Konzepte - Organisationsanwendungen

Hier werden Vorschläge für Anwendungen und Einsatzkonzepte vorgehalten und bei Bedarf auf die Kunden angepasst.

- Referenzarchitektur
  - Einführung in die Referenzarchitektur ISMS-BPM-Doku-Stack
  - Referenzarchitektur ISMS-BPM-Doku-Stack (CISO Assistant · Flowable · Wazuh · BookStack)“
- Prozesse
  - Prozessorganisation in Bookstack
  - Prozessorganisation in Flowable
  - Informationssicherheits- und Compliance-Management (ISMS/GRC) mit CISO Assistent
- Flyer - Integriertes ISMS- und Prozessmanagement

Referenzarchitektur

Referenzarchitektur

Einführung in die Referenzarchitektur ISMS?BPM?Doku?Stack

Titel:
Einführung in die Referenzarchitektur ISMS-BPM-Doku-Stack

Zweck dieser Architektur

Diese Referenzarchitektur beschreibt, wie mehrere spezialisierte Anwendungen kombiniert werden, um Informationssicherheit, Prozesse und Dokumentation in einer Organisation strukturiert und prüfbar abzubilden. Sie dient als Leitlinie für die Konzeption, Implementierung und Weiterentwicklung eines integrierten ISMS- und Prozessmanagement-Stacks.

Zielbild

Ziel ist ein durchgängiger Zusammenhang zwischen:

- verständlich dokumentierten Prozessen und Rollen,
- ausführbaren Workflows im Tagesbetrieb,
- systematischem Risiko- und Maßnahmenmanagement,
- sowie der technischen Sicherheitsüberwachung.

Dadurch entsteht ein System, in dem Dokumentation nicht losgelöst von der Praxis existiert, sondern direkt mit gelebten Prozessen, Risiken, Kontrollen und technischen Sicherheitsereignissen verbunden ist.

Eingesetzte Anwendungen (Rollen im Gesamtbild)

- Ein Dokumentationssystem (z.B. BookStack) als zentrale Wissensbasis für Prozesse, Rollen, Systeme, Richtlinien und Arbeitsanweisungen.
- Eine BPM-Plattform (z.B. Flowable) zur Modellierung und Ausführung operativer Prozesse wie Benutzeranlage, Rechteverwaltung, Changes und Incidents.
- Ein ISMS-/GRC-Werkzeug (z.B. CISO Assistant) zur Verwaltung von Assets, Risiken, Kontrollen, Maßnahmen, Audits und Compliance-Anforderungen.
- Eine Security-Monitoring-Plattform (z.B. Wazuh) zur Erkennung von Sicherheitsereignissen, Schwachstellen und Policy-Verstößen.

Leitprinzipien

1. **Klare Aufgabentrennung**
   Jede Anwendung hat eine klar definierte Rolle (Doku, Workflow, ISMS/GRC, Security-Monitoring), um Doppelstrukturen und Medienbrüche zu vermeiden.
2. **Sprechende Bezeichnungen**
   Inhalte werden mit verständlichen, ausgeschriebenen Präfixen wie „Prozess – …“, „Richtlinie – …“, „Arbeitsanweisung – …“, „Rolle – …“ und „System – …“ benannt, damit sie für alle Nutzer schnell einzuordnen sind.
3. **Technische Kennungen im Hintergrund**
   Kurze Kennungen dienen der technischen Verknüpfung zwischen den Anwendungen, stehen aber nicht im Vordergrund der Benutzeroberfläche.
4. **Lose Kopplung statt harter Abhängigkeiten**
   Die Anwendungen werden über einheitliche Kennungen und einfache Verweise verbunden, sodass einzelne Komponenten bei Bedarf ausgetauscht werden können, ohne das Gesamtkonzept zu verlieren.

Anwendungsfälle

Die Referenzarchitektur unterstützt insbesondere folgende Szenarien:

- Aufnahme, Dokumentation und Automatisierung von Geschäfts- und IT-Prozessen.
- Ableitung und Umsetzung von Rollen- und Berechtigungskonzepten.
- Strukturierte Datenklassifizierung und Schutzbedarfsbetrachtung.
- Aufbau und Betrieb eines ISMS inklusive Risikomanagement, Kontrollen und Audits.
- Rückkopplung technischer Sicherheitsereignisse in das ISMS und in operative Prozesse.

