

# Intervalid ISMS

Informationssicherheitsmanagement System  
Komplexe Themen erfordern einfache Lösungen

# Intervalid GmbH

Wir helfen Unternehmen, das Thema Informationssicherheit & Datenschutz erfolgreich umzusetzen.

- Seit 2017 am Markt
- Lösungen für Datenschutz- und Informationssicherheitsmanagement
- Über 300 Kunden



- Alle Branchen
- Unternehmen von KMU bis Konzerne
- Berater
- National & international im Einsatz
- ISMS stand alone oder mit Datenschutz

**Inhalt**

Europäisches Vorwort.....

Vorwort.....

0 Einleitung.....

1 Anwendungsbereich.....

2 Normative Verweisungen.....

3 Begriffe.....

4 Kontext der Organisation..... 6

4.1 Verstehen der Organisation und ihres Kontextes..... 6

4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien..... 6

4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems..... 7

4.4 Informationssicherheitsmanagementsystem..... 7

5 Führung..... 7

5.1 Führung und Verpflichtung..... 7

5.2 Politik..... 8

5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation..... 8

6 Planung..... 8

6.1 Maßnahmen zum Umgang mit Risiken und Chancen..... 8

6.2 Informationssicherheitsziele und Planung zu deren Erreichung..... 10

7 Unterstützung..... 11

7.1 Ressourcen..... 11

7.2 Kompetenz..... 11

7.3 Bewusstsein..... 11

7.4 Kommunikation..... 12

7.5 Dokumentierte Information..... 12

8 Betrieb..... 13

8.1 Betriebliche Planung und Steuerung..... 13

8.2 Informationssicherheitsrisikobeurteilung..... 13

8.3 Informationssicherheitsrisikobehandlung..... 14

9 Bewertung der Leistung..... 14

9.1 Überwachung, Messung, Analyse und Bewertung..... 14

9.2 Internes Audit..... 14

9.3 Managementbewertung..... 15

10 Verbesserung..... 16

10.1 Nichtkonformität und Korrekturmaßnahmen..... 16

10.2 Fortlaufende Verbesserung..... 16

Anhang A (normativ) Referenzmaßnahmensziele und -maßnahmen..... 17

Literaturhinweise..... 11

Was?

Muster für Richtlinien, Verfahren, Checkliste, etc.

User einbinden

Workflows

Wie?

