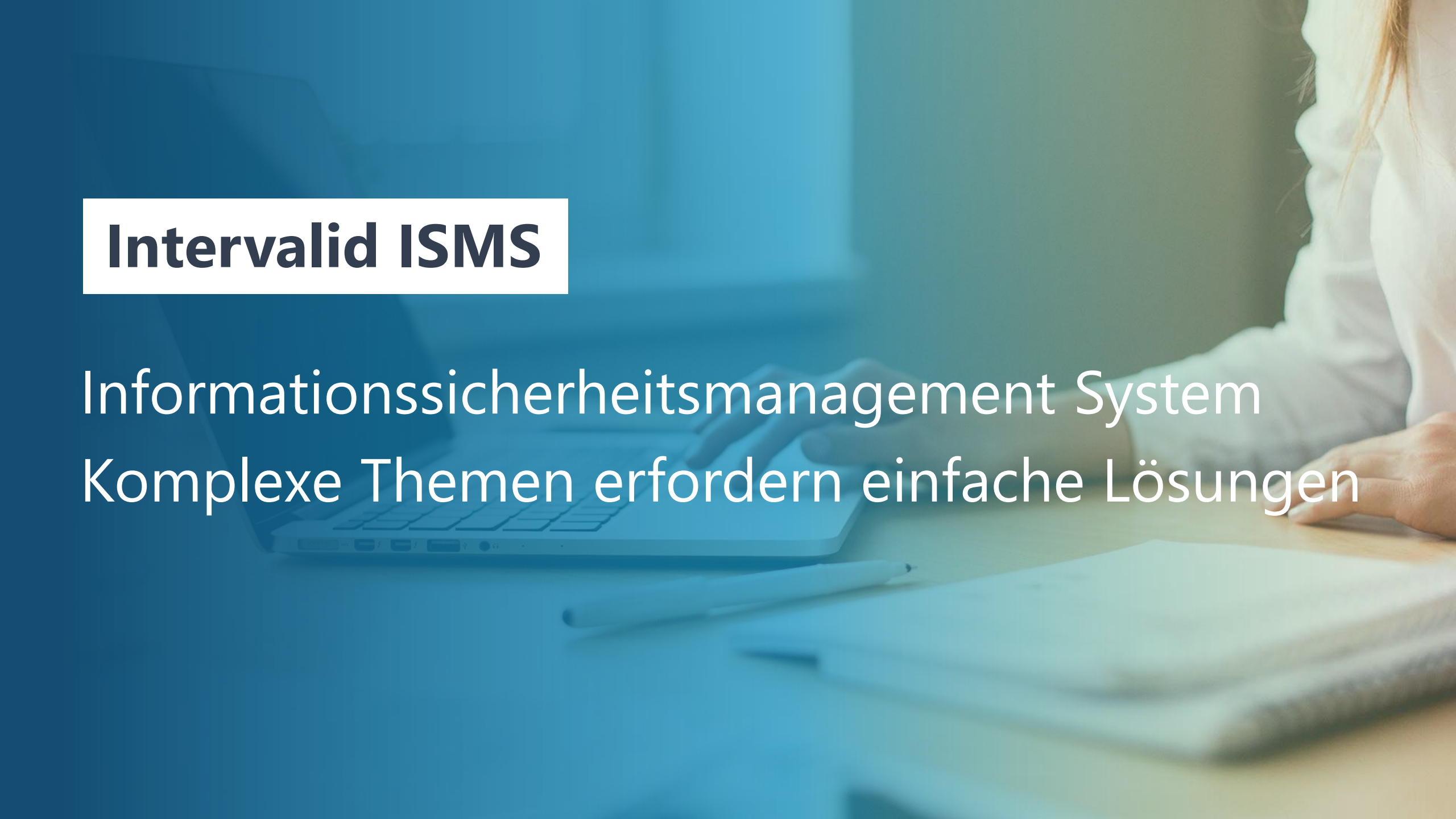


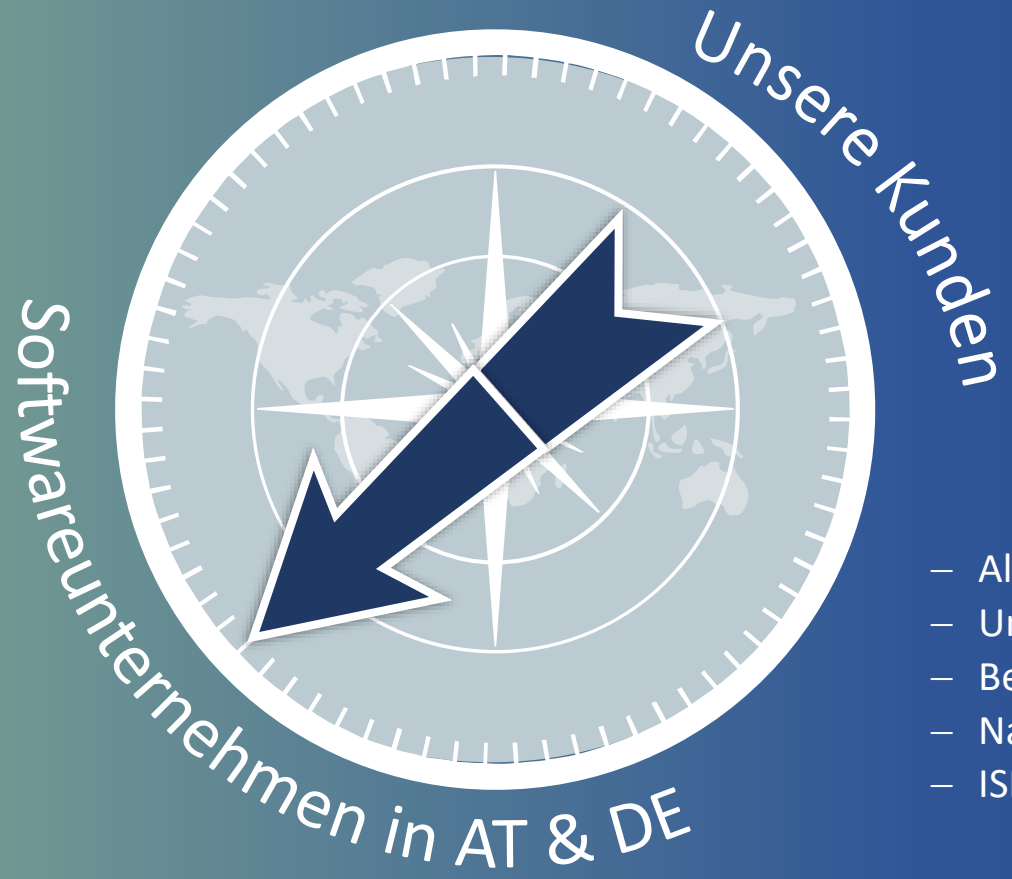
Intervalid ISMS

Informationssicherheitsmanagement System

Komplexe Themen erfordern einfache Lösungen

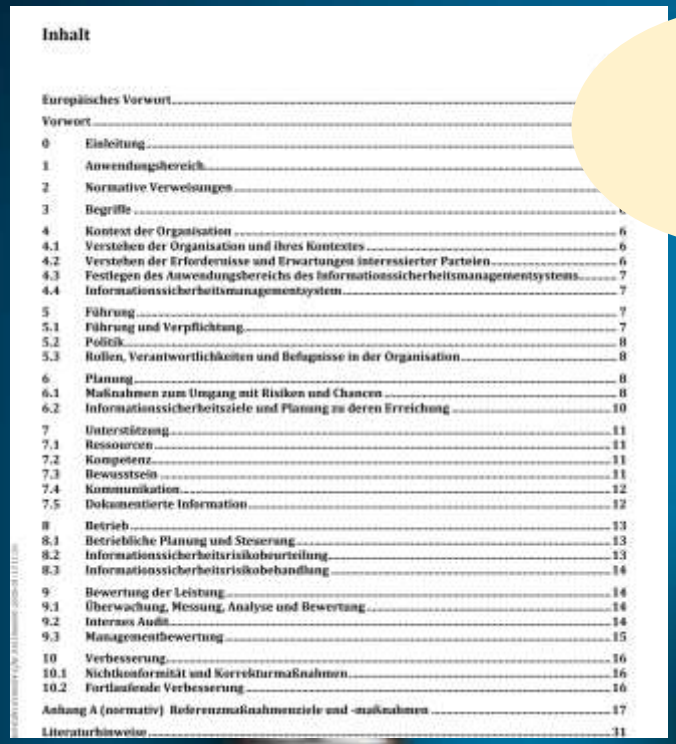