Referenzarchitektur

Referenzarchitektur ISMS?BPM?Doku?Stack (CISO Assistant · Flowable · Wazuh · BookStack)“

Referenzarchitektur ISMS?BPM?Doku?Stack

(CISO Assistant · Flowable · Wazuh · BookStack)

Ziel

Dieses Konzept beschreibt, wie CISO Assistant, Flowable, Wazuh und BookStack gemeinsam eingesetzt werden, um Prozesse, Rollen und Berechtigungen, Datenklassifizierung, Risiken und ISMS-Anforderungen konsistent zu erfassen, zu dokumentieren und zu steuern.

---

1. Aufgabenteilung der Anwendungen

BookStack – Dokumentation & Handbuch

- Ablage von Prozessbeschreibungen, Rollenbeschreibungen, System- und Betriebsdokumentation, Richtlinien und Arbeitsanweisungen.
- Zielgruppe: Fachbereiche, IT, Management (lesbare, verständliche Texte).

Flowable – Ausführbare Prozesse (BPM)

- Modellierung und Ausführung von Prozessen wie Benutzeranlage, Rechteänderung, Rezertifizierung, Changes, Incidents.
- Steuerung von Aufgaben, Eskalationen und Genehmigungen.

CISO Assistant – ISMS/GRC

- Verwaltung von Assets, Risiken, Kontrollen, Maßnahmen, Audits und Framework-Compliance (z.B. ISO, NIST, NIS2).
- Nachweisführung gegenüber Audits und Management.

Wazuh – Sicherheitsüberwachung (SIEM/XDR)

- Technische Sicherheitsüberwachung, Events, Schwachstellen, Compliance-Checks als Input für Risiko- und Maßnahmenmanagement.

Grundregel:

- Prozess- und Betriebsdokumentation steht in BookStack.
- Prozessausführung läuft in Flowable.
- Risiken, Kontrollen, Audits und Maßnahmen werden in CISO Assistant geführt.
- Sicherheitsereignisse und technische Findings kommen aus Wazuh.

---

2. Namenskonzept und Präfixe

Für Nutzeroberflächen werden ausgeschriebene Präfixe verwendet, um Inhalte eindeutig einzuordnen, ohne kryptische Kürzel.

Beispiele für Titel:

- Prozesse:
  - „Prozess – Benutzeranlage im Active Directory“

    - „Prozess – Rechteänderung in Fachanwendungen“
- Richtlinien:
    - „Richtlinie – Passwortsicherheit“
    - „Richtlinie – Berechtigungsmanagement“
- Arbeitsanweisungen (SOP):
    - „Arbeitsanweisung – Benutzeranlage im Active Directory“
- Rollen:
    - „Rolle – Fachadministrator Active Directory“
    - „Rolle – Antragssteller Fachbereich“
- Systeme:
    - „System – Active Directory“
    - „System – Fachanwendung X“

Technische Kennungen (für Mapping/Automatisierung) werden im Hintergrund genutzt, z.B. als Feld im Dokument, Flowable-Key oder CISO-Custom-Feld:

- „Kennung: PR-Benutzeranlage-AD“
- „Kennung: RL-Passwortsicherheit“

Die Kennung wird im Kopfbereich der BookStack-Seite dokumentiert und identisch in Flowable und CISO Assistant wiederverwendet.

---

3. Struktur in BookStack

BookStack dient als zentrale Wissensbasis mit verständlichen Inhalten.

Struktur pro Kunde (Beispiel):

- Shelf: „Kunde <Name>“
    - Book: „Prozesse“
        - Seite: „Prozess – Benutzeranlage im Active Directory“
        - Seite: „Prozess – Rechteänderung in Fachanwendungen“
        - Seite: „Prozess – Regelmäßige Rechte-Reviews“
    - Book: „Systeme & Anwendungen“
        - Seite: „System – Active Directory“
        - Seite: „System – Fachanwendung X“
    - Book: „Rollen & Berechtigungen“
        - Seite: „Rolle – Rollenmodell Kunde <Name>“
        - Seite: „Rolle – Fachadministrator Active Directory“
    - Book: „Richtlinien & Arbeitsanweisungen“
        - Seite: „Richtlinie – Passwortsicherheit“
        - Seite: „Arbeitsanweisung – Benutzeranlage im Active Directory“