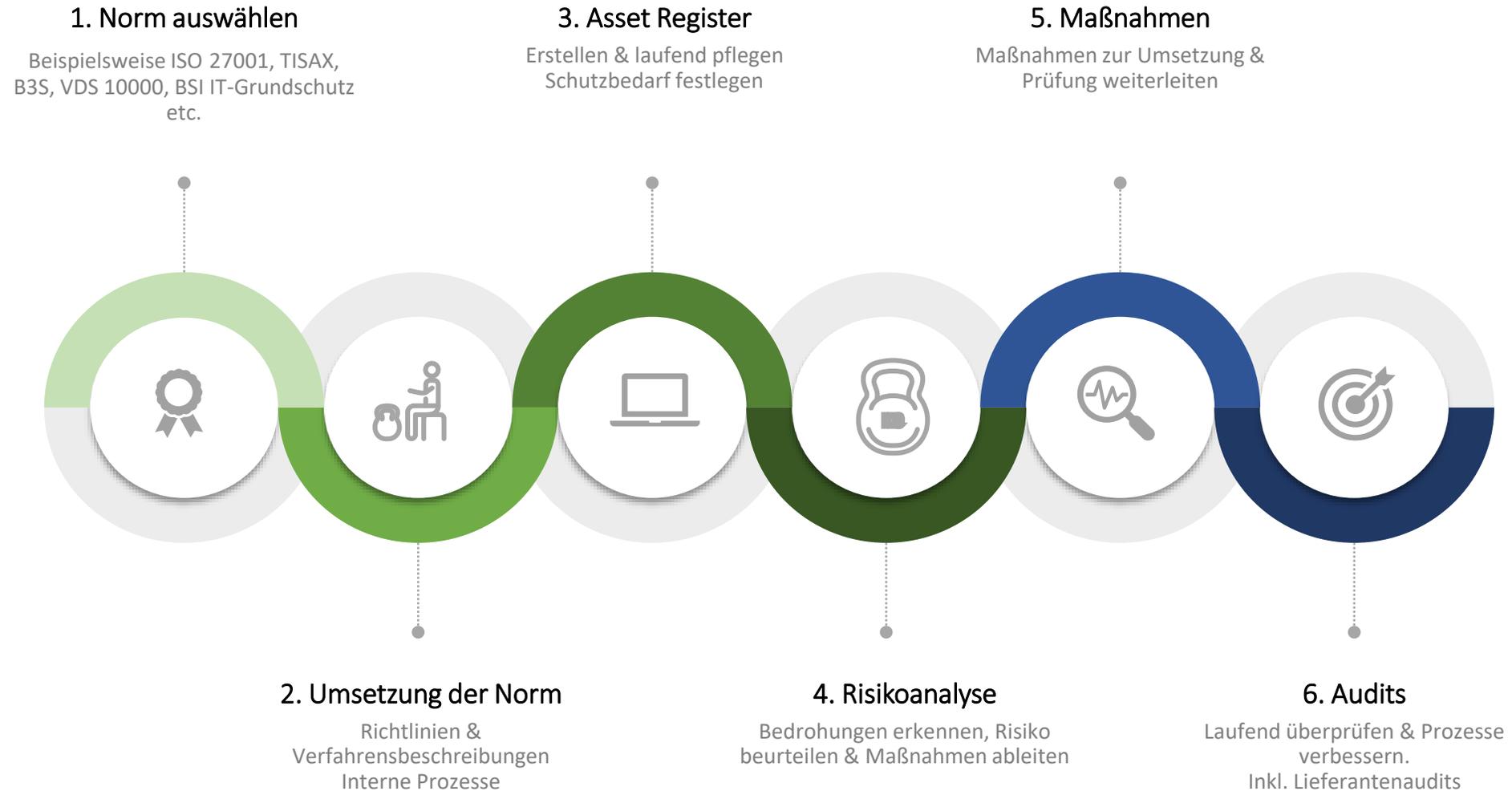
Best Practice Beispiele

Ablauf: der rote Faden

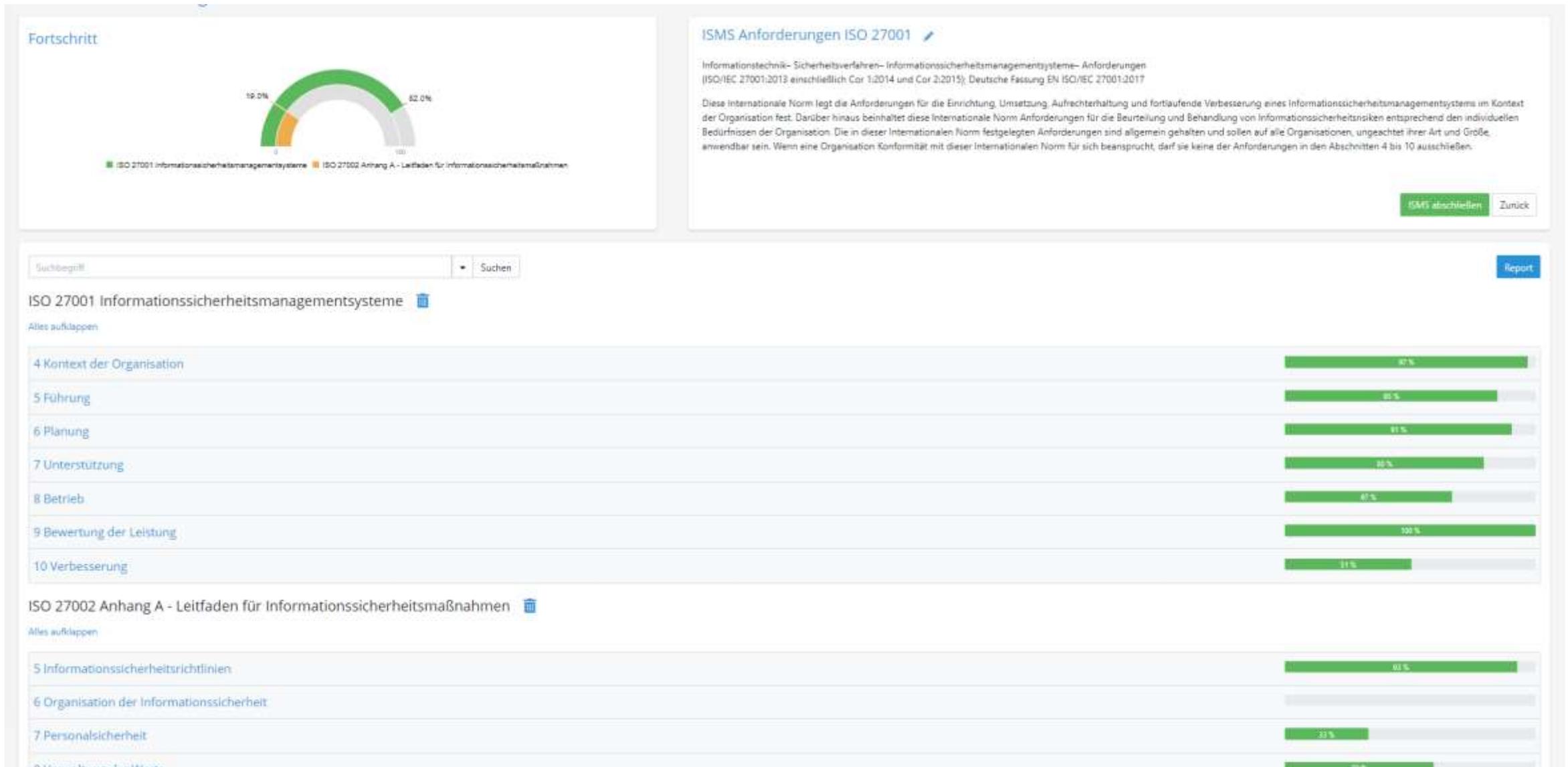


ISMS – Sie fangen nicht bei null an

# ISMS – Der rote Faden



# ISMS Schritt 1 – Die Umsetzung der Norm



# ISMS Schritt 1 – Die Umsetzung der Norm

**5 Führung** 91%

Unterstützung für ISMS durch Top-Management, durch Handlungen und Entscheidungen.  
Definierte Prinzipien und Strukturen für Management der Informationssicherheit.

5.1 Führung und Verpflichtung Verantwortlichen auswählen | Keine Aufgaben

5.2 Politik Christian Mittermeyer | 1 Aufgabe

Die oberste Leitung muss eine Informationssicherheitspolitik festlegen, die:

- a) für den Zweck der Organisation angemessen ist;
- b) Informationssicherheitsziele (siehe 6.2) beinhaltet oder den Rahmen zum Festlegen von Informationssicherheitszielen bietet;
- c) eine Verpflichtung zur Erfüllung zutreffender Anforderungen mit Bezug zur Informationssicherheit enthält; und
- d) eine Verpflichtung zur fortlaufenden Verbesserung des Informationssicherheitsmanagementsystems enthält.

Die Informationssicherheitspolitik muss:

- e) als dokumentierte Information verfügbar sein;
- f) innerhalb der Organisation bekanntgemacht werden; und
- g) für interessierte Parteien verfügbar sein, soweit angemessen.

**Pflichtdokument nach ISO 27001:**  
Leitlinie zur Informationssicherheit

Die Anforderungen in 5.2 beziehen sich auf die Leitlinie zur Informationssicherheit. Eine Leitlinie bezieht sich auf den Geschäftszweck der Organisation, gibt dafür grundlegende Sicherheitsziele vor und fordert die Einhaltung aller dazu notwendigen Vorgaben und Regelungen. Weiterhin soll die Verbesserung der Sicherheit allen Betroffenen als Verpflichtung auferlegt werden.

Aufgaben

Dokumente & Beschreibung

Umsetzung: 5.2 Politik

KOMMENTAR

Siehe Dokument "Informationssicherheitspolitik".  
Die Informationssicherheitsleitlinie ist festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.

