GoCompliant

Die modulare Governance Risk & Compliance Lösung

GoCompliant
Angebot

Unsere Mission und Prinzipien

GoCompliant kombiniert die verschiedenen Komponenten eines umfassenden Governance, Risk und Compliance (GRC) Konzepts. GoCompliant trägt dazu bei, das Risikobewusstsein in ihrem Unternehmen zu schärfen und unterstützt sie dabei, ihre wertvollen Ressourcen auf die wesentlichen Elemente des Risikomanagements zu fokussieren.

Modularer Aufbau
(pay what you use)

Einfach zu implementieren,
hochgradig konfigurierbar

Industrie-agnostisch,
generisch einsetzbar

Direkte Benutzer-
Einbindung

Umfassende und
übersichtliche
Dashboards

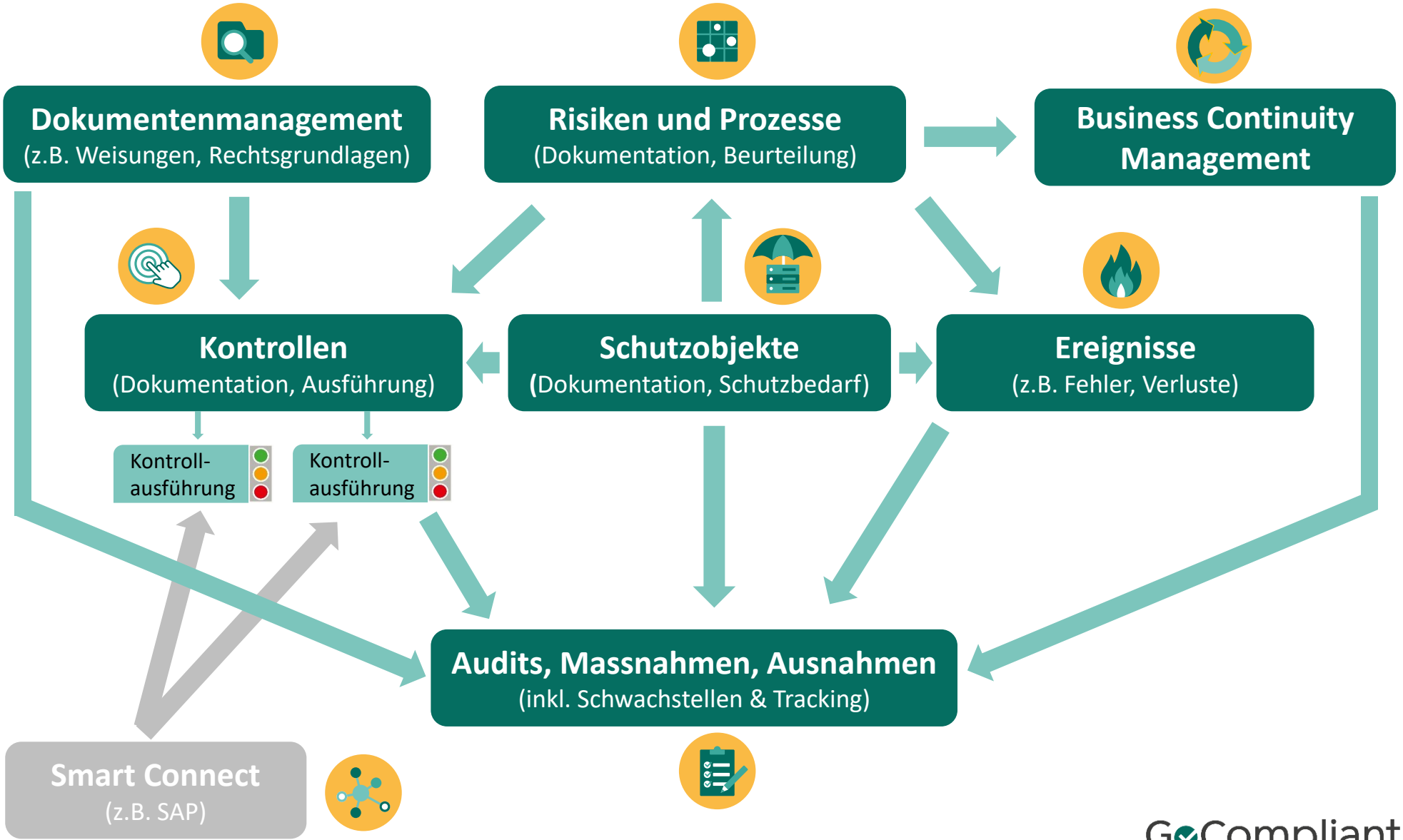
Integrierte Reporting
Funktionalität

Technische
Schnittstellen
(z.B. SAP)

