Informationssicherheits? und Compliance?Management (ISMS/GRC) mit CISO Assistent

1. Zweck von CISO Assistant

CISO Assistant ist in dieser Architektur das zentrale Werkzeug für Informationssicherheits- und Compliance-Management (ISMS/GRC).
Es verbindet die fachlichen und technischen Elemente deiner Umgebung (Prozesse, Systeme, Risiken, Kontrollen, Maßnahmen, Audits) zu einem prüfbaren, strukturierten ISMS.

---

2. Aufgaben von CISO Assistant

In der Gesamtarchitektur übernimmt CISO Assistant insbesondere:

- Verwaltung des **Asset-Inventars**
  - Prozesse („Prozess – …“ aus BookStack)
  - Systeme („System – …“ aus BookStack)
  - Anwendungen, Datenbestände, Dienstleister, Standorte
- Verwaltung von **Risiken und Risikobewertungen**
  - Erfassung von Risiken mit Bezug zu Prozessen und Systemen
  - Bewertung (Eintrittswahrscheinlichkeit, Auswirkung, Risikolevel)
  - Verknüpfung mit Maßnahmen und Kontrollen
- Verwaltung von **Kontrollen und Maßnahmen**
  - Abbildung von Kontrollen (technisch, organisatorisch) je Framework
  - Mapping zu ISO/NIST/NIS2 etc.
  - Verknüpfung mit konkreten Prozessen, Richtlinien und Systemen
- **Audit- und Compliance-Management**
  - Planung und Durchführung von Audits
  - Nachweisführung (Evidenzen)
  - Berichtswesen für Management und Prüfer

---

3. Verbindung zu BookStack

CISO Assistant verlinkt auf die lesbare Dokumentation in BookStack:

- Prozess-Assets in CISO Assistant (z.B. „Prozess – Benutzeranlage im Active Directory“) verweisen auf die entsprechende Prozessbeschreibung in BookStack.
- Richtlinien- und Maßnahmenbeschreibungen in CISO Assistant verweisen auf die ausführliche Richtlinie („Richtlinie – …“) und Arbeitsanweisungen in BookStack.
- So ist für Auditoren und Management klar:
  - fachliche Beschreibung und Arbeitsanweisungen → BookStack
  - ISMS-Sicht (Risiko, Kontrolle, Compliance) → CISO Assistant.

---

4. Verbindung zu Flowable

CISO Assistant dokumentiert, welche Prozesse technisch umgesetzt sind:

- Prozess-Assets in CISO Assistant enthalten eine Kennung zum zugehörigen Flowable-Workflow (z.B. `PR-Benutzeranlage-AD`).
- In Maßnahmen oder Kontrollen kann festgehalten werden, dass eine bestimmte Anforderung „durch Workflow <Kennung> in Flowable“ umgesetzt ist.
- So wird transparent, dass z.B. ein Rollen-Rezertifizierungsprozess nicht nur auf Papier existiert, sondern als konkreter Workflow im Betrieb läuft.

---

5. Verbindung zu Wazuh

CISO Assistant nimmt die technische Realität aus Wazuh auf und überführt sie in ISMS-Sicht:

- Sicherheitsereignisse, Schwachstellen oder Policy-Verstöße aus Wazuh werden in CISO Assistant als Incidents oder Risiken mit Bezug zu Prozessen und Systemen dokumentiert.
- Daraus abgeleitete Maßnahmen (z.B. Härtung, zusätzliche Kontrollen, Prozessanpassungen) werden ebenfalls in CISO Assistant geführt und nachverfolgt.
- Damit schließt sich der Kreis:
  - Wazuh entdeckt Probleme,
  - CISO Assistant bewertet, steuert und dokumentiert deren Behandlung,
  - Flowable setzt ggf. die Gegenmaßnahmen als Prozess um,
  - BookStack hält die aktualisierte Doku und Richtlinien fest.

---

6. Zusammenfassung der Rolle

Kurz beschrieben ist CISO Assistant:

- das **„Gehirn“ des ISMS**: Risiko-, Kontroll- und Compliance-Steuerung,
- die **Brücke** zwischen fachlicher Doku (BookStack) und operativer Umsetzung (Flowable),
- der **Nachweis- und Reporting-Layer** gegenüber Management, Kunden und Auditoren,
- der **Einsammelpunkt** für sicherheitsrelevante Erkenntnisse aus der Technik (z.B. Wazuh), die in Management-Entscheidungen und Maßnahmen überführt werden.

Damit wird CISO Assistant in deiner Architektur der zentrale Ort, an dem sichtbar wird, dass die dokumentierten Prozesse (BookStack) und Workflows (Flowable) die Anforderungen aus Normen, Gesetzen und Sicherheitszielen wirklich erfüllen.

Revision #1
Created 2026-03-30 10:18:54 UTC by Gerd
Updated 2026-03-30 10:20:30 UTC by Gerd