Intervalid GmbH

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

Was?

Muster für Richtlinien, Verfahren, Checkliste, etc.

User einbinden

Workflows

Wie?

Best Pratice Beispiele

Ablauf: der rote Faden

ISMS – Sie fangen nicht bei null an

ISMS – Der rote Faden

1. Norm auswählen

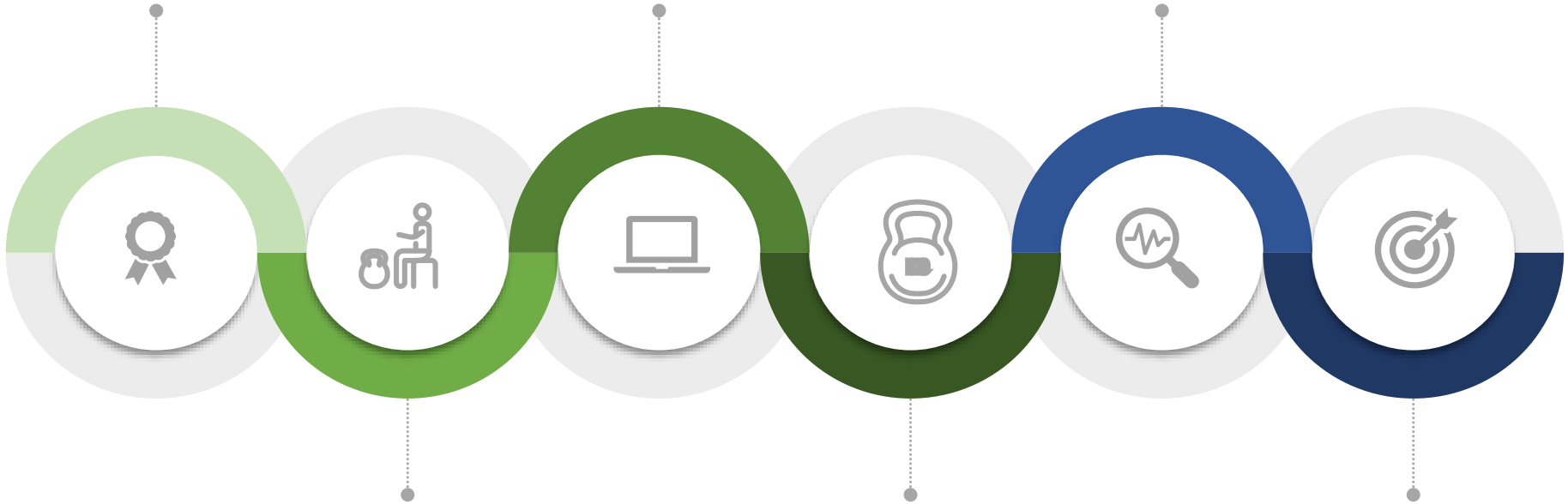
Beispielsweise ISO 27001, TISAX, B3S, VDS 10000, BSI IT-Grundschutz etc.