Inhaltlicher Aufbau einer Prozess-Seite (Beispiel „Prozess – Benutzeranlage im Active Directory“):

- Kopfbereich:
    - Kennung: PR-Benutzeranlage-AD
    - Version / Datum
    - Verantwortliche Rolle
- Kapitel:
    - Zweck und Geltungsbereich
    - Beteiligte Rollen
    - Auslöser und Inputs
    - Ablauf in Schritten (Kurzbeschreibung, kein BPMN)
    - Verweise:
        - zugehörige Arbeitsanweisung
        - Flowable-Workflow (Kennung/Name)
        - CISO-Asset / Kontrollen

4. Nutzung von Flowable

Flowable bildet die ausführbaren Workflows ab.

Für jeden relevanten Prozess:

- Process Name (sichtbar):
  - z.B. „Prozess – Benutzeranlage im Active Directory“
- Process Key (technische Kennung):
  - z.B. `PR-Benutzeranlage-AD`
- In der Prozessbeschreibung:
  - Hinweis auf die entsprechende BookStack-Seite:
    - „Siehe Prozessbeschreibung ‚Prozess – Benutzeranlage im Active Directory‘ in BookStack.“
- In User-Tasks:
  - Kurzbeschreibung des Schritts
  - Verweis auf die passende Arbeitsanweisung in BookStack, z.B.:
    - „Siehe ‚Arbeitsanweisung – Benutzeranlage im Active Directory‘.“

Regel:
Jeder Flowable-Prozess verweist mindestens auf eine Prozess-Seite und – falls vorhanden – eine Arbeitsanweisung in BookStack.

---

5. Nutzung von CISO Assistant

CISO Assistant ist das zentrale ISMS-/GRC-System.

Pro Kunde werden mindestens abgebildet:

- Assets, z.B.:
  - „Prozess – Benutzeranlage im Active Directory“ (Prozess-Asset)
  - „System – Active Directory“ (System-Asset)
- Risiken, z.B.:
  - „Risiko – Fehlende Vier-Augen-Prüfung bei Benutzeranlage“
- Kontrollen, z.B.:
  - „Kontrolle – Vier-Augen-Prinzip bei Benutzeranlage“

Zusätzliche Felder pro Objekt (Beispiele):

- `dokumentation_url`:
  - Link zur relevanten BookStack-Seite (Prozess, Richtlinie, Arbeitsanweisung).
- `workflow_kennung`:
  - Kennung des zugehörigen Flowable-Prozesses (z.B. `PR-Benutzeranlage-AD`).

Beispiel-Asset:

- Name: „Prozess – Benutzeranlage im Active Directory“
- Kennung: `PR-Benutzeranlage-AD`
- dokumentation_url: Verweis auf BookStack
- workflow_kennung: `PR-Benutzeranlage-AD`

So bleibt die Verbindung zwischen Dokumentation (BookStack), Ablauf (Flowable) und ISMS-Sicht (CISO Assistant) konsistent.

---

6. Nutzung von Wazuh

Wazuh liefert technische Sicherheitsinformationen.

Integration auf konzeptioneller Ebene:

- Relevante Findings (z.B. verdächtige Logons, fehlende Patches, Policy-Verstöße) werden in CISO Assistant als Risiken, Incidents oder Findings mit Bezug zu Assets erfasst.

Beispiele:

- Titel in CISO Assistant:
  - „Incident – Verdächtige Logons im System – Active Directory“
- Referenzen:
  - Quelle: Wazuh
  - Alert-ID
  - optional Link zum Wazuh-Dashboard

Diese Incidents oder Risiken können Flowable-Workflows anstoßen, z.B. einen Incident-Prozess oder einen Prozess für Notfall-Berechtigungsentzug.

