.

Ergebnis der Business Impact Analyse

ID	Geschäftsprozess	4 h	24 h	3 d	7 d	Risikostrategie
P01	1.1 Überprüfung Benutzerrechte					Akzeptieren
P02	1.2 Benutzerunterstützung					Akzeptieren
P03	1.3 IT-Betrieb					Akzeptieren
P04	1.4 IT-Innovationsmanagement					Akzeptieren
P05	1.5 IT-Projekte					Akzeptieren
P06	2.1 Debitorenbuchhaltung					Akzeptieren
P07	2.2 Forderungsmanagement					Akzeptieren
P08	2.3 Kreditorenbuchhaltung					Akzeptieren
P09	2.4 Finanzmanagement					Akzeptieren
P10	2.5 Steuern und Abgaben					Akzeptieren
P11	3.1 Vertragsmanagement					Akzeptieren
P12	3.2 Beschaffungsmanagement					Akzeptieren
P13	3.3 Kundenvertragsmanagement					Akzeptieren
P14	4.1 Gehaltsabrechnung					Akzeptieren
P15	4.2 Recruiting					Akzeptieren
P16	4.3 Personal Lifecycle					Akzeptieren
P17	4.4 Abwesenheitsverwaltung					Akzeptieren
P18	4.5 Personalentwicklung					Akzeptieren
P19	5.1 Veröffentlichungen, Social Media					Akzeptieren
P20	5.2 Presse- und Öffentlichkeitsarbeit					Akzeptieren
P21	6.1 Strategie					Akzeptieren
P22	6.2 Projektmanagement					Akzeptieren
P23	6.3 UX Design					Akzeptieren
P24	6.4 UI Design					Akzeptieren
P25	6.5 Content Design					Akzeptieren
P26	6.6 Entwicklung					Akzeptieren
P27	6.7 Qualitätsmanagement					Akzeptieren
P28	6.8 Auslieferung					Akzeptieren
P29	6.9 Regelbetrieb PwC					Akzeptieren
P31	7.1 Governance					Akzeptieren
P32	7.2 Risikomanagement					Akzeptieren
P33	7.3 Compliance					Akzeptieren
P34	8.1 Schulung und Sensibilisierung					Akzeptieren
P35	8.2 Interner Audit					Akzeptieren
P36	8.3 Datenschutz-Folgenabschätzung					Akzeptieren
P37	8.4 Meldung von Datenschutzverletzungen					Akzeptieren
P38	8.5 Datenschutzauskunft					Akzeptieren
P39	8.6 Analyse Informationssicherheitsvorfälle					Akzeptieren
P40	8.7 Optimierung TOMs					Akzeptieren

Legende

Die Ausfallzeit ist tolerabel.

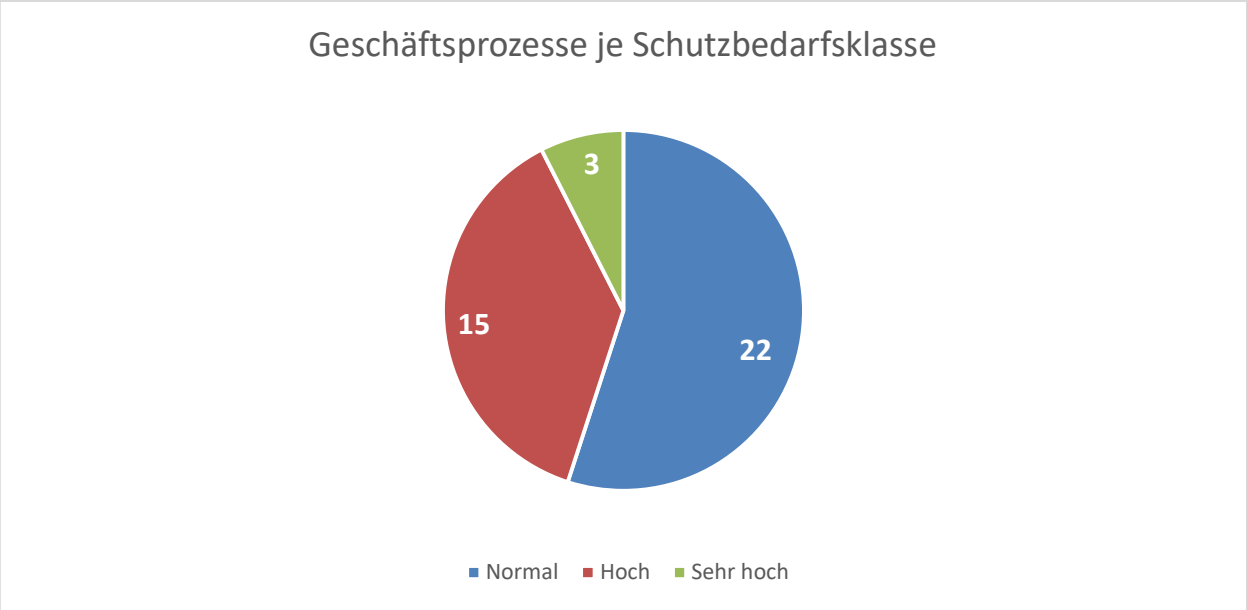
Die Ausfallzeit ist kritisch, mit Folgen für das Unternehmen.

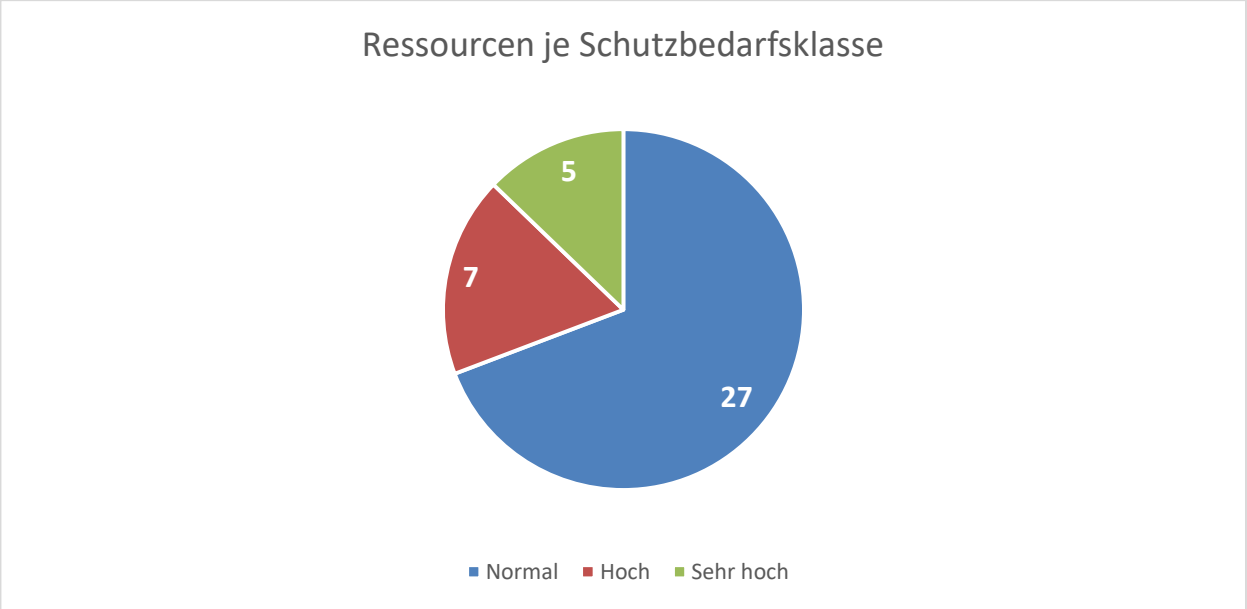
Quelle: Risiko-Tool → Reiter "BIA-Summary"

4. Schutzbedarfsanalyse

Die Schutzbedarfsanalyse (SBA) verfolgt mehrere Ziele:
- Bewertung der Geschäftsprozesse und dafür benötigte Ressourcen im Hinblick auf:
  - Schutzbedarf hinsichtlich Vertraulichkeit
  - Schutzbedarf hinsichtlich Integrität
  - Schutzbedarf hinsichtlich Verfügbarkeit
  - Schutzbedarf hinsichtlich Authentizität
- Ermittlung des für diese Schutzklasse gültigen Maßnahmenkatalogs
- Ermittlung ggf. zusätzlicher Security-Anforderungen aus den Fachbereichen
- Durchführung eines Soll-/Ist-Vergleichs (Gap-Analyse)
- Aufzeigen und Bewertung der Gaps in Form von Risiken
- Definition von geeigneten Maßnahmen für die Behandlung der Risiken

Im Rahmen der Schutzbedarfsanalyse haben sich die folgenden Zuordnungen von Ressourcen bzw. Geschäftsprozessen zu Schutzklassen ergeben.