3. Asset Register

Erstellen & laufend pflegen
Schutzbedarf festlegen

5. Maßnahmen

Maßnahmen zur Umsetzung & Prüfung weiterleiten



2. Umsetzung der Norm

Richtlinien & Verfahrensbeschreibungen
Interne Prozesse

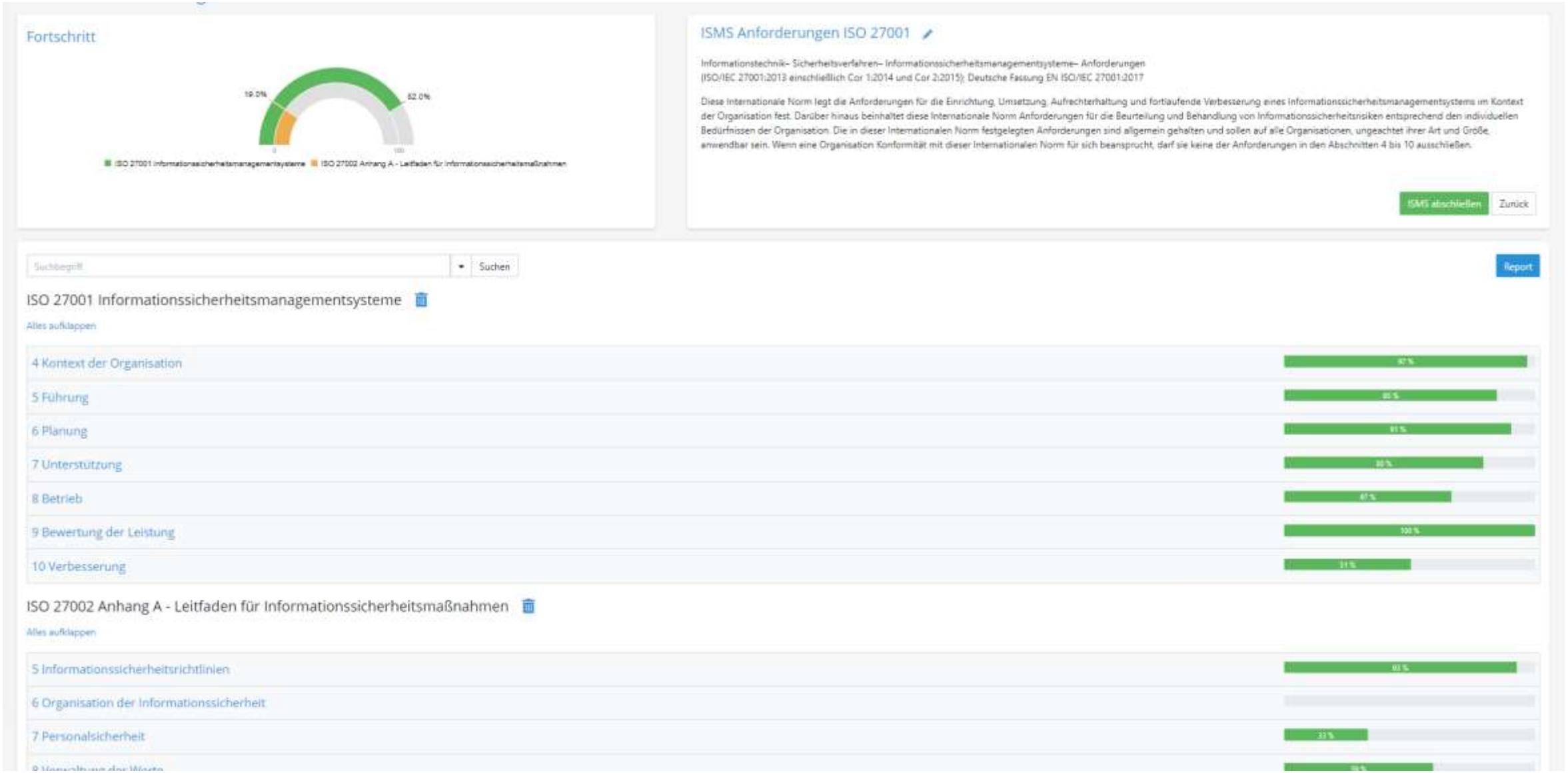
4. Risikoanalyse

Bedrohungen erkennen, Risiko beurteilen & Maßnahmen ableiten

6. Audits

Laufend überprüfen & Prozesse verbessern.
Inkl. Lieferantenaudits

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:

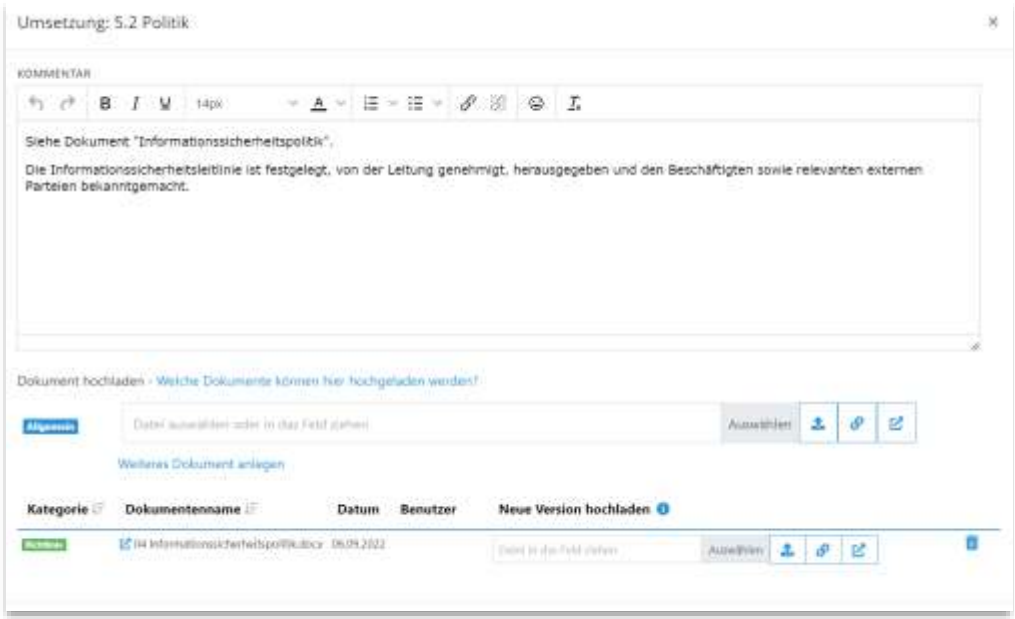
a) für den Zweck der Organisation angemessen ist;
b) Informationssicherheitsziele (siehe 6.2) beinhaltet oder den Rahmen zum Festlegen von Informationssicherheitszielen bietet;
c) eine Verpflichtung zur Erfüllung zutreffender Anforderungen mit Bezug zur Informationssicherheit enthält; und
d) eine Verpflichtung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



ISMS Schritt 1 – Unternehmensdokumente

Unternehmensdokumente

Suchbegriff | Suchen | Dokumente kopieren | Dokument hochladen | Dokument erstellen

Unternehmen	Kategorie	Dokumentenname	Dateityp	Datum	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 beitung durch Benigna Prochaska	Benigna Prochaska
Holding	Richtlinien	A.9.2 Kennwort Richtlinie.docx			geladen	Benigna Prochaska
Holding	Richtlinien	A.10 Richtlinie des Einsatzes von Verschlüsselung.docx			geladen beitung durch Benigna Prochaska	Benigna Prochaska
Holding	Richtlinien	A.11.1 Richtlinie zum aufgeräumten Arbeitsplatz leeren Bildschirm.docx			geladen	
Holding	Richtlinien	A.11.2 Richtlinie zur Entsorgung und Vernichtung.docx			geladen	
Holding	Richtlinien	A.12.2 Richtlinie zum Änderungsmanagement.docx			geladen	
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