---

7. Grundprinzipien für ein sauberes Gesamtbild

1. **Klare Verantwortlichkeiten pro System**
   - BookStack: lesbare Dokumentation und Handbuch.
   - Flowable: ausführbare Prozesse.
   - CISO Assistant: Risiko-, Kontroll-, Maßnahmen- und Auditverwaltung.
   - Wazuh: technische Sicherheitslage.
2. **Sprechende Titel mit ausgeschriebenen Präfixen**
   - Präfixe wie „Prozess – …“, „Richtlinie – …“, „Arbeitsanweisung – …“, „Rolle – …“, „System – …“ werden durchgängig verwendet.
3. **Technische Kennungen nur für Mapping**
   - Kurze Kennungen (z.B. `PR-Benutzeranlage-AD`) werden konsistent in allen Systemen genutzt, aber nicht als primäre Anzeige für Nutzer.
4. **Verknüpfung über Kennungen und Klartext-Verweise**
   - Verknüpfungen zwischen den Systemen erfolgen über einheitliche Kennungen und benannte Verweise, nicht über komplexe, starre Integrationen.

Prozesse

Prozesse

Prozessorganisation in Bookstack

Alles klar, dann passe ich nur den Teil „Struktur der Prozessorganisation“ so an, dass er explizit als Kapitel „Prozessorganisation in BookStack“ verwendbar ist.

Prozessorganisation in BookStack

1. Ziel der Prozessorganisation in BookStack

Die Prozessorganisation in BookStack stellt sicher, dass alle Prozesse, Rollen, Systeme, Richtlinien und Arbeitsanweisungen einheitlich strukturiert dokumentiert sind und sich schnell wiederfinden lassen.
BookStack dient dabei als zentrale, lesbare Wissensbasis, unabhängig von den ausführenden oder auswertenden Systemen.

---

2. Struktur in BookStack

Pro Kunde wird die Prozessorganisation in BookStack wie folgt abgebildet:

- Shelf: „Kunde <Name>“
  - Book: „Prozesse“
  - Book: „Systeme & Anwendungen“
  - Book: „Rollen & Berechtigungen“
  - Book: „Richtlinien & Arbeitsanweisungen“

Beispiele für Seitentitel:

- „Prozess – Benutzeranlage im Active Directory“
- „Prozess – Rechteänderung in Fachanwendungen“
- „System – Active Directory“
- „Rolle – Fachadministrator Active Directory“
- „Richtlinie – Passwortsicherheit“
- „Arbeitsanweisung – Benutzeranlage im Active Directory“

---

3. Kopfblöcke in Prozess? und Richtliniendokumenten

Jede Prozess-, Richtlinien- oder Arbeitsanweisungsseite bekommt oben einen standardisierten Kopfblock, zum Beispiel:

```
Kennung: PR-Benutzeranlage-AD
Reifegrad: Definiert
Prozessart: Unterstützungsprozess
Prozessverantwortlicher: Rolle – Fachadministrator Active Directory
Prozesseigner: Rolle – IT-Leitung
Betroffene Systeme: System – Active Directory
Beteiligte Rollen: Rolle – Antragssteller Fachbereich, Rolle – Fachadministrator Active
Directory
```

Für Richtlinien können Kopfblöcke z.B. enthalten:

```
Kennung: RL-Passwortsicherheit
Geltungsbereich: Gesamtunternehmen
Verbindlichkeit: Verpflichtend
Verantwortlich: Rolle – Informationssicherheitsbeauftragter
Betroffene Prozesse: Prozess – Benutzeranlage im Active Directory, Prozess – Rechteänderung in Fachanwendungen
```

Damit sind alle wichtigen Meta-Informationen für Leser sofort sichtbar.

---

4. Tags als Labels in BookStack

Zur maschinenlesbaren Kennzeichnung werden Tags verwendet.
Empfohlene Tag-Konventionen (jeweils „Name: Wert“):

- Reifegrad
  - `Reifegrad: Initial`
  - `Reifegrad: Definiert`
  - `Reifegrad: Etabliert`
  - `Reifegrad: Optimiert`
- Prozessart
  - `Prozessart: Managementprozess`
  - `Prozessart: Kernprozess`
  - `Prozessart: Unterstützungsprozess`
- Systeme
  - `System: Active Directory`
  - `System: Fachanwendung X`
- Rollen
  - `Rolle: Fachadministrator AD`
  - `Rolle: Antragssteller Fachbereich`

Diese Tags werden in BookStack auf Seitenebene vergeben.
Dadurch lassen sich z.B. alle Prozesse mit Reifegrad „Initial“ oder alle Seiten zum System „Active Directory“ filtern.