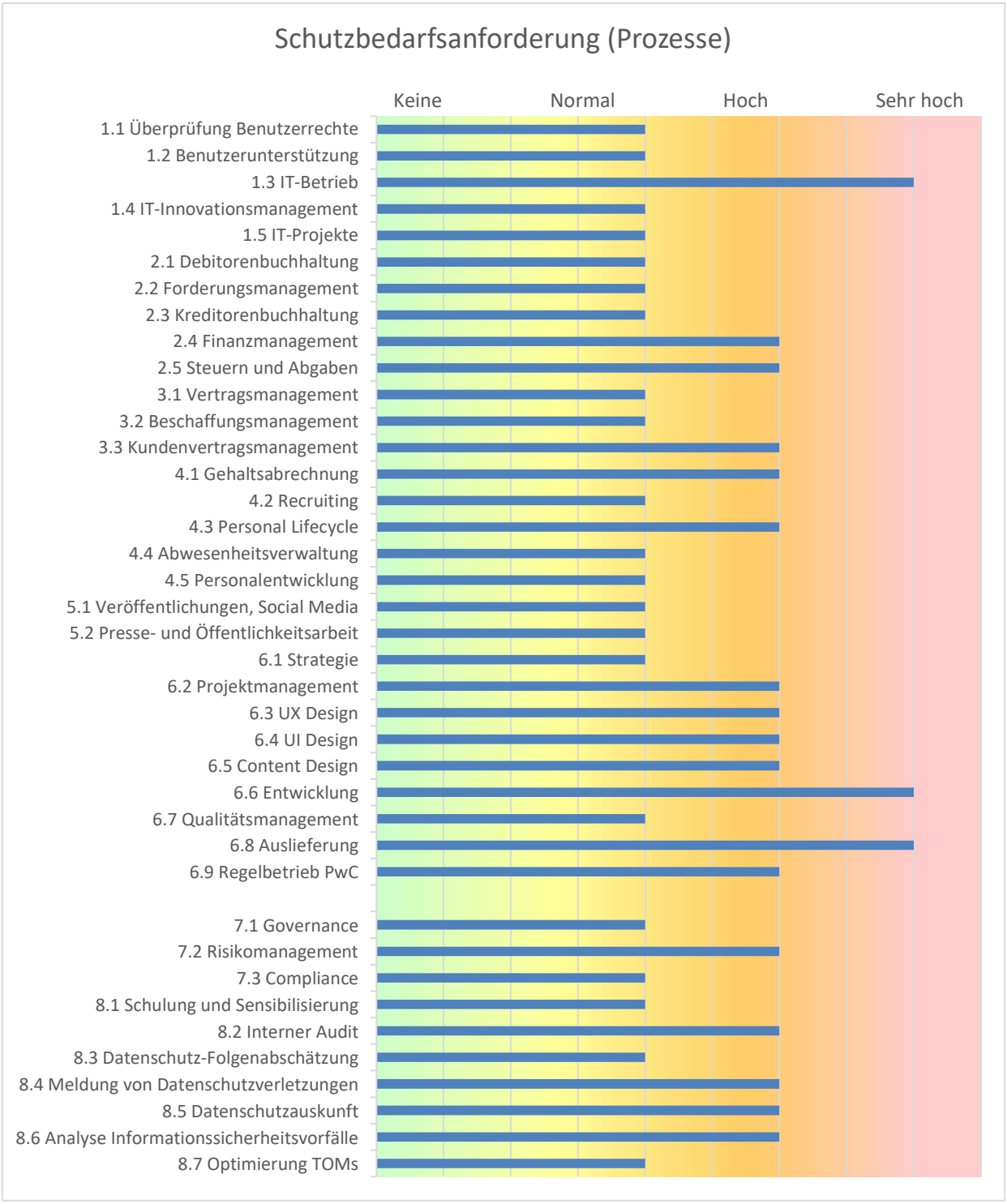


Quelle: Risiko-Tool → Reiter "SBA-Summary"

4.1 Schutzbedarf der Geschäftsprozesse

Die Ermittlung des Schutzbedarfs für die Geschäftsprozesse ergibt sich durch:
• Ermittlung der in dem Geschäftsprozess verarbeiteten Datenkategorien
• Ermittlung des Schutzbedarfs der verarbeiteten Daten
• Ermittlung des Schutzbedarfs für den Geschäftsprozess nach dem Maximumprinzip

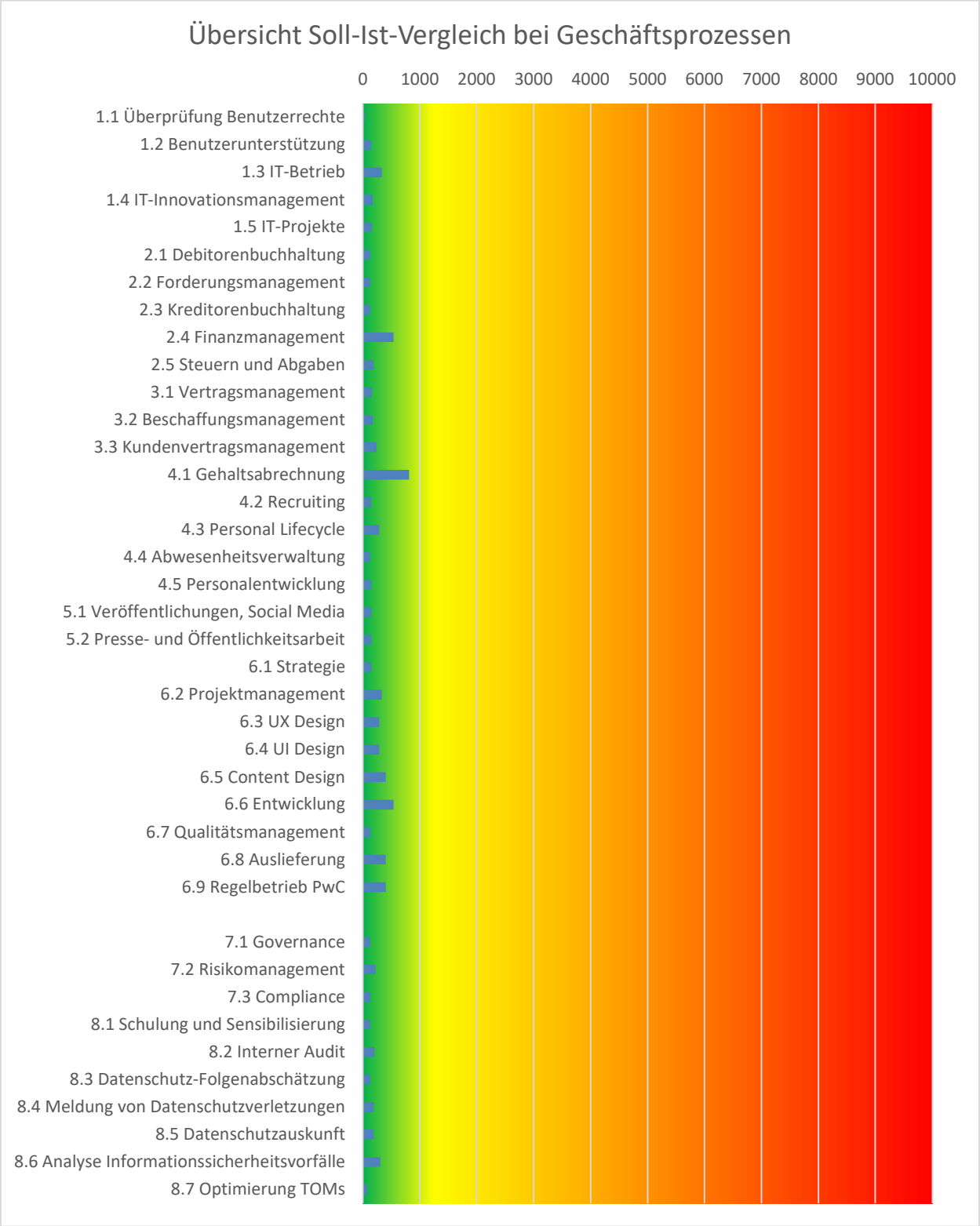
Die Vorgehensweise hat für die Geschäftsprozesse folgendes Ergebnis ergeben:



Quelle: Risiko-Tool → Reiter "Process-Summary"

4.2 Schutzbedarfsanalyse der Geschäftsprozesse

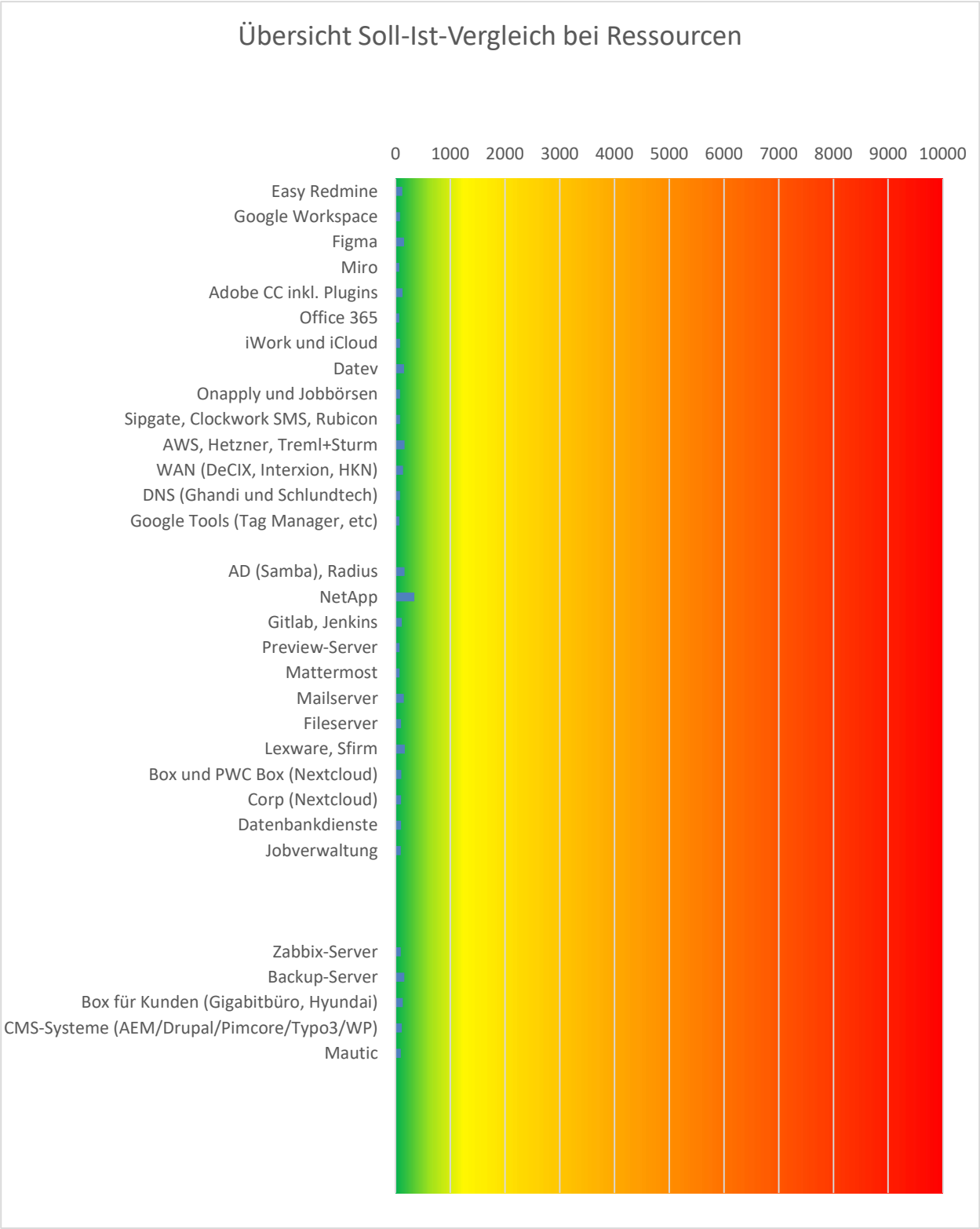
Die folgende Grafik veranschaulicht das Ergebnis der Schutzbedarfsanalyse für die Geschäftsprozesse. Ein Gap bis zum Schwellwert 1.000 wird als tolerierbar bzw. akzeptabel bewertet. Liegt der Wert darüber, wurde ein entsprechendes Risiko mit geeigneten Maßnahmen dokumentiert.



Quelle: Risiko-Tool → Reiter "SBA-Summary"

4.3 Schutzbedarfsanalyse der IT-Ressourcen

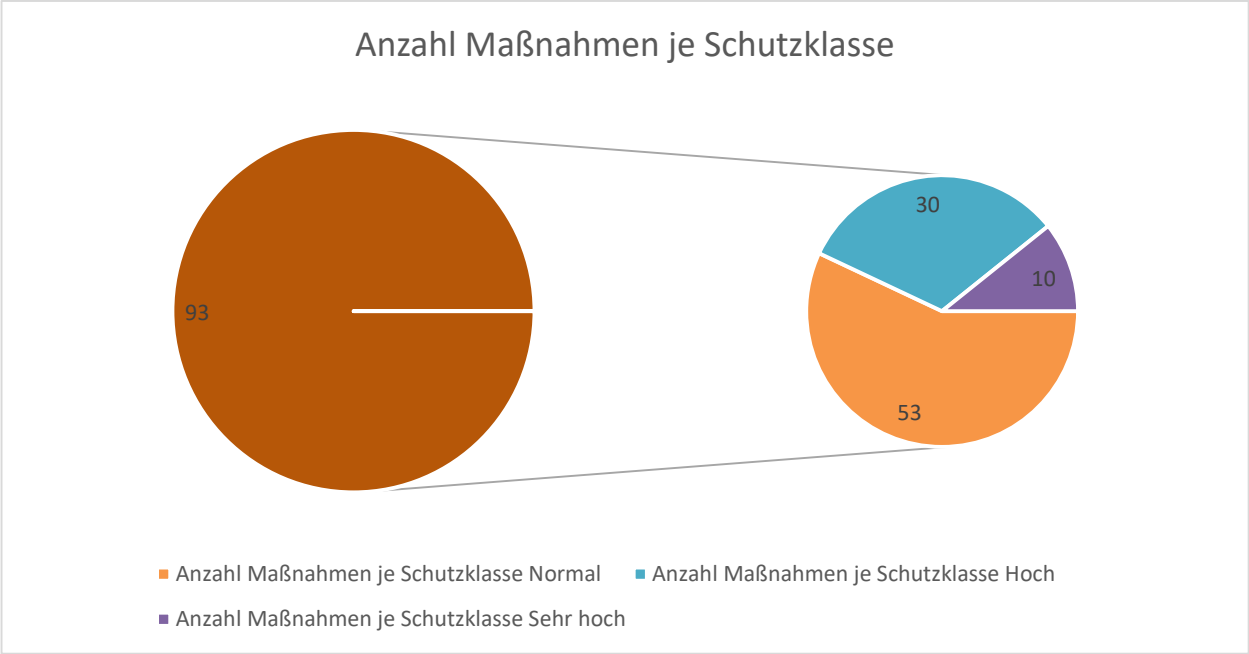
Die folgende Grafik veranschaulicht das Ergebnis der Schutzbedarfsanalyse für Ressourcen. Auch hier wird ein Gap bis zum Schwellwert 1.000 toleriert und akzeptiert. Liegt der Wert darüber, wurde ein entsprechendes Risko mit Maßnahmen dokumentiert.