Asset Register

Suchbegriff | Suchen | Asset hinzufügen

Nr.	Kategorie	Unternehmen	Abteilung	Titel	Merkmal	Fortschritt	Verantwortlicher Benutzer	Schutzbedarf
Geschäftsprozesse								
GP 0001	Kategorie setzen	Holding	IT	Benutzerverwaltung	Interner Gebrauch	1 2 3	Andreas Bergmann	2 3 1 3
GP 0003	Kategorie setzen	Holding	Personalabteilung	Bewerberverwaltung	Interner Gebrauch	1 2 3	Andreas Bergmann	2 1 2 2
GP 0002	Kategorie setzen	Holding	Geschäftsführung	Datenschutzmanagement	Vertraulich	1 2 3	Andreas Bergmann	2 1 1 2
GP 0004	Kategorie setzen	Holding	Finanz-und Rechnungswesen	Finanz- und Rechnungswesen	Vertraulich	1 2 3	Andreas Bergmann	3 2 2 3
GP 0013	Leistungsprozesse	Holding	Marketing	Kunden akquirieren	Merkmal setzen	1 2 3	Andreas Bergmann	1 2 1 2
GP 0006	Leistungsprozesse	Holding	Marketing	Kundenbetreuung (CRM)	Merkmal setzen	1 2 3	Andreas Bergmann	2 2 2 2
GP 0007	Leistungsprozesse	Holding	Marketing	Newsletter Versand an Kunden und Interessenten	Eingeschränkt	1 2 3	Andreas Bergmann	1 1 1 1
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.

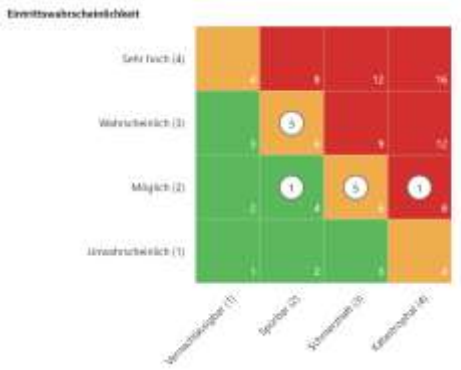
3 Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

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	Schwachstelle	Risiko	Neues Risiko	Risikobehandlung
Rechtemissbrauch	Die Rechtevergabe ist im System nur auf Administratoren Rechte beschränkt.	2 2 4	2 1 2	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

