

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

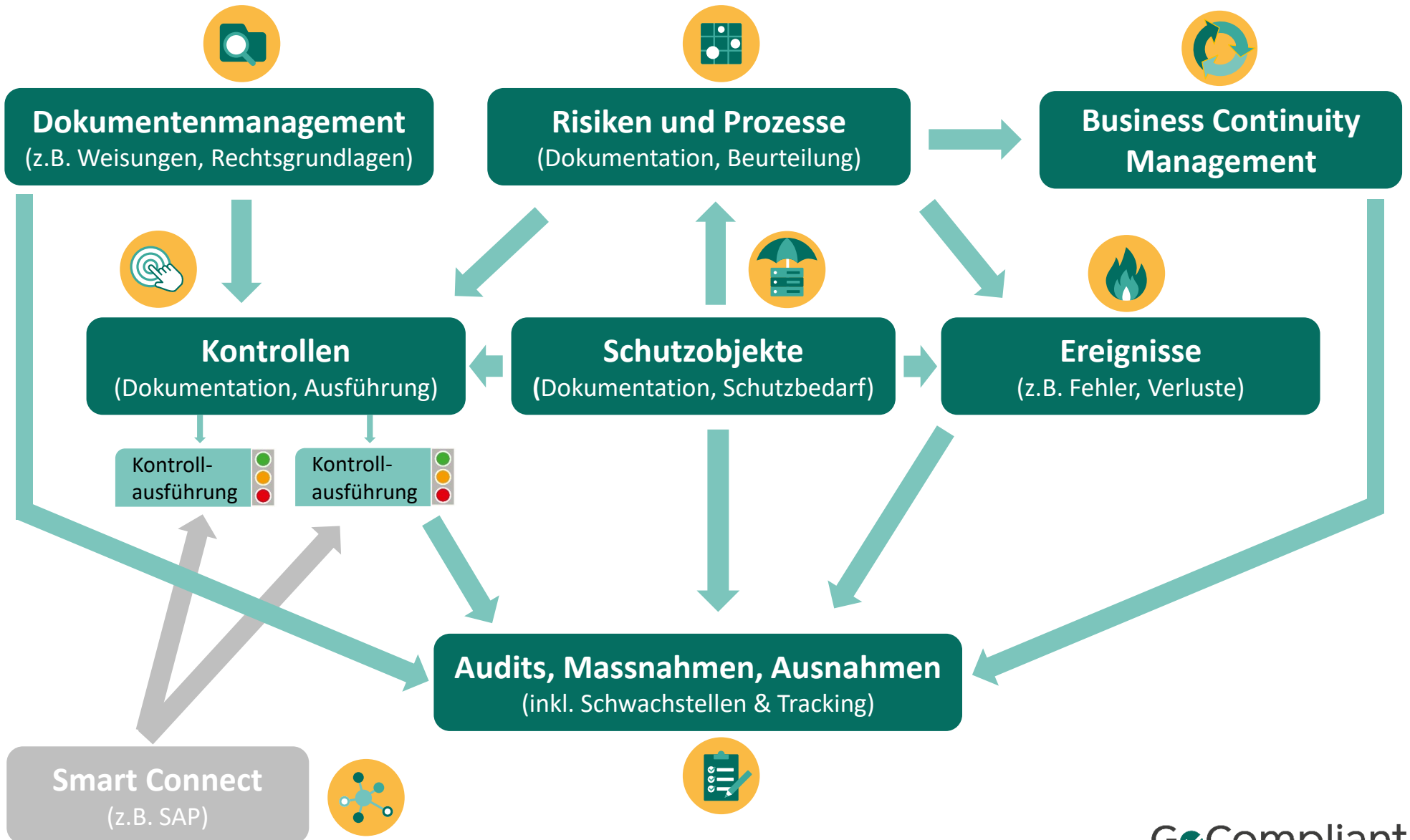


Technische
Schnittstellen
(z.B. SAP)



On-premises
Lösung oder
Cloud (SaaS)