---

5. Templates für einheitliche Prozessdokumentation

Um Konsistenz sicherzustellen, werden in BookStack Seiten-Templates für Prozess-, Richtlinien- und Arbeitsanweisungsdokumente verwendet.

Beispiele:

- Template „Prozessbeschreibung“ mit:
  - Kopfblock (Kennung, Reifegrad, Prozessart, Verantwortliche, Systeme, Rollen)
  - Abschnittsüberschriften: Zweck, Anwendungsbereich, Rollen, Inputs/Outputs, Ablauf, Schnittstellen, Kennzahlen
- Template „Richtlinie“ mit:
  - Kopfblock (Kennung, Geltungsbereich, Verbindlichkeit, Verantwortliche Rolle, betroffene Prozesse)
  - Abschnittsüberschriften: Ziel, Geltungsbereich, Vorgaben, Ausnahmen, Durchsetzung, Überprüfung
- Template „Arbeitsanweisung“ mit:
  - Kopfblock (Kennung, zugehöriger Prozess, Zielgruppe, benötigte Systeme/Rollen)
  - Abschnittsüberschriften: Voraussetzungen, Schritt-für-Schritt-Anleitung, Hinweise, Kontrollpunkte

Die Templates werden in den jeweiligen Books als Standardvorlagen für neue Seiten eingestellt, sodass jede neue Prozess- oder Richtliniendokumentation automatisch dem gewünschten Aufbau folgt.

Prozesse

Prozessorganisation in Flowable

Hier das Flowable-Kapitel im selben Stil, damit du es direkt in deine Doku aufnehmen kannst.

Prozessorganisation in Flowable

1. Ziel der Prozessorganisation in Flowable

Die Prozessorganisation in Flowable stellt sicher, dass operativ gelebte Abläufe als ausführbare Workflows abgebildet werden, die direkt zu den in BookStack dokumentierten Prozessen passen.
Flowable dient als technische Umsetzungsschicht für Prozesse, inklusive Aufgabensteuerung, Genehmigungen, Eskalationen und Automatisierung.

---

2. Grundprinzipien für Prozesse in Flowable

- Jede fachlich dokumentierte Prozessbeschreibung in BookStack („Prozess – …“) hat, sofern nötig, eine passende technische Umsetzung in Flowable.
- Namen der Workflows sind für Fachanwender verständlich, technische Details (Keys, Variablen) werden im Hintergrund konsistent gehalten.
- Flowable verweist in Beschreibungen und Aufgaben eindeutig auf die zugehörigen Dokumente in BookStack (Prozessbeschreibung, Arbeitsanweisungen).

---

3. Benennung von Prozessen in Flowable

Für jeden relevanten Prozess werden zwei Bezeichnungen verwendet:

1. **Process Name (sichtbar für Anwender)**
   - entspricht dem lesbaren Titel aus BookStack
   - Beispiel:
     - „Prozess – Benutzeranlage im Active Directory“
2. **Process Key (technische Kennung)**
   - kompakte, eindeutige Kennung zur Wiederverwendung in anderen Systemen
   - orientiert sich an der Kennung im Kopfblock der BookStack-Seite
   - Beispiel:
     - Kennung in BookStack: `PR-Benutzeranlage-AD`
     - Process Key in Flowable: `PR-Benutzeranlage-AD`

Der Process Key wird nicht für Anwender kommuniziert, sondern dient der Integration (z.B. in CISO Assistant oder Skripten).

---

4. Struktur eines Flowable?Prozesses

Jeder Flowable-Prozess basiert fachlich auf der entsprechenden Prozessbeschreibung in BookStack.
Er enthält mindestens:

- Start-Ereignis (z.B. manueller Start, Formular, API-Call)
- eine Reihe von User-Tasks (für manuelle Schritte)
- Service-Tasks (für Automatisierungen, z.B. Anbindung an ein IAM-System)
- Gateways für Entscheidungen
- Endereignis(e) (z.B. erfolgreich abgeschlossen, abgelehnt, abgebrochen)

Der fachliche Ablauf (Schritte, Rollen, Entscheidungen) stammt aus der Prozessbeschreibung in BookStack.