Quelle: Risiko-Tool → Reiter "SBA-Summary"

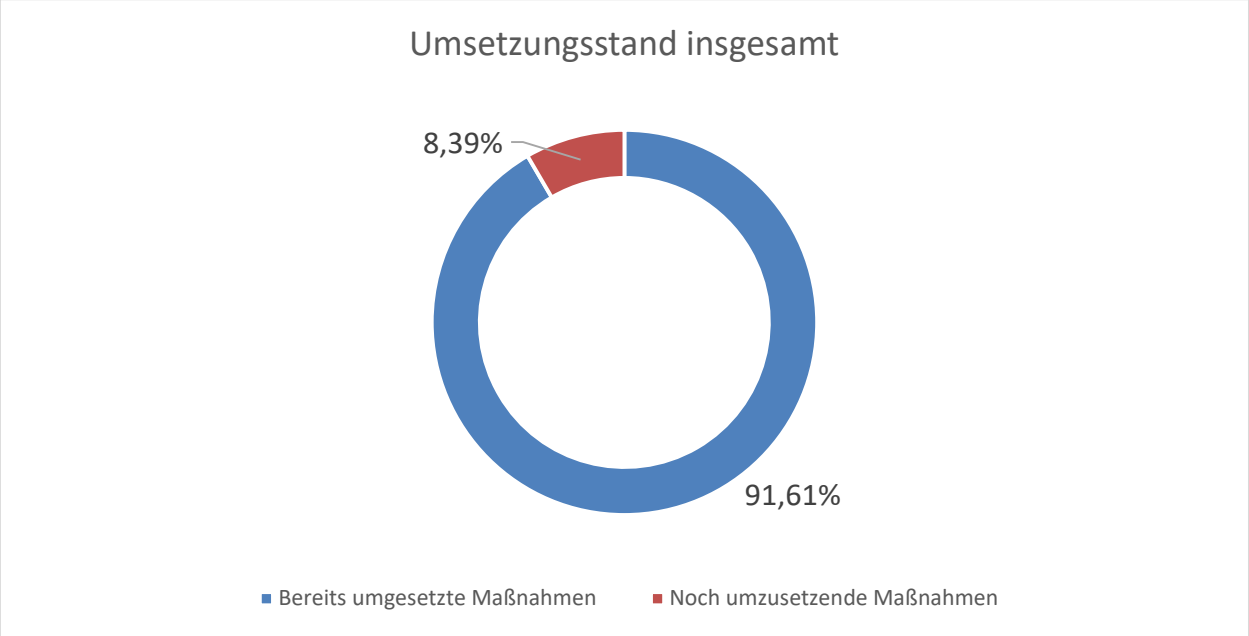
5. Umsetzungsstand Sollmaßnahmenkatalog

Um die gesetzten Schutzziele zu erreichen, wurde ein Sollmaßnahmenkatalog definiert. Dieser orientiert sich an den Best Practices der ISO 27002 und besteht aus 3 additiven Sets von Maßnahmen. Daten ohne Schutzbedarf werden intern den Maßnahmen der Schutzklasse "Normal" unterworfen. Der Inhalt der 3 Maßnahmenkataloge kann im Risikomanagement-Tool im Reiter "Measures" nachgelesen werden. Die Gesamtzahl an Maßnahmen sowie die Verteilung auf die jeweiligen Einzelkataloge wird durch die nachfolgende Grafik veranschaulicht.



Quelle: Risiko-Tool → Reiter "Measures"

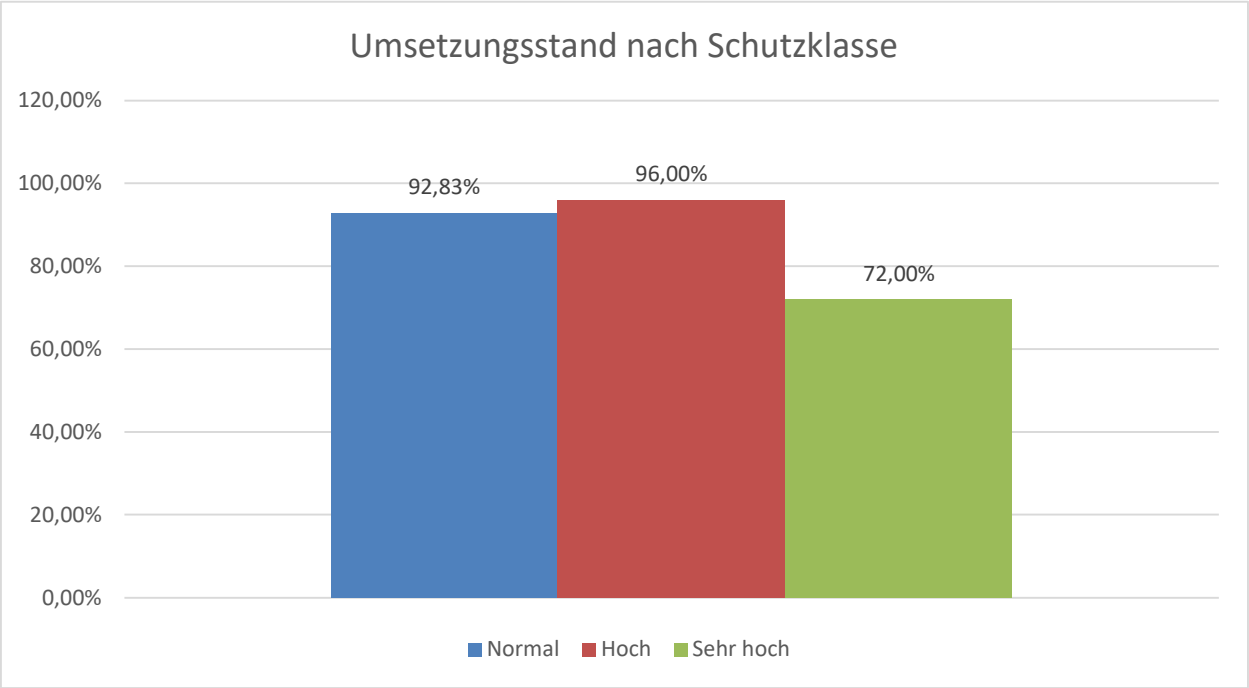
Den prozentualen Umsetzungsstand des Sollmaßnahmenkatalogs zeigt die nachfolgende Grafik:



Quelle: Risiko-Tool → Reiter "Measures"

An der Umsetzung des Sollmaßnahmenkatalogs wird kontinuierlich weitergearbeitet. Der Status wird nachfolgend aufgezeigt oder kann jederzeit beim Risikomanager erfragt werden.

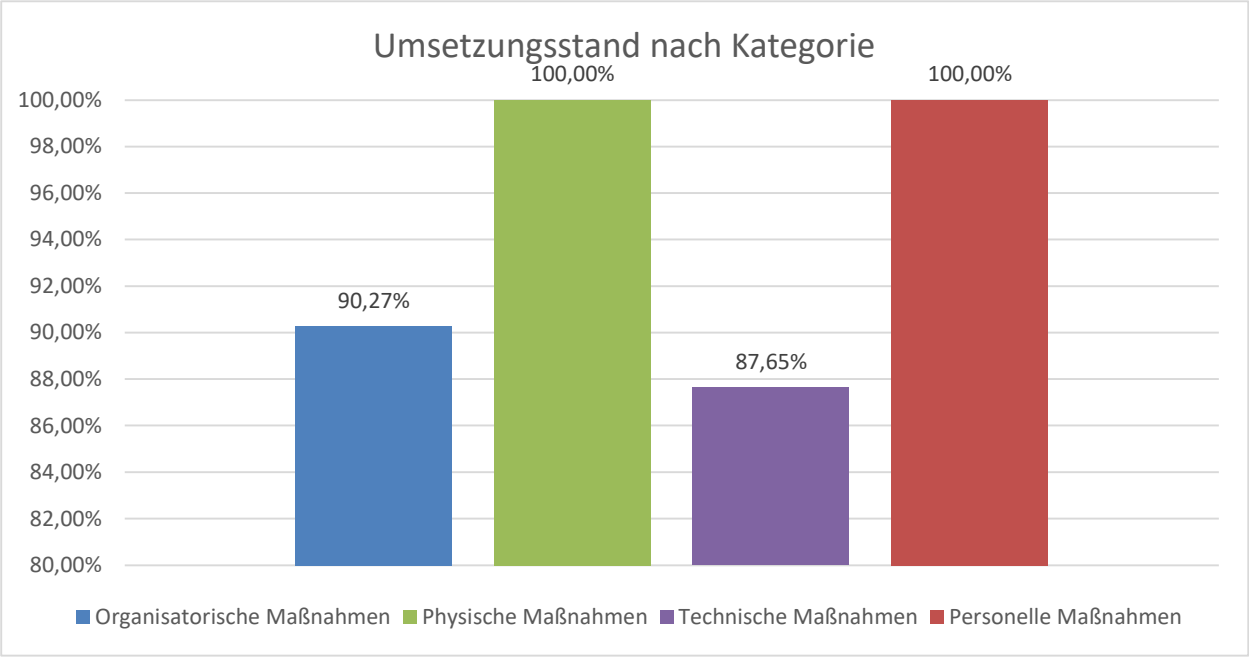
Der Umsetzungsstand je Schutzklasse wird durch die folgende Grafik veranschaulicht:



Quelle: Risiko-Tool → Reiter "Measures"

Der Sollmaßnahmenkatalog verteilt sich auf Maßnahmen in folgenden Themengebieten:
- 37 Organisatorische Maßnahmen
- 8 Personelle Maßnahmen
- 14 Physische Maßnahmen
- 34 Technische Maßnahmen

Der Umsetzungsstand je Themengebiet wird durch die folgende Grafik dargestellt:



Quelle: Risiko-Tool → Reiter "Measures"

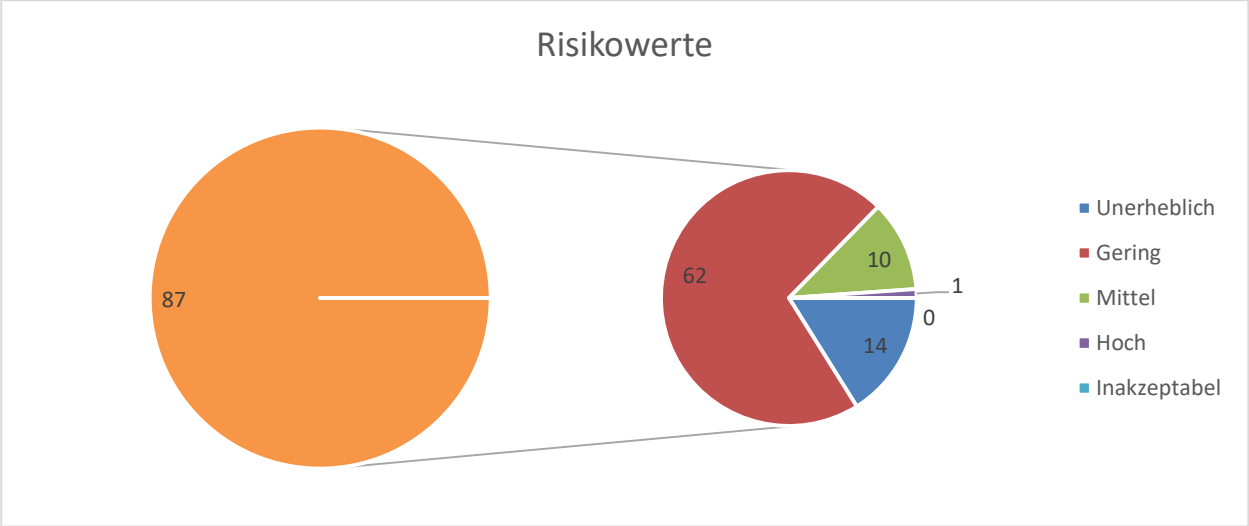
6. Risikomanagement

Das Risikomanagement verantwortet die Handhabung von Unternehmensrisiken durch deren Identifikation, Analyse, Bewertung und abschließende Risikobehandlung. Die Identifikation von Risiken erfolgt durch den Risikomanager in Zusammenarbeit mit den jeweiligen Risk Ownern. Risiken können sich aus den folgenden Bereichen ergeben:

- Mangelnde Vorkehrungen in Bezug auf den Datenschutz und die Informationssicherheit
- Optimierungsbedarf, der durch die jeweiligen Fachabteilungen gemeldet wird
- Feststellungen durch den Risikomanager oder durch Auditoren
- Bedrohungen durch Umwelteinflüsse oder gesellschaftliche Veränderungen
- Bedrohungen durch nicht beeinflussbare Ereignisse, z.B. Gesetzesänderungen, Gerichtsurteile, o.ä.

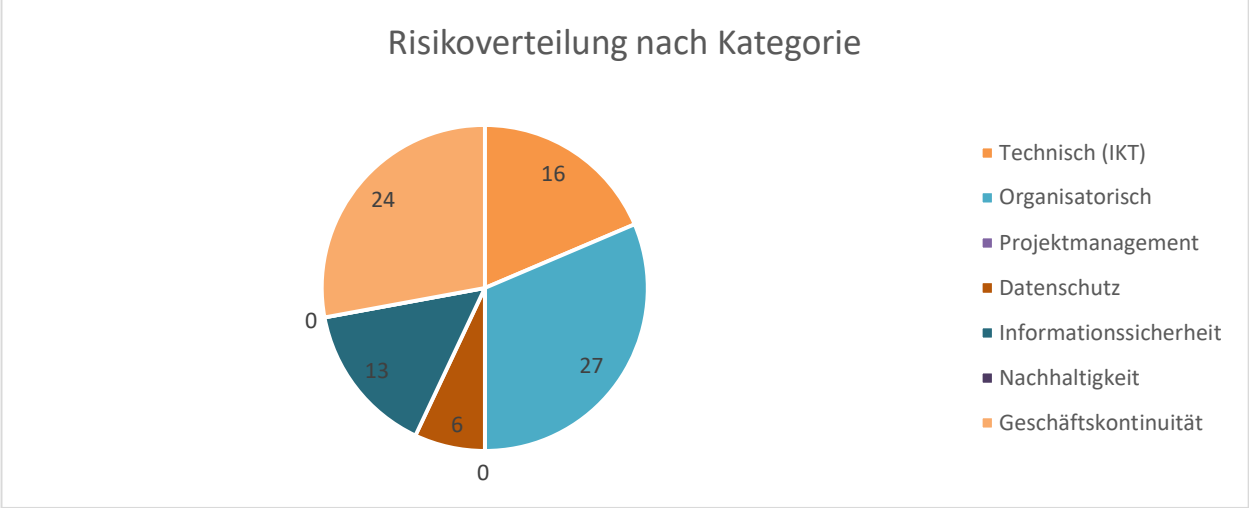
Alle Risiken werden in einer zentralen Risikomatrix verwaltet. Der Status sieht wie folgt aus:

6.1 Anzahl Risiken und Verteilung auf die jeweiligen Risikowerte



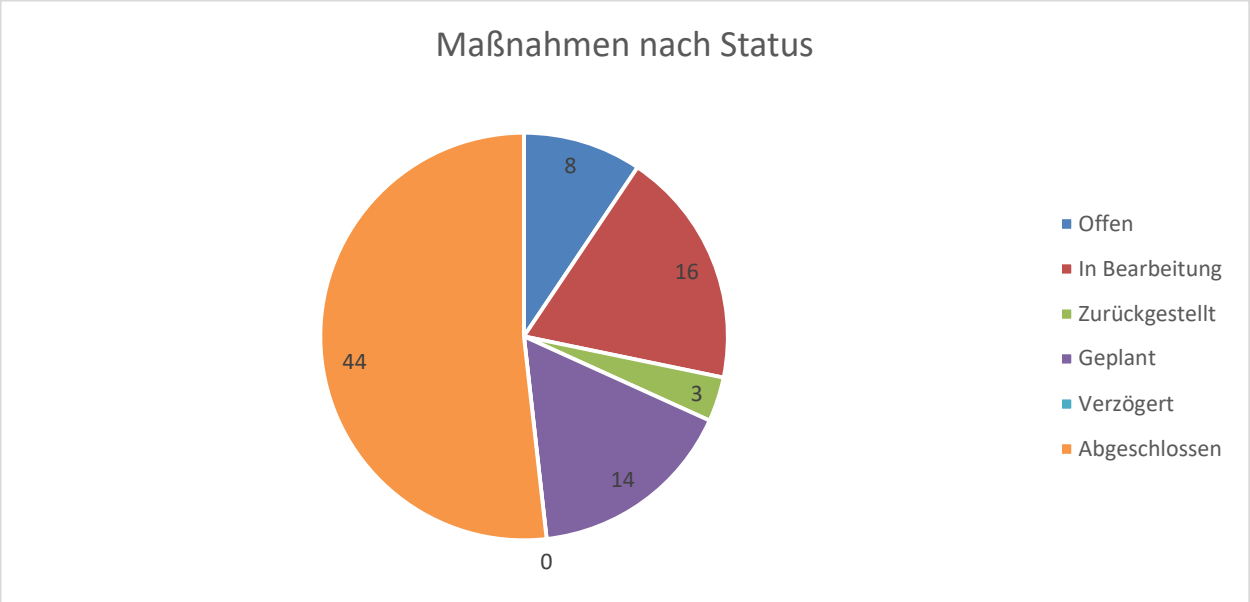
Quelle: Risiko-Tool → Reiter "Risk-Scoring"

6.2 Verteilung der Risiken auf die jeweiligen Risikokategorien



Quelle: Risiko-Tool → Reiter "Risk-Scoring"

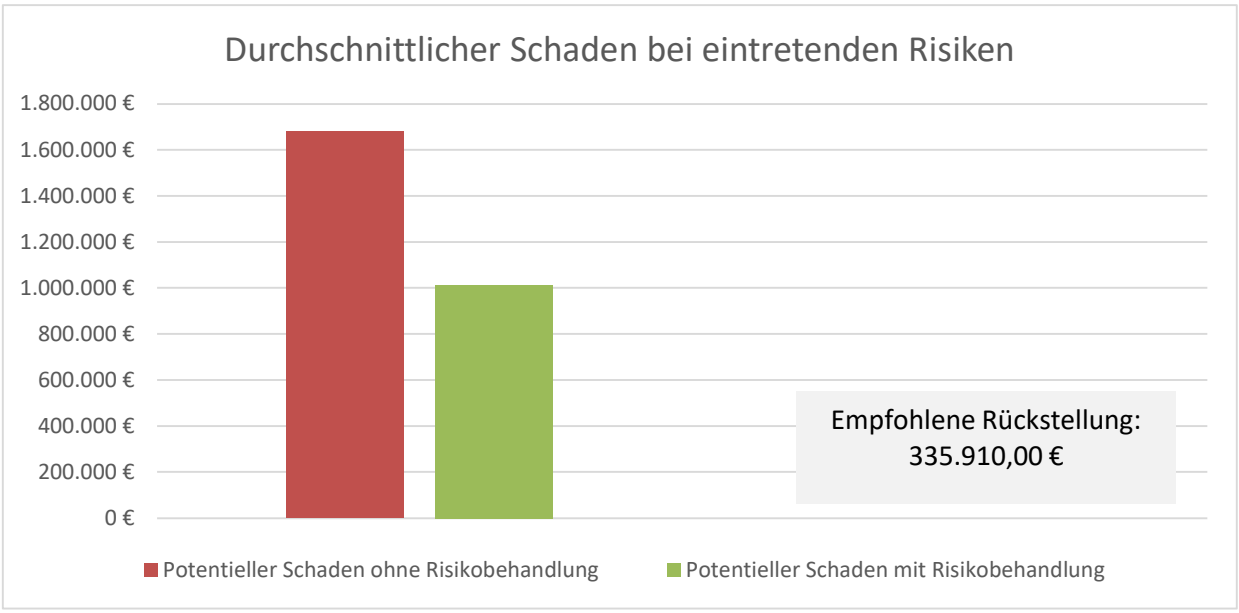
6.3 Anzahl der Maßnahmen zur Risikobehandlung und deren Status



Quelle: Risiko-Tool → Reiter "Risk-Scoring"

6.4 Durchschnittlich erwarteter Schaden bei eintretenden Risiken

Wird von den in Kapitel 2.3 genannten Schadensspannbreiten die Hälfte als Erwartungswert angenommen und multipliziert diesen mit der Eintrittswahrscheinlichkeit, dann ergibt sich eine erste qualifizierte Aussage zum potentiellen Schaden, wenn alle Risiken mit der angenommen Wahrscheinlichkeit eintreten. Durch die vorgesehenen Maßnahmen zur Behandlung von Risiken kann dieser Schaden begrenzt werden (2. Säule im Diagramm).

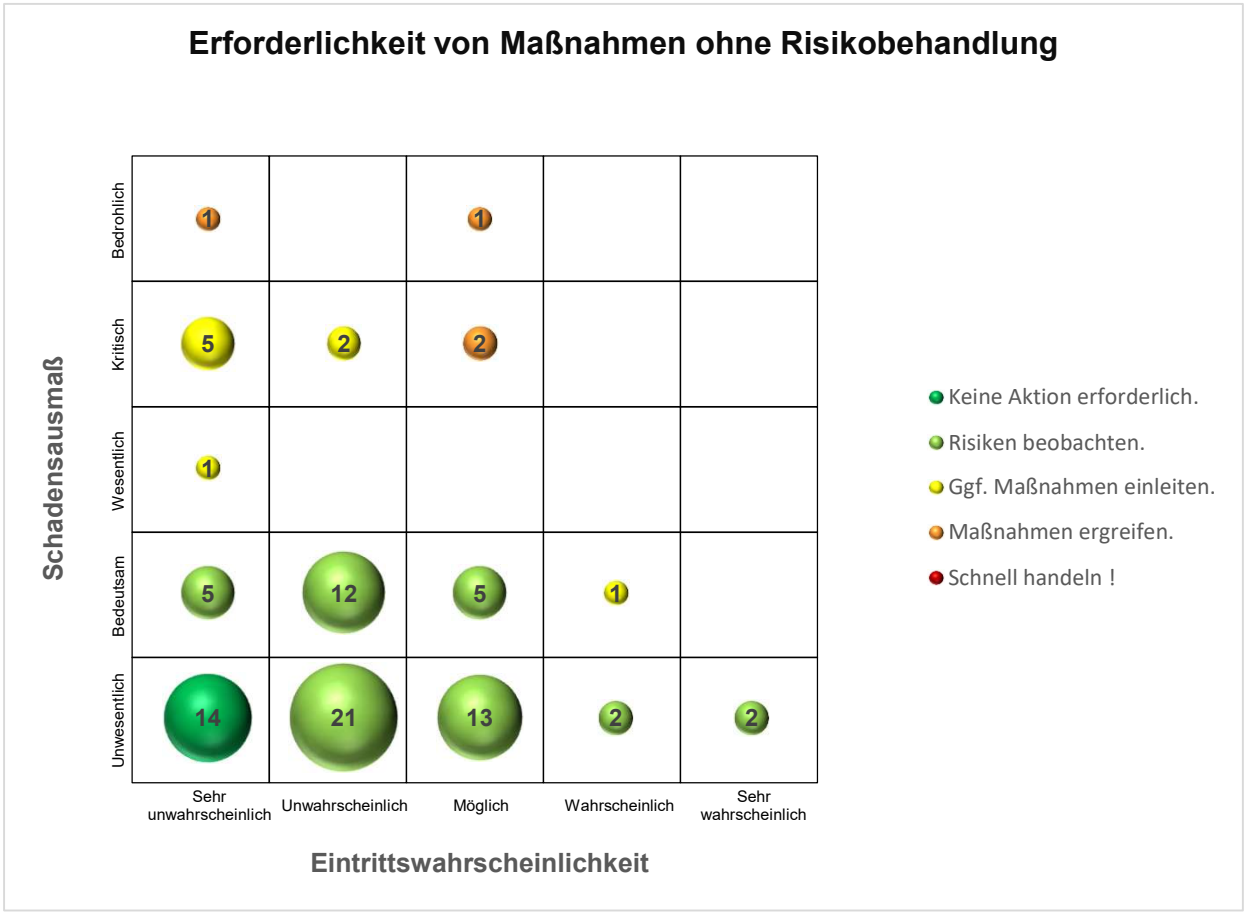


Quelle: Risiko-Tool → Reiter "Risk-Scoring"

Angelehnt an das oben dargestellte erwartete Schadensausmaß, würde es sich anbieten, ein Risikokapital in angemessener Höhe als Rückstellung zu bilden. Als angemessen kann ein Betrag von 20% (± 10%) der potentiellen Schadenssumme betrachtet werden.