On-premises
Lösung oder
Cloud (SaaS)

GoCompliant

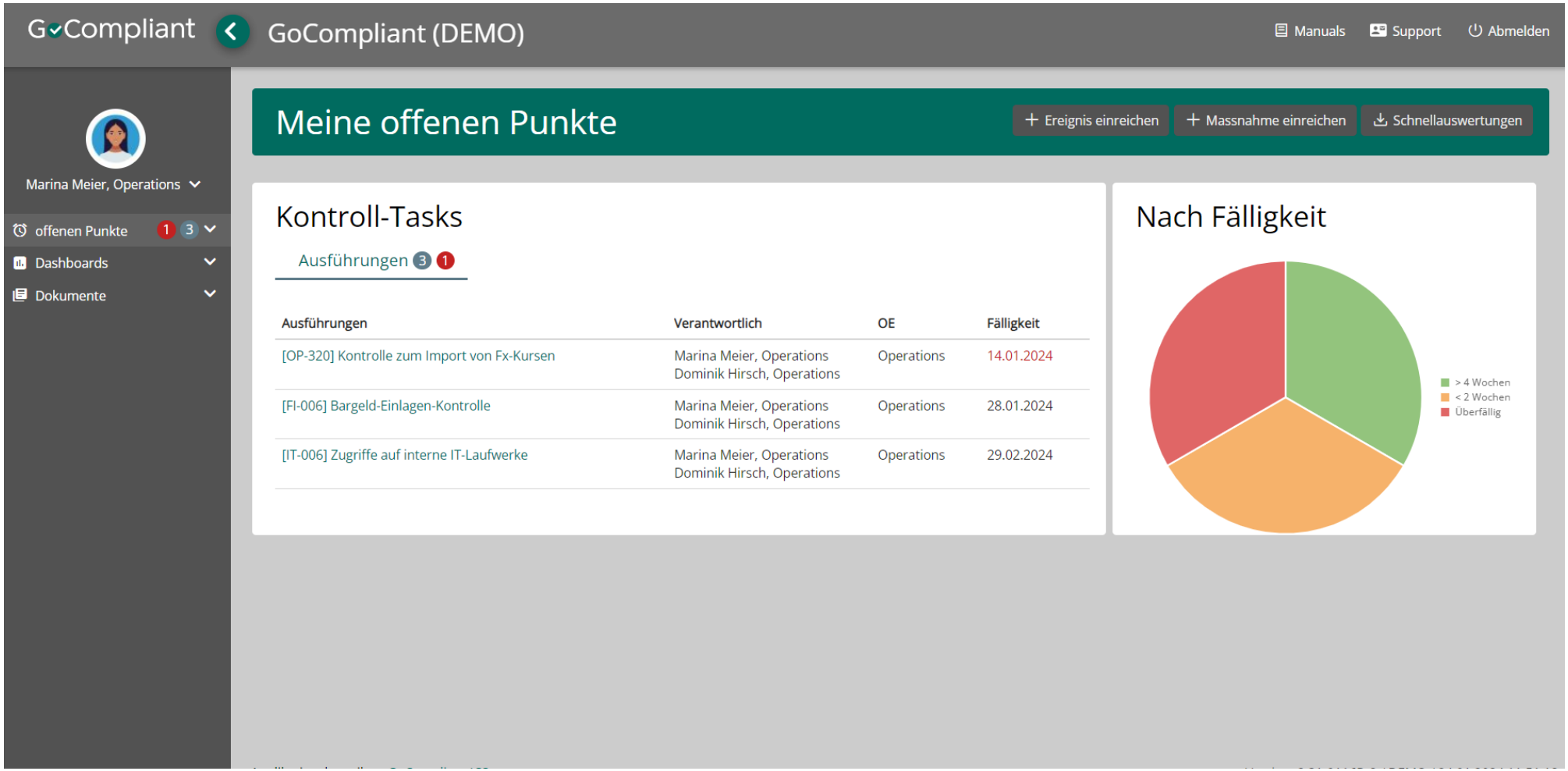
Übersicht der Module



GoCompliant

Screenshots

Einstiegsseite



Logos, Farben, Texte etc. sind konfigurierbar

GoCompliant

Kontrollausführung

[IT-006] Zugriffe auf interne IT-Laufwerke

Kontroll-Task | Frühere Ausführungen | Kontakte und Details

Task ID 49650 (Ausführung pendent)

