COD GRC Module

Governance, Risk & Compliance on Living Data

Most GRC tools act as if infrastructure stood still: filled in once, half-heartedly maintained, months out of date. The gap between **real infrastructure** and **documented compliance** is the blind spot. The **COD GRC Module** works on the same living asset data as your operations and closes that gap. What started as an ISMS has grown into a fully-fledged **Governance, Risk & Compliance platform**.

At a glance: multi-standard GRC • **ISO/IEC 27001 & 27002, ISO 9001, ISO 22301** and **NIS2** • multi-standard SoA with a consolidated view • cases/incidents with site-specific SLAs • document control with two-person approval • asset-based risk assessment in line with BSI 200-3 • tamper-evident audit log • on-premise.

Multiple Standards, One Management System

A versioned catalogue maps **ISO/IEC 27001 & 27002, ISO 9001, ISO 22301** and the **NIS2 directive** as a hierarchical requirements tree. The **Statement of Applicability** is available per standard and as a global view that merges overlapping requirements into a single row carrying all standard tags. A **standards matrix widget** presents the integrated management system as topics × standards. NIS2 as demonstrable **readiness**, not a claim of conformity.

Cases, Incidents & Activities

Typed **cases** with a status machine, due dates and asset references: **incidents** with four severity levels and **site-specific SLA response times**. When personal data is affected, the **GDPR Art. 33 branch** with its 72-hour deadline opens automatically. The **activity tracker** manages operational follow-up as a list or Kanban board with a full change history.

Document Control with Two-Person Approval

All controlled documents are versioned in a store with a status machine (draft → published, revisions, restore). Approval enforces **segregation of duties**: owner approval and countersignature must come from different people. Exceptions appear only as an **audited admin override**. Plus an editable org chart, a central glossary and asset-based risk assessment in line with BSI 200-3.

Connectable & Auditable

Content comes in via **Markdown/DokuWiki import** and from **i-doit**. Odoo tickets are referenced **read-only**, and GRC API keys are tightly scoped. Embed **Mermaid diagrams** and the **live network topology** in documents. Reports go out as LaTeX-typeset PDFs. Every change is logged **append-only, protected against modification and deletion by DB triggers**.

GRC that knows what it protects. Compliance on living data. See COD live in your environment, no sales pressure.

extoco.de • extocode GmbH