6.5 Anzahl umzusetzender Maßnahmen

Für die in der Risikomatrix identifizierten Risikomaßnahmen ergibt sich eine Priorisierung bezüglich der Dringlichkeit bei der Umsetzung. Diese wird nachfolgend veranschaulicht.



Quelle: Risiko-Tool → Reiter "Risk-Summary"

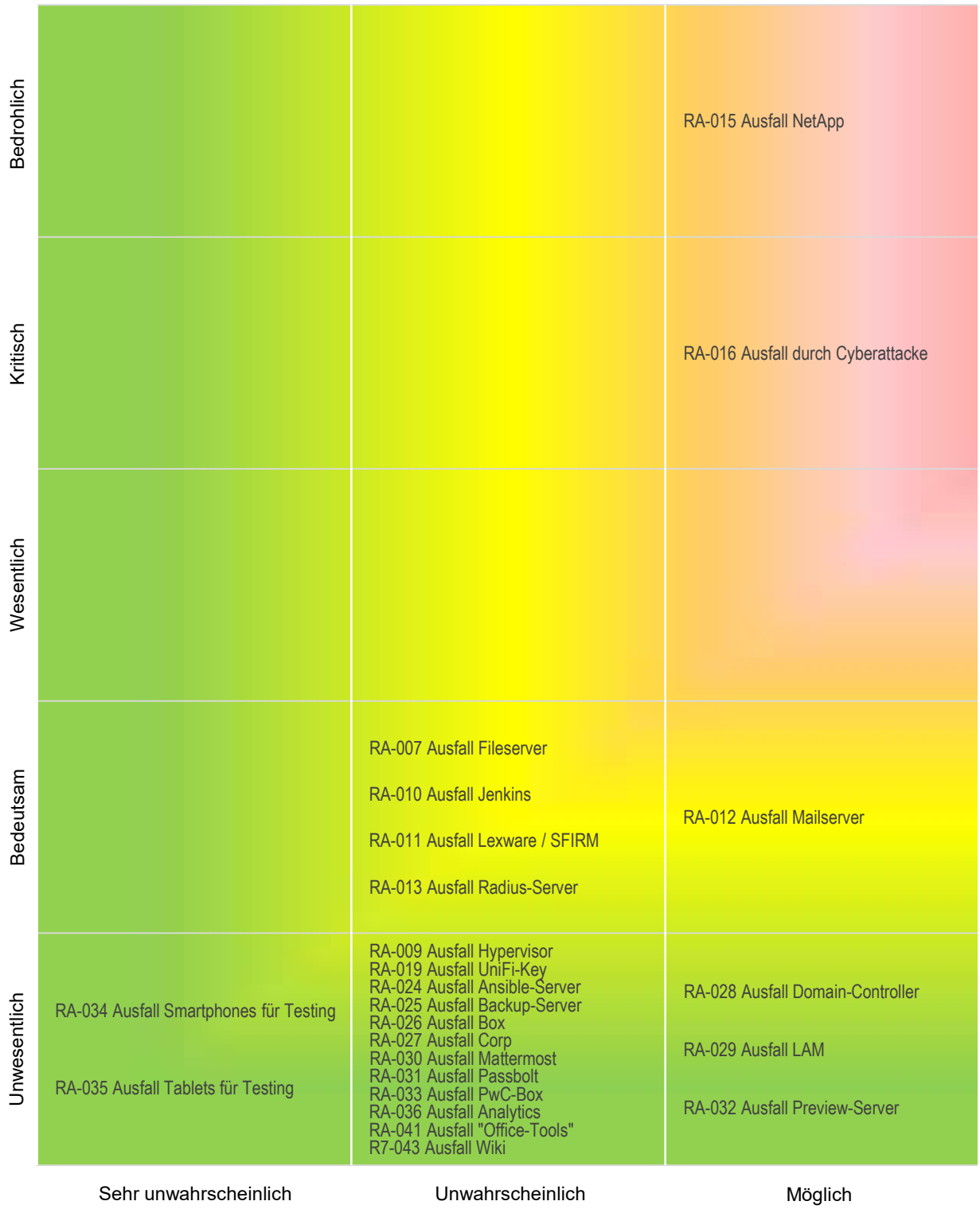
6.6 Übersicht der wesentlichen Risiken

Alle Risiken mit einem Risikowert größer als "gering" werden nachfolgend (inkl. der vorgeschlagenen Maßnahmen) aufgeführt.

Risiko	Geplante Maßnahme
R1-001 Unzureichende Kennwerte oder Logfiles	Monitoring-Kennwerte erweitern
R6-002 Figma-Nutzdaten nicht verfügbar	Daten aus dem Cloudservice sichern
RA-012 Ausfall Mailserver	Neubau des Mailservers per Docker
RA-014 Key-Beschäftigte fallen aus	Redundantes Knowhow schaffen
RA-015 Ausfall NetApp	Notfalltest "Ausfall NetApp" durchführen
RA-016 Ausfall durch Cyberattacke	Schulung und Recovery-Maßnahmen
RA-017 Kundenwegfall wegen fehlender ISO-Zertifizierung	Zertifizierung
R6-023 Ausfall von UI-Personal nicht kompensierbar	Keine Maßnahme vorgesehen
R2-045 Virenverseuchung durch infizierte Rechnung	Virenscan auf Mailserverebene
RA-069 Nachbesetzung IT-Koordinator verzögert sich	Recruiting eines Nachfolgers
R8-087 Folgekosten durch unzureichender ISV-Analyse	Gewissenhafte Analyse des Vorfalls

7. Notfallmanagement

Im Rahmen des Notfallmanagements wurden alle Ausfallszenarien als Risiken erfasst, der Kategorie "Geschäftskonituität" zugeordnet und - wo erforderlich - mit Maßnahmen belegt. Die nachfolgende Risikomatrix zeigt alle Risiken der Kategorie "Geschäftskontinuität". Außerdem wurden die Spalten "wahrscheinlich und "sehr wahrscheinlich" ausgeblendet, da es dort keine Einträge gibt.



8. Definitionen und Bewertungsmaßstäbe

In diesem Bericht wurden an etlichen Stellen Bewertungen durchgeführt. Diese erfolgten gemäß den nachfolgenden Definitionen und Bewertungsmaßstäben:

8.1 Schutzziele

Für die Bewertung der Datensicherheit werden die sog. VIVA-Schutzziele betrachtet, die sich an der ISO 27001 orientieren:

- **V**ertraulichkeit: Daten und Systeme dürfen nur berechtigten Personen zugänglich sein.
- **I**ntegrität: Daten dürfen nicht manipuliert werden oder worden sein.
- **V**erfügbarkeit: Daten und Systeme müssen zu definierten Zeiten abrufbar/nutzbar sein.
- **A**uthentizität: Die Quelle der Daten muss vertrauenswürdig und verifizierbar sein.

8.2 Schutzbedarfsklassen

Um den Schutzbedarf von Daten und Prozessen definieren zu können, wurden die folgenden Schutzbedarfsklassen definiert:

Nr.	Klasse	Beschreibung
1.	Keine	Öffentlich zugängliche Daten
2.	Normal	Die unbefugte Verwendung dieser Daten kann von der betroffenen Person leicht durch Aktivitäten verhindert oder abgestellt werden oder lässt keine besonderen oder akzeptablen Beeinträchtigungen erwarten.
3.	Hoch	Die unbefugte Verarbeitung solcher Daten kann zu Beeinträchtigungen der betroffenen Person in ihrer gesellschaftlichen Stellung oder ihren wirtschaftlichen Verhältnissen führen („Ansehen“). Bei sog. „Artikel 9“-Daten ist von einem hohen Schutzbedarf auszugehen.
4.	Sehr hoch	Die unbefugte Verarbeitung solcher Daten kann zu erheblichen Nachteilen für die betroffene Person hinsichtlich ihrer gesellschaftlichen Stellung und ihren wirtschaftlichen Verhältnissen führen („Existenz“).