Übersicht der Module



Screenshots

GoCompliant GoCompliant (DEMO) Manuals Support Abmelden

Marina Meier, Operations

offenen Punkte 1 3

Dashboards

Dokumente

Meine offenen Punkte

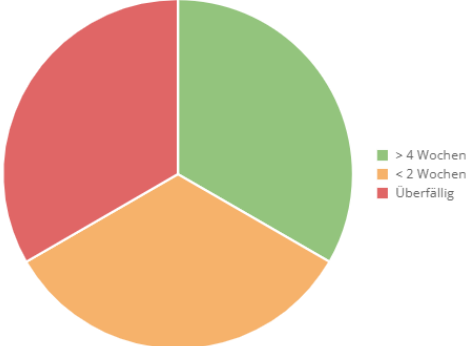
+ Ereignis einreichen + Massnahme einreichen ⬇ Schnellauswertungen

Kontroll-Tasks

Ausführungen 3 1

Ausführungen	Verantwortlich	OE	Fälligkeit
[OP-320] Kontrolle zum Import von Fx-Kursen	Marina Meier, Operations Dominik Hirsch, Operations	Operations	14.01.2024
[FI-006] Bargeld-Einlagen-Kontrolle	Marina Meier, Operations Dominik Hirsch, Operations	Operations	28.01.2024
[IT-006] Zugriffe auf interne IT-Laufwerke	Marina Meier, Operations Dominik Hirsch, Operations	Operations	29.02.2024

Nach Fälligkeit



Legend:
■ > 4 Wochen (green)
■ < 2 Wochen (orange)
■ Überfällig (red)

Logos, Farben, Texte etc. sind konfigurierbar

[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	
---------	-------	-----	-----	-------------------------	-------------	-----	--

Risikobewertung (konfigurierbar)

▼ [01] Markt Risiken 25%

▼ [01.01] Aktienkursrisiko Hoch (16) Mittel (6)

Beschreibung Die Gefahr von Verlusten, die sich aus der ungünstigen Entwicklung von Aktienkursen ergibt. Das Aktienkursrisiko zählt zu den Marktrisiken. Auch Aktienderivate sind einem Aktienkursrisiko ausgesetzt, da der Wert des Derivats vom Aktienkurs abhängt.

Risiko trifft zu Ja Nein

Kommentar

Brutto-Einschätzung

Eintrittswahrscheinlichkeit	Schadensausmass	Score
4 Wahrscheinlich	4 Erheblich	Hoch (16)

Massnahmen / Bewertungshilfen

Kontrollpläne 1 Kontroll-Tasks 6 Actions 1 1 Ereignisse 0 Dokumente 0

Allokation (OE)	Kontrollplan	Kontrolle	Periodizität	Empfängergruppen	Status
Group	CP-00229	<input checked="" type="checkbox"/> [MA-002] Marktrisikolimiten	<input checked="" type="checkbox"/> Monatlich	Risk Management Operations	<input checked="" type="checkbox"/> Aktiv <input checked="" type="checkbox"/>

Risikominderungsstrategie 1 = Akzeptanz und Transfer: Versicherung

Netto-Einschätzung

Eintrittswahrscheinlichkeit	Schadensausmass	Score
3 Möglich	2 Gering	Mittel (6)

