

# Prozesse

- [Prozessorganisation in Bookstack](#)
- [Prozessorganisation in Flowable](#)
- [Informationssicherheits- und Compliance-Management \(ISMS/GRC\) mit CISO Assistent](#)

# 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. Kopfböcke 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 Kopfböcke 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.

# 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/Rolle-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).

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

## 1. Zweck von CISO Assistent

CISO Assistent 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 prüfbar, strukturierten ISMS.

---

## 2. Aufgaben von CISO Assistent

In der Gesamtarchitektur übernimmt CISO Assistent 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 Assistent verlinkt auf die lesbare Dokumentation in BookStack:

- Prozess-Assets in CISO Assistent (z.B. „Prozess – Benutzeranlage im Active Directory“) verweisen auf die entsprechende Prozessbeschreibung in BookStack.
  - Richtlinien- und Maßnahmenbeschreibungen in CISO Assistent 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 Assistent.
- 

## 4. Verbindung zu Flowable

CISO Assistent dokumentiert, welche Prozesse technisch umgesetzt sind:

- Prozess-Assets in CISO Assistent 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.