

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.
-

Revision #1

Created 2026-03-30 10:03:15 UTC by Gerd

Updated 2026-03-30 10:03:55 UTC by Gerd