Berichtszuordnung All Risks Key Risks Top 10 Risks Top 3 Risks

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

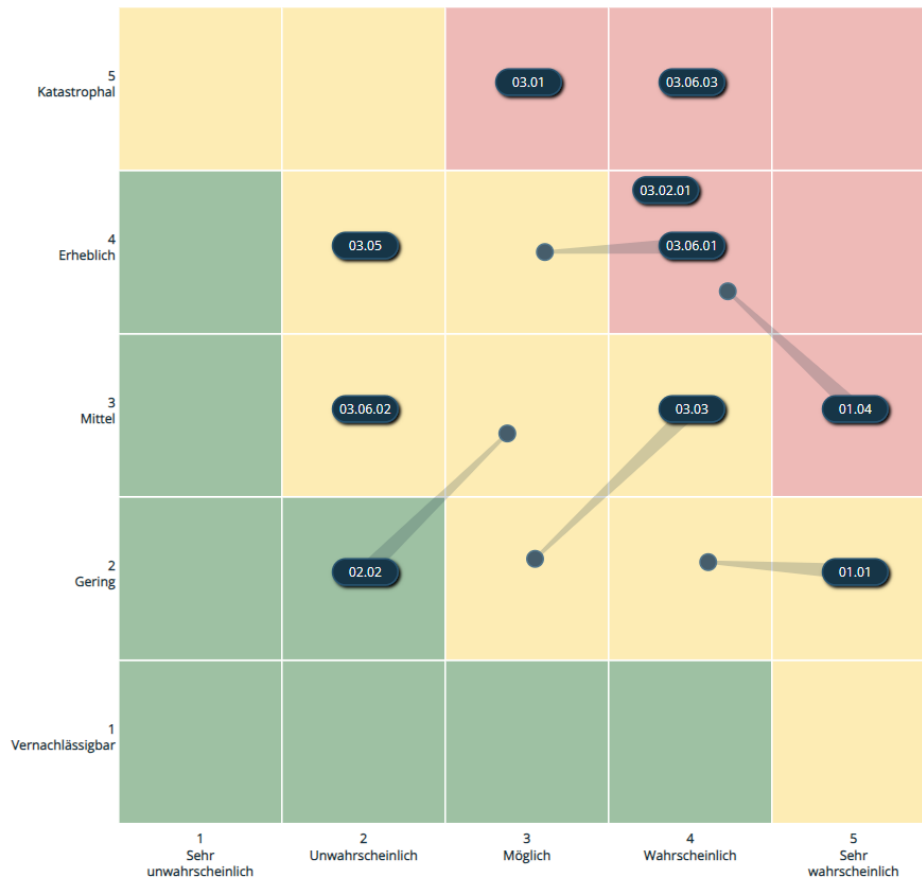
Trendvisualisierung

- 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	L...	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

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?	<input type="radio"/> Öffentliche Informationen <input type="radio"/> Geschäftsbezogene Informationen <input checked="" type="radio"/> Persönliche oder personenbezogene Daten <input type="radio"/> 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?	<input type="radio"/> Ohne Klassifizierung <input type="radio"/> Intern <input checked="" type="radio"/> Vertraulich <input type="radio"/> 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?	<input type="radio"/> Geringfügige Auswirkungen <input checked="" type="radio"/> Mittlere bis schwere Auswirkungen	
Schutzbedarfskategorie		Hoher Schutzbedarf

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					

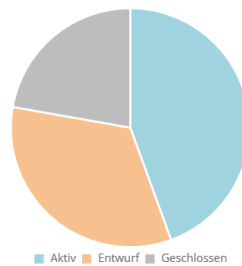
ISMS-Übersicht

↓ Schnellauswertungen

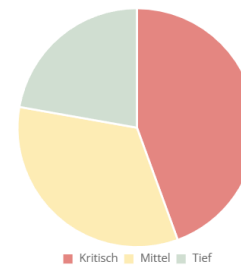
ISMS-Feststellungen

Verantwortlicher Bereich	Status			Überfällig	Schweregrad			Behandlung	Vermeiden	Mindern	Akzeptieren
	Entwurf	Aktiv	Geschlossen		Tief	Mittel	Kritisch				
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	-	-

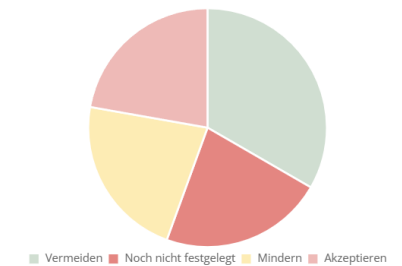
Status



Schweregrad



Behandlung



¹⁾ Aggregierte Werte