Dokument hochladen - Welche Dokumente können hier hochgeladen werden?

Auswählen 📄 📁 📧

[Weiteres Dokument anlegen](#)

Kategorie	Dokumentname	Datum	Benutzer	Neue Version hochladen
Leitlinie	IS Informationssicherheitspolitik.docx	06.04.2022		<input type="text" value="Datei in das Feld ziehen"/> <span>Auswählen</span> <span>📄</span> <span>📁</span> <span>📧</span>

# ISMS Schritt 1 – Unternehmensdokumente

Unternehmensdokumente

Suchbegriff  Suchen

[Dokumente kopieren](#) [Dokument hochladen](#) [Dokument erstellen](#)

Unternehmen <i>if</i>	Kategorie <i>if</i>	Dokumentenname <i>if</i>	Dateityp <i>if</i>	Datum <i>if</i>	Status	Benutzer	
Holding	Allgemein	Überblick ISO 27001 Dokumente.pdf	PDF-Datei	09.12.2020	Hochgeladen		
Holding	Allgemein	A.17.02 Methodik der Geschäftsauswirkungsanalyse.docx	DOCX-Datei	03.08.2021	Hochgeladen	Benigna Prochaska	
Holding	Protokolle 2021	11.2 Protokoll zur Managementbewertung.docx	DOCX-Datei	11.05.2021	Freigegeben	Benigna Prochaska	
Holding	Richtlinien	05 Methodik zur Risikoeinschätzung und Risikobehandlung.docx		05.2021	Hochgeladen	Benigna Prochaska	
Holding	Richtlinien	A.6.2 Richtlinie zu Mobilgeräten und Telearbeit.docx		05.2021	Hochgeladen	Benigna Prochaska	
Holding	Richtlinien	A.8.2 IT Sicherheitspolitik.docx		05.2021	Hochgeladen	Benigna Prochaska	
Holding	Richtlinien	A.8.3 Richtlinie zur Klassifizierung von Informationen.docx			geladen	Benigna Prochaska	
Holding	Richtlinien	A.9.1 Zugangssteuerungsrichtlinie.docx			geladen	Benigna Prochaska	
Holding	Richtlinien	A.9.2 Kennwort Richtlinie.docx			geladen	Benigna Prochaska	
Holding	Richtlinien	A.10 Richtlinie des Einsatzes von Verschlüsselung.docx			geladen	Benigna Prochaska	
Holding	Richtlinien	A.11.1 Richtlinie zum aufgeräumten Arbeitsplatz leeren Bildschirm.docx			geladen	Benigna Prochaska	
Holding	Richtlinien	A.11.2 Richtlinie zur Entsorgung und Vernichtung.docx			geladen	Benigna Prochaska	
Holding	Richtlinien	A.12.2 Richtlinie zum Änderungsmanagement.docx			geladen	Benigna Prochaska	
Holding	Richtlinien	A.12.3 Backup Richtlinie.docx			geladen	Benigna Prochaska	
Holding	Richtlinien	A.13 Richtlinie zur Informationsübertragung.docx			geladen	Benigna Prochaska	
Holding	Richtlinien	A.14 Richtlinie zur Entwicklungssicherheit.docx			geladen	Benigna Prochaska	
Holding	Richtlinien	A.15.1 Sicherheitspolitik für Lieferanten.docx			geladen	Benigna Prochaska	

50 Vorlagen



Dokumenten Lenkung

# ISMS Schritt 2 – Das Asset Register

## Umsetzung

- Erfassen [Import] der Assets im Register
- Zentrale Assets für mehrere Unternehmen
- Owner festlegen
- Laufende Pflege
- Assets verknüpfen (Anwendungen mit Server, Server mit Raum, etc.)
- Schutzbedarf festlegen und vererben