Beschreibung & Ergebnisanleitung

Kontrollbeschreibung	Zweimal jährlich werden sämtliche Zugriffsrechte von Mitarbeitenden auf alle internen Laufwerke geprüft. Es muss geprüft werden, ob die Zugriffsrechte mit dem Aufgabenprofil des Mitarbeitenden im Einklang stehen.
Kontrollanleitung	• Liste aller Laufwerke und Zugriffsrechte von IT Support anfordern • Prüfen, ob noch Zugriffsrechte für inzwischen ausgetretene Mitarbeitende vorhanden sind • Prüfen, ob Zugriffsrechte von Mitarbeitenden mit internem Stellenwechsel angepasst wurden • Prüfen, ob sämtliche Zugriffsrechte mit dem Aufgabenprofil des Mitarbeitenden im Einklang stehen • Im Zweifelsfall: Meinung vom Vorgesetzten einholen

Kontroll-Task

Kontrollzeitraum	01.01.2023 - 31.12.2023	Signoffzeitraum	01.03.2024 - 30.04.2024
Ausführungszeitraum	01.01.2024 - 29.02.2024	Signoff Empfänger	Karin Schilter, FINOP
Ausführung Empfänger	Marina Meier, Operations Dominik Hirsch, Operations	OE	Operations

Rating *

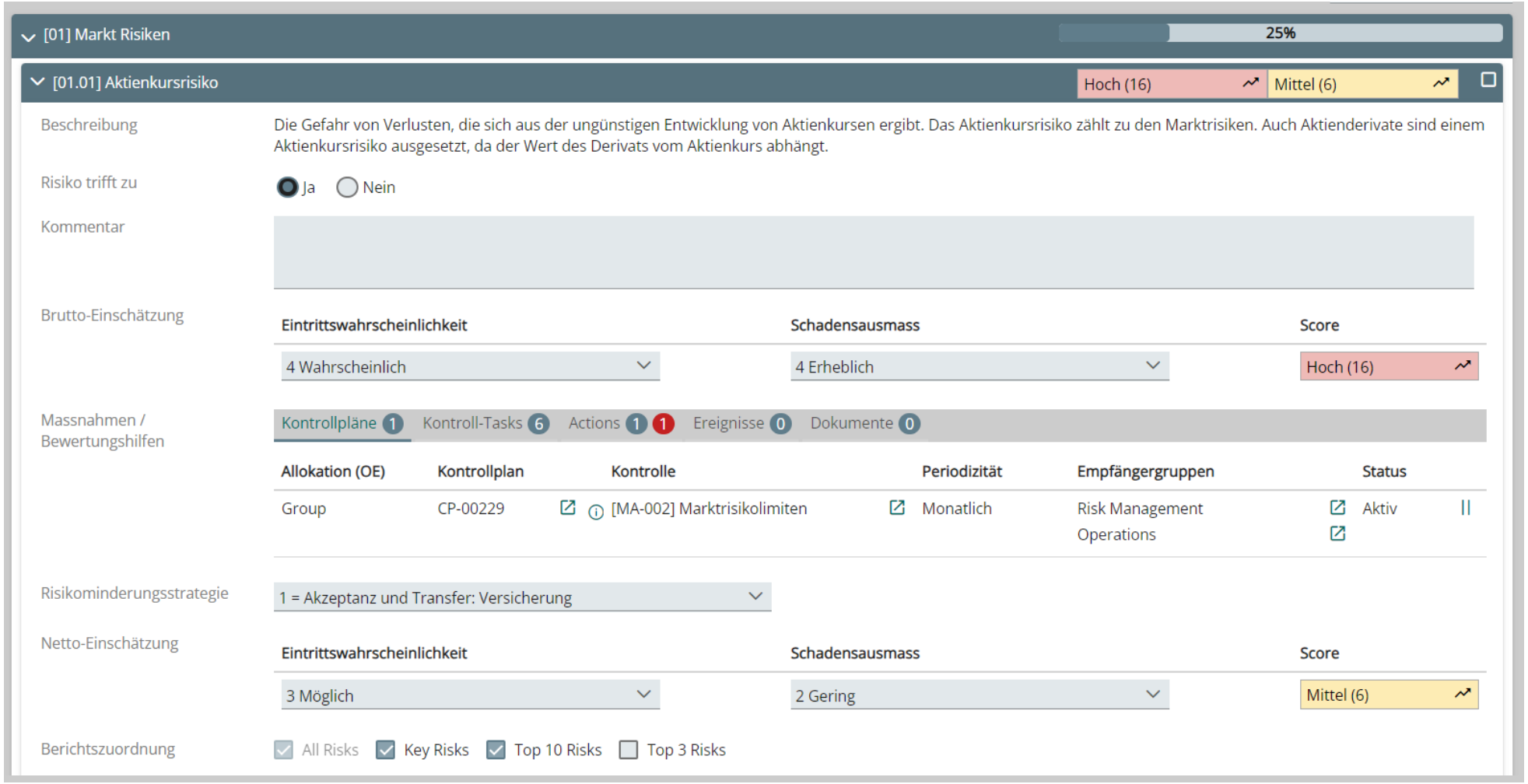
Kommentar Ausführung

Anhänge

Titel	Typ	Ort	Gültigkeitsbeschränkung	Hinzugefügt	Von

GoCompliant

Risikobewertung (konfigurierbar)



GoCompliant

Risiko-Heatmap

Filter Bericht
- All Risks
- Key Risks
- Top 10 Risks
- Top 3 Risks

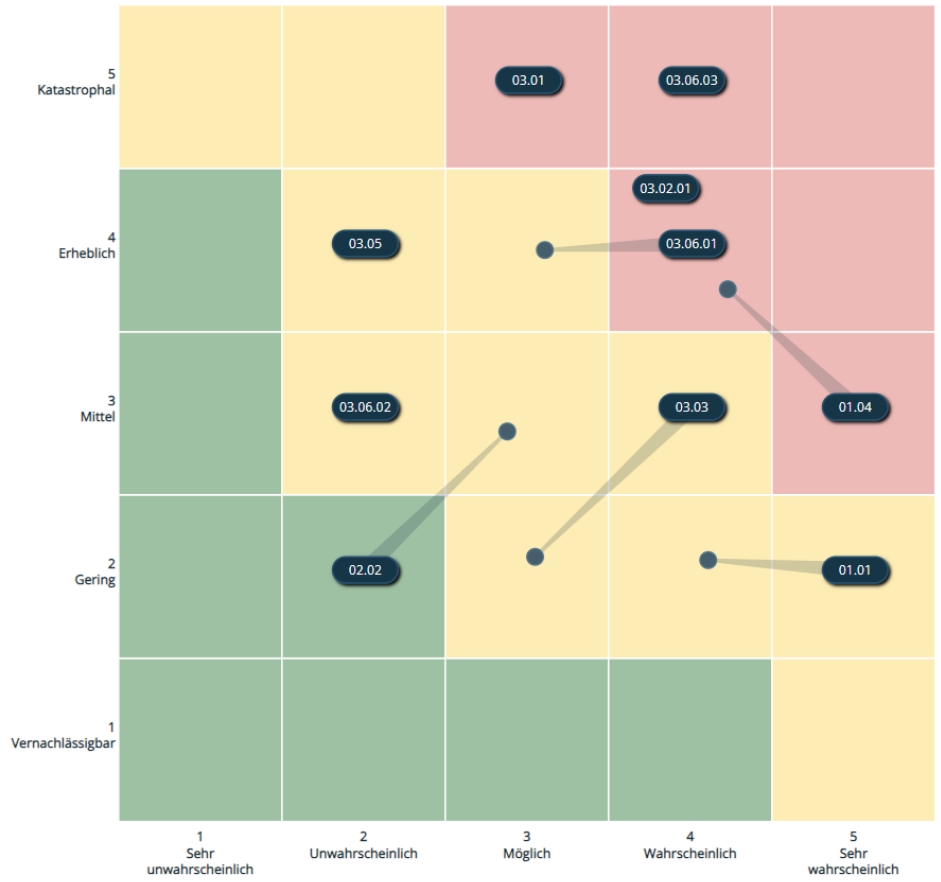
Filter Risiko / OE
- Risiko
- Risiko OE

Heatmap
- Inhärent (Inhärent)
- Residual (Residual)