8.3 Schadensausmaß (SA)

Sollten Geschäftsprozesse ausfallen, dann kann das verschiedene negative Auswirkungen auf die Kunden- und Lieferantenbeziehungen haben oder sich ungünstig auf das Business auswirken.
Im Rahmen der Business Impact Analyse wurden die folgenden Szenarien definiert, die sich als Folge von Prozessausfällen ergeben können:

Nr.	Art des Schadens	Schadensszenario
1.	Finanziell	Unmittelbare finanzielle Auswirkungen
2.	Operationell	Beeinträchtigungen der Aufgabenerfüllung
3.	Juristisch	Verstöße gegen Gesetze, Vorschriften oder Verträge
4.	Image	Negative Außenwirkung und Imageverlust
5.	Personell	Beeinträchtigungen der persönlichen Unversehrtheit

Während bei den finanziellen Auswirkungen die Kosten sofort spürbar sind (z.B. Kauf neuer Hardware nach Wasserschaden), stellen die anderen Kategorien eher indirekte Kosten dar.
Wenn die Aufgabenerfüllung nicht gewährleistet ist, weil beispielsweise Online-Shops nicht funktionieren, dann kann dies zu deutlichen Umsatzeinbrüchen führen.
Bei Verstößen gegen Gesetze, Vorschriften und Verträge kann sich im Nachgang ein Bußgeld oder eine Vertragsstrafe ergeben.
Kommen unerwünschte Fakten an die Öffentlichkeit, so kann dies zu einem Verlust des Ansehens führen, was in der Folge einen Auftragsrückgang bedeuten kann.
Bei der Beeinträchtigung der persönlichen Unversehrtheit sind negative Auswirkungen bei Personen gemeint, die körperlicher oder seelischer Art sein können sowie Verletzungen des Rechts auf informationelle Selbstbestimmung. Dies kann schlimmstenfalls zu Klagen mit anschließenden Schadensersatzzahlungen führen.
Am Ende lassen sich alle Schadensszenarien in Geld beziffern. Dazu wurden die folgenden Schadensklassen definiert. Die verwendeten Bezeichnungen finden sich später in der Risikomatrix wieder. Der Score-Wert wird für verschiedene interne Berechnungen benötigt und zusätzlich für die Verortung des Risikos in der Risikomatrix. Die Schadensklasse "Vernachlässigbar" ist eine Untermenge der Klasse "Unwesentlich", über die sog. "Bagatellschäden" abgebildet werden können.

Nr.	Bezeichnung	Schadensausmaß	Score SA	Bemerkung
1.	Unbeschadet	Kein finanzieller Impact	0	
2.	Vernachlässigbar	1 - 1.000 EUR	1	Bagatellschäden
3.	Unwesentlich	1 - 25.000 EUR	1	
4.	Bedeutsam	25.000 - 50.000 EUR	2	
5.	Wesentlich	50.000 - 100.000 EUR	3	
6.	Kritisch	100.000 - 500.000 EUR	4	
7.	Bedrohlich	> 500.000 EUR	5	

8.4 Eintrittswahrscheinlichkeit (EW)

Ein Schaden wird nur dann relevant, wenn er tatsächlich eintritt. Daher wurden die nachfolgenden Wertebereich für die Bestimmung der Eintrittswahrscheinlichkeit definiert.

Nr.	Bezeichnung	Wahrscheinlichkeit	Score EW	Bemerkung
1.	Ausgeschlossen	0 %	0	
2.	Sehr unwahrscheinlich	1 - 20 %	1	
3.	Unwahrscheinlich	20 - 40 %	2	
4.	Möglich	40 - 60 %	3	
5.	Wahrscheinlich	60 - 80 %	4	
6.	Sehr Wahrscheinlich	80 - 100 %	5	

Auch in diesem Fall wird der Score-Wert für interne Berechnungen sowie für die Verortung auf der Risikomatrix benötigt.

Für die Bewertung der Eintrittswahrscheinlichkeit gelten zusätzlich die folgenden Vorgaben:

- Ist ein Risiko in der Vergangenheit bereits mindestens ein Mal eingetreten, dann wird es mit „Möglich“ bewertet.
- Ist ein Risiko in der Vergangenheit bereits mehrmals eingetreten (3- bis 5-mal pro Jahr), dann wird es als “wahrscheinlich” bewertet.
- Ist ein Risiko in der Vergangenheit bereits mehr als 5 Mal pro Jahr eingetreten, dann wird es mit „Sehr wahrscheinlich“ bewertet.

8.5 Risikobewertung

Die Risikobewertung ergibt sich durch Verortung des Risikos in einer Risikomatrix. Hierbei werden die Eintrittswahrscheinlichkeit (Score EW) und das Schadensausmaß (Score SA) als Koordinaten verwendet. Der dazugehörige Risikowert ergibt sich aus dem Produkt dieser beiden Werte. Für diesen Bericht wurde die folgende Risikomatrix zugrunde gelegt.

Bedrohlich		**Beispiel-Risiko 1** Wahrscheinlichkeit = 1 Schadensausmaß = 5 Risikoscore = 1 x 5 = 5 Risikowert = gering				**Beispiel-Risiko 2** Wahrscheinlichkeit = 5 Schadensausmaß = 5 Risikoscore = 5 x 5 = 25 Risikowert = inakzeptabel
Kritisch						
Wesentlich				**Beispiel-Risiko 5** Wahrscheinlichkeit = 3 Schadensausmaß = 3 Risikoscore = 3 x 3 = 9 Risikowert = mittel		
Bedeutsam						
Unwesentlich		**Beispiel-Risiko 4** Wahrscheinlichkeit = 1 Schadensausmaß = 1 Risikoscore = 1 x 1 = 1 Risikowert = unerheblich				**Beispiel-Risiko 3** Wahrscheinlichkeit = 5 Schadensausmaß = 1 Risikoscore = 5 x 1 = 5 Risikowert = gering
Unbeschadet						
	Ausgeschlossen	Sehr unwahrscheinlich	Unwahrscheinlich	Möglich	Wahrscheinlich	Sehr wahrscheinlich

Die Risikowerte worden wie folgt definiert:

Bezeichnung	ich (EW*SA)
Kein Risiko	0 bis 0
Unerheblich	1 bis 1
Gering	2 bis 5
Mittel	6 bis 14
Hoch	15 bis 24
Inakzeptabel	25 bis 25

Risiken mit der Wahrscheinlichkeit "ausgeschlossen" oder dem Schadensausmaß "unbeschadet" werden zwar intern mitgeführt, allerdings in den grafischen Darstellungen nicht angezeigt.

Die Risikomatrix für das Notfallmanagement beschränkt sich auf die Darstellung von maximal "möglichen" Risiken, da die wahrscheinlichen und sehr wahrscheinlichen Risiken bereits adressiert wurden.

8.6 Verfügbarkeitsanforderungen

Für die Geschäftsprozesse wurde mit Hilfe der jeweiligen Risk Owner die Kritikalität ermittelt. Diese besteht aus den Verfügbarkeitsanforderungen für Daten und Systeme, sowie dem jeweiligen Schutzbedarf. Bei der Verfügbarkeit wird unterschieden zwischen den folgenden Wiederherstellungszeiten:

- bis zu 4 Stunden
- bis zu 8 Stunden
- bis zu 3 Tage
- bis zu 7 Tage

Alle Risk Owner wurden befragt, nach welcher Zeit Daten und Systeme wieder verfügbar sein müssen, z.B. nach einer größeren Störung oder einem Ausfall.

Um diese gewonnene Informationen besser verarbeiten zu können, wurden die oben genannten Zeitfenster definiert. Eine Ausfallzeit größer 7 Tage wird nicht betrachtet, da gemäß Notfallkonzept und Wiederanlaufplan die wichtigsten Kernprozesse innerhalb von 7 Tagen nach einem Totalausfall wiederhergestellt werden können.