Suchbegriff

Suchen



Asset hinzufügen

<input type="checkbox"/>	Nr.	Kategorie	Unternehmen	Abteilung	Titel	Merkmal	Fortschritt	Verantwortlicher Benutzer	Schutzbedarf			
<input type="checkbox"/>	GP 0001	Kategorie setzen	Holding	IT	Benutzerverwaltung	Interner Gebrauch	1-2-3	Andreas Bergmann	2 3 1 3			
<input type="checkbox"/>	GP 0003	Kategorie setzen	Holding	Personalabteilung	Bewerberverwaltung	Interner Gebrauch	1-2-3	Andreas Bergmann	3 1 2 2			
<input type="checkbox"/>	GP 0002	Kategorie setzen	Holding	Geschäftsführung	Datenschutzmanagement	Vertraulich	1-2-3	Andreas Bergmann	2 1 1 2			
<input type="checkbox"/>	GP 0004	Kategorie setzen	Holding	Finanz- und Rechnungswesen	Finanz- und Rechnungswesen	Vertraulich	1-2-3	Andreas Bergmann	3 2 2 3			
<input type="checkbox"/>	GP 0013	Leistungsprozess	Holding	Marketing	Kunden akquirieren	Merkmal setzen	1-2-3	Andreas Bergmann	1 2 1 2			
<input type="checkbox"/>	GP 0006	Leistungsprozess	Holding	Marketing	Kundenbetreuung (CRM)	Merkmal setzen	1-2-3	Andreas Bergmann	2 2 2 2			
<input type="checkbox"/>	GP 0007	Leistungsprozess	Holding	Marketing	Newsletter Versand an Kunden und Interessenten	Eingeschränkt	1-2-3	Andreas Bergmann	1 1 1 1			
<input type="checkbox"/>	GP 0008	Kategorie setzen	Holding	Personalabteilung	Personalabrechnung inkl. Abwesenheiten	Vertraulich	1-2-3	Andreas Bergmann	2 1 3 3			

Fortschritt

Owner

Schutzbedarf

### 1 Verlust der Integrität

#### Integrität

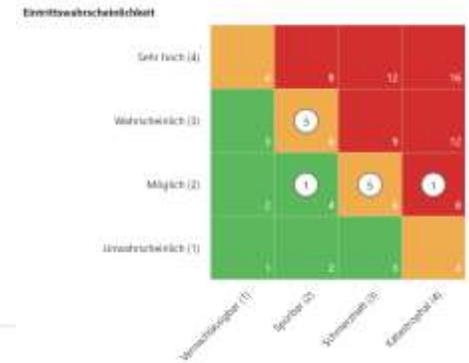
- 1 Die Schadensauswirkungen sind begrenzt und überschaubar.
- 2 Die Schadensauswirkungen können beträchtlich sein.
- 3 Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

# ISMS Schritt 3 – Risikoanalyse

## Umsetzung

- Bedrohungen & Schwachstellen identifizieren
- Schaden & Eintrittswahrscheinlichkeit bestimmen
- Risikobehandlung
- Maßnahmen setzen [Deadline, Verantwortliche, Kosten..]
- Regelmäßiger Review

# ISMS Schritt 3 – Die Risikoanalyse



## Geschäftsprozesse

Fortschritt setzen	Benutzerverwaltung	Analyse gestartet	Christian Mittermeyer	+
Fortschritt setzen	Bewerberverwaltung	Analyse in Arbeit	Christian Mittermeyer	+

### Bedrohung

Rechtmissbrauch

### Schwachstelle

Die Rechtevergabe ist im System nur auf Administratoren Rechte beschränkt.

### Risiko

2 2 4

### Neues Risiko

2 1 2

### Risikobehandlung

Reduktion: Rechte müssen eingeschränkt werden, eigene Rollen definiert.  
 Geplant bis: 30.10.2020  
 Verantwortlich: Christian Mittermeyer  
 Keine zusätzlichen Kosten

Bedrohung wählen

Schwachstelle

Risiko

Risikobehandlung

### ☰ Physischer Schaden

Konkrete Bedrohungen, die auftreten können und im Zusammenhang mit einer bestehenden Schwachstelle ein Risiko für das Unternehmen darstellen.