Trendvisualisierung
- Keine Trends
- Trendvisualisierung von Vorperiode
- Trendvisualisierung ganze Historie

Filter Vergleich mit Vorperiode
- Zunahme
- Abnahme
- Unverändert
- Neues Risiko
- In Bezug auf gewählte Heatmap

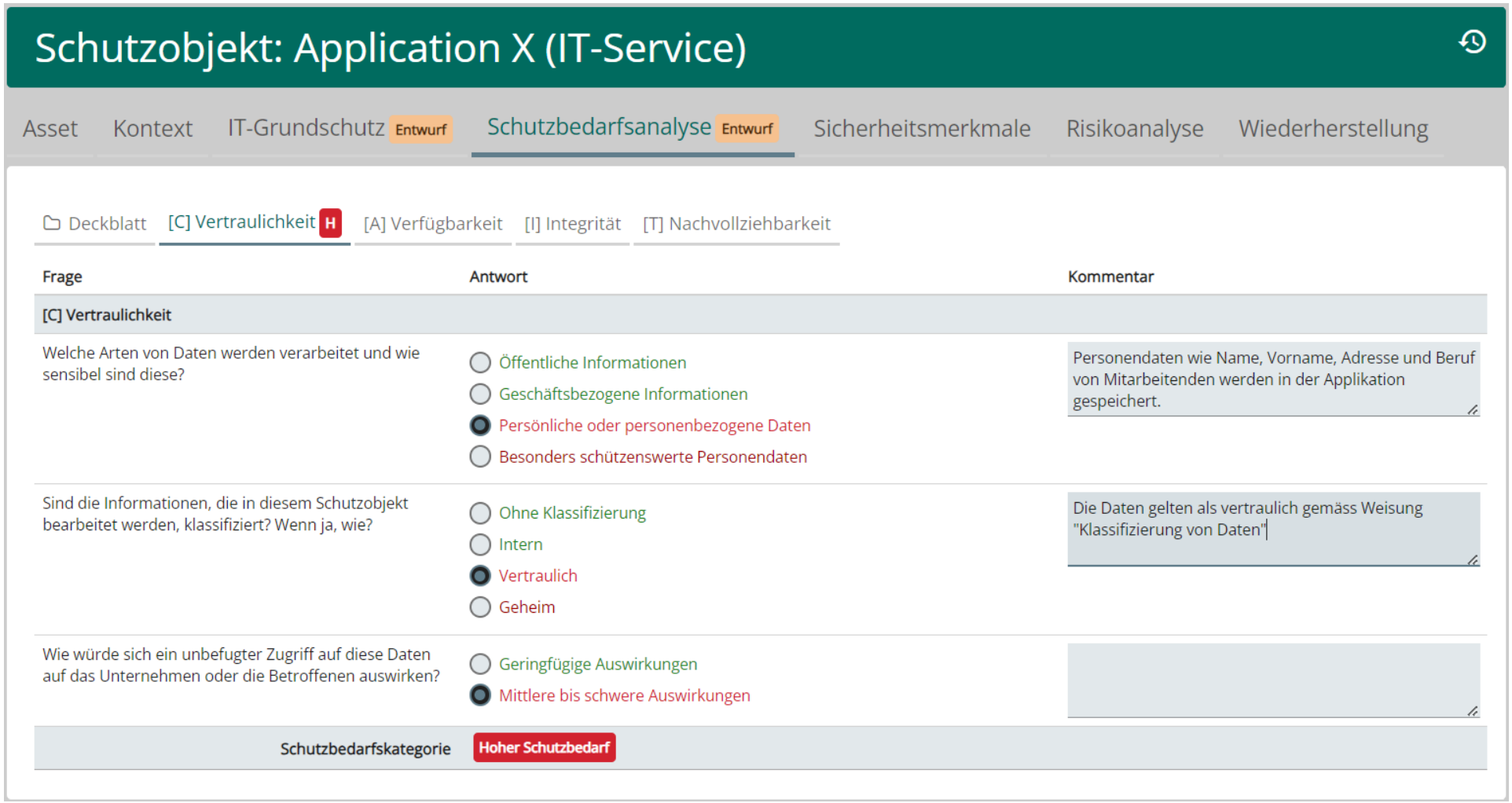
Exportieren



Nummer	Risiko	I...	R...
03.01	Interner Betrug	→	→
03.06.03	Netzwerk-Fehler	→	↘
03.06.01	Hardware-Fehler	↗	↗
03.02.01	Diebstahl und Betrug	→	↘
01.04	Währungsrisiko	↘	↗
03.03	Sicherheit am Arbeitsplatz	↗	↗
01.01	Aktienkursrisiko	↗	↗
03.06.02	Software-Fehler	→	→
03.05	Sachschäden	→	↘
02.02	Kreditrisiko	↘	↘