5. Verweise von Flowable auf BookStack

In Flowable werden die Verknüpfungen zu BookStack an folgenden Stellen gepflegt:

- **Prozessbeschreibung (Properties des Prozesses)**
  - Textbeschreibung, die u.a. enthält:
    - „Siehe Prozessbeschreibung ‚Prozess – <Name>' in BookStack."
    - „Siehe Arbeitsanweisung ‚Arbeitsanweisung – <Name>' in BookStack."
- **User-Tasks**
  - Beschreibung/Titel des Tasks mit Hinweis auf relevante Arbeitsanweisungen, z.B.:
    - „Führe die Benutzeranlage gemäß ‚Arbeitsanweisung – Benutzeranlage im Active Directory' durch."

So bleibt für Bearbeiter klar, wo die inhaltlichen Details nachzulesen sind.

---

6. Rollen und Verantwortlichkeiten in Flowable

Flowable nutzt Benutzer, Gruppen und Rollen, um Aufgaben zuzuweisen:

- Gruppen/Role-Zuweisung orientiert sich an den Rollen, die in BookStack als „Rolle – …" beschrieben sind.
- Beispiel:
  - Rolle in BookStack: „Rolle – Fachadministrator Active Directory"
  - entsprechende Gruppe/Rolle in Flowable: `Fachadministrator_AD`

User-Tasks werden in Flowable nicht an konkrete Personen, sondern an Gruppen/Rollen zugewiesen; die Zuordnung von Personen zu Rollen erfolgt über die Identity-Verwaltung.

---

7. Verbindung von Flowable zur ISMS?Sicht (CISO Assistant)

Um Flowable mit dem ISMS zu verknüpfen, wird pro Prozess eine gemeinsame Kennung genutzt:

- Kennung in BookStack: `PR-Benutzeranlage-AD`
- Process Key in Flowable: `PR-Benutzeranlage-AD`
- Feld `workflow_kennung` in CISO Assistant: `PR-Benutzeranlage-AD`

CISO Assistant kann so z.B. in einem Prozess-Asset dokumentieren, welcher Flowable-Workflow diesen Prozess technisch abbildet.
Umgekehrt kann ein Flowable-Prozess in seiner Beschreibung auf das entsprechende Asset in CISO Assistant verweisen.

---

8. Typische Flowable?Prozessarten

Flowable wird insbesondere für folgende Prozessarten genutzt:

- Benutzer- und Berechtigungsmanagement
  - Benutzeranlage, Rechteänderung, Rechteentzug, Rezertifizierungsprozesse
- Sicherheits- und Incident-Prozesse
  - Reaktion auf Wazuh-Findings, Security-Incidents, Notfallprozesse
- Change- und Request-Prozesse
  - Changes an Anwendungen/Systemen, Service Requests aus Fachbereichen
- ISMS-bezogene Prozesse
  - Risiko-Bewertungen, Umsetzung von Maßnahmen, Durchführen von Kontrollen

Für jede dieser Prozessarten existiert eine Prozessbeschreibung in BookStack und eine dazu passende technische Umsetzung in Flowable.

---

9. Templates und Wiederverwendung in Flowable

Um einheitliche Prozessmodelle zu erreichen, können wiederkehrende Muster als Vorlage genutzt werden:

- Standard-Genehmigungsworkflow (Antrag – Prüfung – Genehmigung/Ablehnung)
- Standard-Rezertifizierungsworkflow (Start – Prüfung pro Berechtigung – Bestätigung/Entzug – Abschluss)
- Standard-Incident-Workflow (Erfassung – Klassifizierung – Bearbeitung – Abschluss)

Diese Muster werden als eigene Prozessdefinitionen oder Modellierungsrichtlinien bereitgestellt und bei Bedarf für neue Prozesse kopiert und angepasst.

---

10. Pflege und Reifegrad

- Für jeden Flowable-Prozess ist definiert, welcher Prozessverantwortliche (aus der Prozessbeschreibung in BookStack) fachlich zuständig ist.
- Technische Anpassungen (z.B. neue Schritte, geänderte Zuweisungen) werden mit diesem Prozessverantwortlichen abgestimmt.
- Der Reifegrad des Prozesses wird primär in der BookStack-Doku gepflegt; Änderungen im Flowable-Modell werden dort vermerkt (z.B. als neue Version der Prozessbeschreibung).

Prozesse

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.

Flyer - Integriertes ISMS- und Prozessmanagement

isms-bpm-doku-stack-flyer.pdf