- Feuer
- Wasserschaden
- Umweltverschmutzung
- Schwerer Unfall
- Vernichtung von Ausrüstung oder Medien
- Staub, Korrosion, Gefrieren

# ISMS Schritt 4 – Maßnahmen

## Umsetzung

Maßnahmen aus:

- einer Risikoanalyse
- Bearbeitung eines Sicherheitsvorfalls
- einem internen oder externen Audit
- dem laufenden Betrieb

Zur Umsetzung und Prüfung weiterleiten,  
protokollieren, ISMS laufend verbessern



# ISMS Schritt 4 – Maßnahmenplan

## Aufgaben & Maßnahmen ⓘ

Alle anzeigen ☰ Aufgaben 📌 Maßnahmen

Suchbegriff  Suchen 🔍

[Maßnahmenplan](#) [Report](#) [Neu anlegen](#)

Art	Unternehmen	Beschreibung	Verknüpft mit:	Verantwortlich	Fällig bis	Priorität	Status	
Maßnahme	Holding	0030 - Webanwendung aktualisieren	Risikoanalyse HR Software	Benigna Prochaska	28.06.2021 !	niedrig	Erfasst In Umsetzung durch Benigna Prochaska	
Maßnahme	Holding	0033 - Externen Arbeitskräfte	Risikoanalyse Personalabrechnung inkl. Abwesenheiten	Benigna Prochaska	30.06.2021 !	niedrig	Erfasst	
Maßnahme	Holding	0058 - Verschlüsselung der Laptops		Benigna Prochaska	31.07.2021 !	niedrig	Erfasst Bei der Freigabe durch Benigna Prochaska	
Maßnahme	Holding	0039 - Maßnahme Wasserschäden	Risikoanalyse Serverraum		30.08.2021 !	niedrig	Erfasst In Umsetzung durch Benigna Prochaska	
Maßnahme	Holding	0161 - Penetration Test durchführen	Sicherheitsvorfall Cyber Angriff		31.10.2021	mittel	Erfasst	
Maßnahme	Holding	0086 - System absichern		Benigna Prochaska	31.10.2021	mittel	Erfasst	
Maßnahme	Holding	0162 - Trainingskurse umsetzen für den Bereich Vertrieb	Audit Unterstützung [7]	Andreas Krüger	31.10.2021	niedrig	Erfasst Bei der Freigabe durch Benigna Prochaska	

Aus  
Audit, Sicherheitsvorfall,  
Risikoanalyse, etc.

Zur Umsetzung &  
Überprüfung weiterleiten

# ISMS Schritt 5 – Audit

## Umsetzung

- Audit planen
- Audit durchführen & Schwachstellen identifizieren
- Offene Punkte abarbeiten
- Maßnahmen setzen, verteilen, überwachen
- Management Report
- Interne, externe Audit & Lieferantenaudits

# ISMS Schritt 5 – Audit Checkliste

## Allgemeine Checkliste: Holding

75%

- 1 Kontext der Organisation [4] ✓
- 2 Führung [5] ✓
- 3 Planung [6] ●
- 4 Unterstützung [7] ●
- 5 Betrieb [8]
- 6 Bewertung der Leistung [9]
- 7 Verbesserung [10]
- ✓ Checkliste abschließen

### Unterstützung [7]

Werden für alle Elemente des ISMS angemessene Ressourcen bereitgestellt? (7.1)

Sind die notwendigen Kompetenzen definiert, die Trainingskurse durchgeführt, und werden Aufzeichnungen über die Kompetenzen geführt? (7.2)

- Nein geplant für Q4

Dokumentenname	Datum	Benutzer
09_Plan_fuer_Training_und_Awareness_Premium_DE...	04.10.2022	Benigna Prochaska

Ist das Personal sich bewusst über die Informationssicherheitspolitik, deren jeweilige Rollen im Rahmen derselben, sowie der Konsequenzen bei Nichteinhaltung der Vorschriften? (7.3)

- Ja

- BP Zur **Bearbeitung weitergeleitet** von Andreas Bergmann an Benigna Prochaska
- BP Zur **Bearbeitung weitergeleitet** von Andreas Bergmann an Benigna Prochaska
- AB Zur **Bearbeitung weitergeleitet** von Benigna Prochaska an Andreas Bergmann

# ISMS Schritt 5 – Audit Ergebnis

Ergebnisse im Detail anzeigen

Zurück

FILTER:

KONFORM RISIKO HOHES RISIKO NICHT BEURTEILBAR

Suchbegriff  Suchen

Risiko	Abschnitt	Frage	Antwort	Aufgaben & Maßnahmen
<b>Internes Audit ISO 27001 - Holding</b>				
	Führung [5]	Sind Rollen und Verantwortlichkeiten für die Informationssicherheit vergeben und kommuniziert? (5.3)	- Nein Rollen und Verantwortlichkeiten für die Informationssicherheit sind definiert und werden im Q4 kommuniziert	1 Maßnahme
	Planung [6]	Wurde die Erklärung zur Anwendbarkeit einschließlich der Rechtfertigungen und dem Status für jede Maßnahme erstellt? (6.1.3)	- Nein In Arbeit	Keine Aufgaben
	Unterstützung [7]	Sind die notwendigen Kompetenzen definiert, die Trainingskurse durchgeführt, und werden Aufzeichnungen über die Kompetenzen geführt? (7.2)	- Nein geplant für Q4	Keine Aufgaben
	Unterstützung [7]	Existiert ein Verfahren für Kommunikation im Zusammenhang mit Informationssicherheit, einschließlich der Verantwortlichkeiten und Einzelheiten darüber, was zu kommunizieren ist? (7.4)	- Nein	Keine Aufgaben

**Audit**  
Internes Audit ISO 27001  
Internes Audit SMS Umsetzung auf Basis ISO 27001  
Beginn: 07.09.2022

**Verweis:** ISO 27001 und ISO 27002  
**Auditor:** Friedrich Mayerhofer (Auditor), Jorg Hader (Co-Auditor)  
**Weitere Informationen:** Einzelinterviews, Stichproben

**Ergebnisse**  
Gesamtwertung:

**Prüfung Zusammenfassung**

18	13	1	1	8
Frage	Beantwortet	Warte	Hohes Risiko	Nicht beurteilt

[Erstelle Report](#)

Aufgaben & Maßnahmen setzen

# ISMS Schritt 5 – Lieferantenaudit

Lieferantenaudit

Suchbegriff  Suchen

Aktion wählen

<input type="checkbox"/>	Unternehmen	Art	Name	Freigegeben	Klassifizierung	Letzter Start	Status	Offen	Nächstes Audit
<input type="checkbox"/>	Alle Unternehmen	Auftragsverarbeiter	Auftragsverarbeiter	Freigegeben	Hohes Risiko	19.09.2022	Fragebogen ausfüllen	1 offen von 1	01.01.2024
<input type="checkbox"/>	Holding	Auftragsverarbeiter	Intervalid GmbH	Freigegeben	Klassifizierung setzen				tt.mm.jjjj
<input type="checkbox"/>	Alle Unternehmen	Auftragsverarbeiter	Microsoft	Freigegeben	Mittleres Risiko				tt.mm.jjjj
<input type="checkbox"/>	Alle Unternehmen	IT Dienstleister	Rechenzentrum	Freigegeben	Mittleres Risiko				tt.mm.jjjj
<input type="checkbox"/>	Alle Unternehmen	IT Dienstleister	Softwareanbieter GmbH	Freigegeben	Geringes Risiko				tt.mm.jjjj

Ihre  
Geschäftspartner

Freigabe &  
Klassifizierung

Fragebögen  
versenden

# ISMS – Was Sie noch tun können

## Weitere Funktionen

- Sicherheitsvorfälle erfassen, bearbeiten, weiterleiten
- Reports erstellen
- Dashboard & Grafiken
- Notfallplanung (BCM)



**WIR BERATEN SIE GERNE**  
**Halle 7 – Standnummer: 7-216**  
**(Advantage Austria)**



## Intervalid ISMS



**BENIGNA PROCHASKA**

**Geschäftsführerin | Intervalid GmbH**

Tel: +43 1 905 10 44 11

E-Mail: [benigna.prochaska@intervalid.at](mailto:benigna.prochaska@intervalid.at)

## Intervalid DSMS



**CORINNA SALLMUTTER**

**Marketing & Sales | Intervalid GmbH**

Tel: +43 1 905 10 44 12

E-Mail: [corinna.sallmutter@intervalid.at](mailto:corinna.sallmutter@intervalid.at)