Total: 10 « ‹ 1 › » 20

GoCompliant


Schutzobjekt: Application X (IT-Service)
Asset
Kontext
IT-Grundschutz Entwurf
Schutzbedarfsanalyse Entwurf
Sicherheitsmerkmale
Risikoanalyse
Wiederherstellung
Deckblatt
[C] Vertraulichkeit H
[A] Verfügbarkeit
[I] Integrität
[T] Nachvollziehbarkeit
Frage
Antwort
Kommentar
[C] Vertraulichkeit
Welche Arten von Daten werden verarbeitet und wie sensibel sind diese?
Öffentliche Informationen
Geschäftsbezogene Informationen
Persönliche oder personenbezogene Daten
Besonders schützenswerte Personendaten
Personendaten wie Name, Vorname, Adresse und Beruf von Mitarbeitenden werden in der Applikation gespeichert.
Sind die Informationen, die in diesem Schutzobjekt bearbeitet werden, klassifiziert? Wenn ja, wie?
Ohne Klassifizierung
Intern
Vertraulich
Geheim
Die Daten gelten als vertraulich gemäss Weisung "Klassifizierung von Daten"
Wie würde sich ein unbefugter Zugriff auf diese Daten auf das Unternehmen oder die Betroffenen auswirken?
Geringfügige Auswirkungen
Mittlere bis schwere Auswirkungen
Schutzbedarfskategorie
Hoher Schutzbedarf

Information Security Management (ISMS)

ISMS-Feststellungen

+ Neu: Feststellung

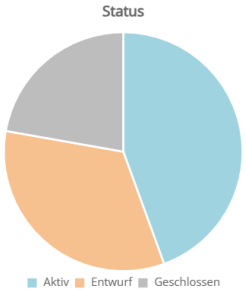
Nummer	Titel	Status	Schweregrad	Behandlung	OE	Asset
I11801	Log4J-Security Issue	Entwurf	M	Vermeiden	PB/IT	HR-Tool
I11701	Fehlende Software-Upgrades bei HR-Tool	Akzeptieren (Freigabe nötig)	T	Akzeptieren	HR	HR-Tool
I11901	Fehlende Überwachung bei Zulassung externer MA	Entwurf	K	Noch Nicht Festgelegt	CEO	ISMS-Tool
I12001	Mitarbeiter Offboarding unzureichend					
I11601	Log4j-Sicherheitslücke					

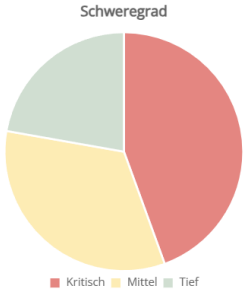
ISMS-Übersicht

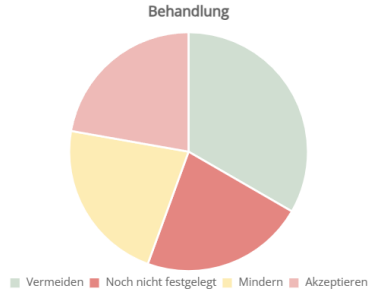
Schnellauswertungen

ISMS-Feststellungen

Verantwortlicher Bereich	Status			Überfällig	Schweregrad			Behandlung			
	Entwurf	Aktiv	Geschlossen		Tief	Mittel	Kritisch	Noch nicht festgelegt	Vermeiden	Mindern	Akzeptieren
Alle	3	4	2	3	2	3	4	2	3	2	2
CEO	2	-	2	-	-	2	2	2	2	-	-
HR	-	4	-	3	2	-	2	-	-	2	2
PB/IT	1	-	-	-	-	1	-	-	1	-	-







[1] Aggregierte Werte

GoCompliant