

Referenzarchitektur

- [Einführung in die Referenzarchitektur ISMS-BPM-Doku-Stack](#)
- [Referenzarchitektur ISMS-BPM-Doku-Stack \(CISO Assistant · Flowable · Wazuh · BookStack\)“](#)

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 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.