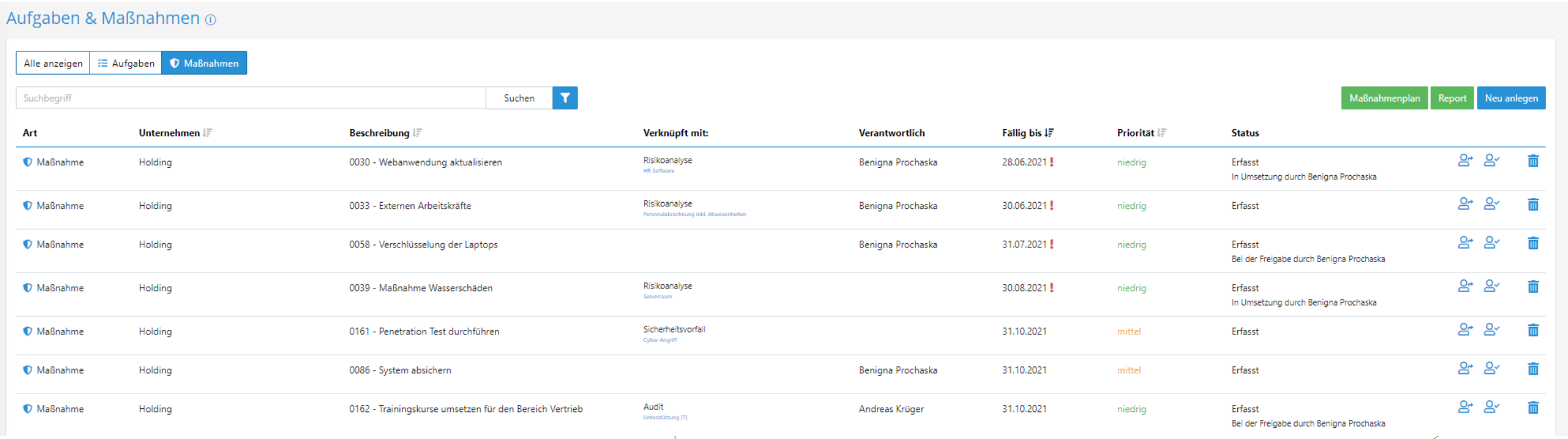
ISMS Schritt 4 – Maßnahmen

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



Aus
Audit, Sicherheitsvorfall,
Risikoanalyse, etc.

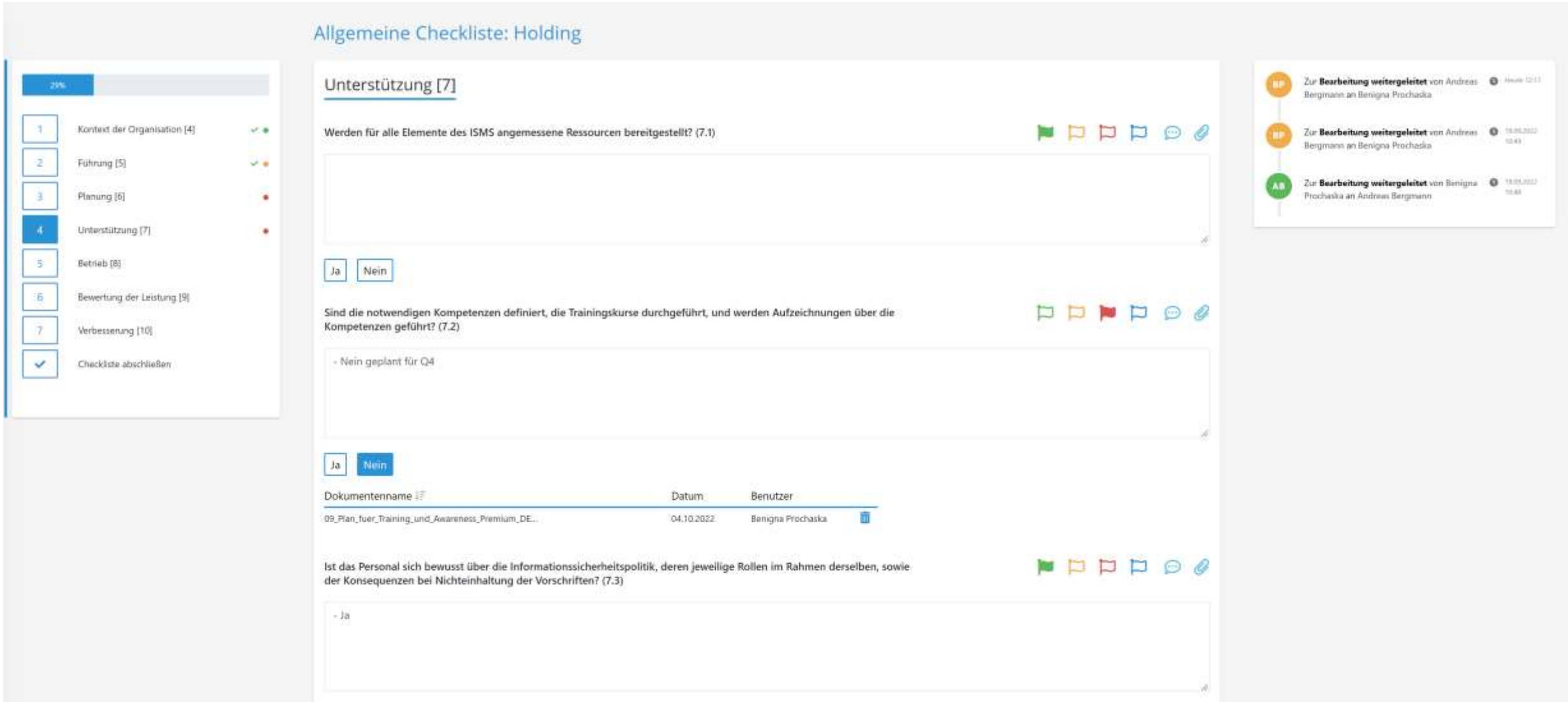
Zur Umsetzung &
Überprüfung weiterleiten

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



ISMS Schritt 5 – Audit Ergebnis


Audit
Internes Audit ISO 27001

Ergebnisse

Gesamtwertung

Prüfung Zusammenfassung

Ergebnisse im Detail anzeigen

Zurück

FILTER:

KONFORM | RISIKO | HOHES RISIKO | NICHT BEURTEILBAR

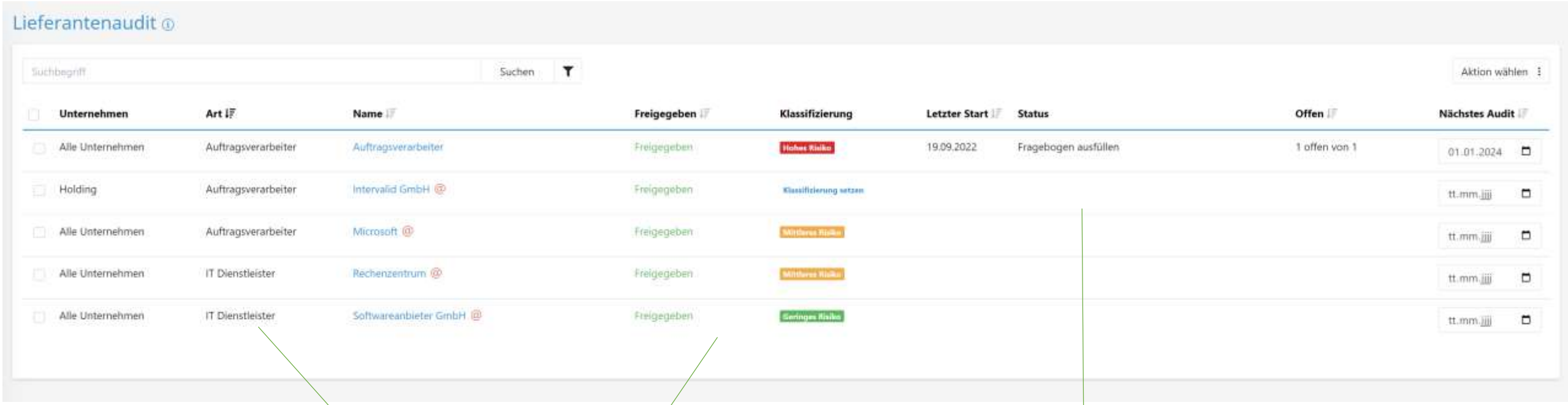
Suchbegriff | Suchen

Erstelle Report

Risiko	Abschnitt	Frage	Antwort	Aufgaben & Maßnahmen
Internes Audit ISO 27001 - Holding				
	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

Aufgaben & Maßnahmen setzen

ISMS Schritt 5 – Lieferantenaudit



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

Intervalid DSMS

CORINNA SALLMUTTER

Marketing & Sales | Intervalid GmbH

Tel: +43 1 905 10 44 12
E-Mail: corinna.sallmutter@intervalid.at