COD GRC-Modul

Governance, Risk & Compliance auf lebenden Daten

Die meisten GRC-Werkzeuge tun so, als stünde Infrastruktur still: einmal befüllt, halbherzig gepflegt, mit Stand von vor Monaten. Die Lücke zwischen **realer Infrastruktur** und **dokumentierter Compliance** ist der blinde Fleck. Das **COD GRC-Modul** arbeitet auf denselben lebenden Asset-Daten wie Ihr Betrieb und schließt die Lücke. Aus dem früheren ISMS ist eine vollwertige **Governance-, Risk- & Compliance-Plattform** geworden.

Auf einen Blick: Multi-Norm-GRC • **ISO/IEC 27001 & 27002, ISO 9001, ISO 22301** und **NIS2** • Multi-Norm-SoA mit zusammengeführter Sicht • Vorgänge/Incidents mit standortbezogener SLA • Dokumentenlenkung mit Zwei-Personen-Freigabe • asset-basierte Risikobewertung nach BSI 200-3 • manipulationssicheres Audit-Log • On-Premise.

Mehrere Normen, ein Managementsystem

Ein versionierter Katalog bildet **ISO/IEC 27001 & 27002, ISO 9001, ISO 22301** und die **NIS2-Richtlinie** als hierarchischen Anforderungsbaum ab. Das **Statement of Applicability** gibt es je Norm und als globale Ansicht, die überlappende Anforderungen zu einer Zeile mit allen Norm-Tags zusammenführt. Ein **Norm-Matrix-Widget** stellt das integrierte Managementsystem als Themen × Normen dar. NIS2 als nachweisbare **Readiness**, nicht als Konformitätszusage.

Vorgänge, Incidents & Aktivitäten

Typisierte **Cases** mit Status-Maschine, Fälligkeiten und Asset-Bezug: **Incidents** mit vier Schweregraden und **standortbezogener SLA-Reaktionszeit**. Bei personenbezogenen Daten öffnet sich automatisch der **DSGVO-Art.-33-Zweig** mit 72-Stunden-Frist. Der **Aktivitäten-Tracker** führt das operative Follow-up als Liste oder Kanban-Board mit voller Änderungshistorie.

Dokumentenlenkung mit Zwei-Personen-Freigabe

Alle gelenkten Dokumente liegen versioniert in einem Store mit Status-Maschine (Entwurf → Veröffentlicht, Revisionen, Wiederherstellen). Die Freigabe erzwingt **Funktionstrennung**: Owner-Freigabe und Countersign müssen von verschiedenen Personen kommen, Ausnahmen erscheinen nur als **auditierter Admin-Override**. Dazu editierbares Org-Chart, zentrales Glossar und asset-basierte Risikobewertung nach BSI 200-3.

Anschlussfähig & prüfbar

Inhalte kommen per **Markdown-/DokuWiki-Import** und aus **i-doit** herein. Odoo-Tickets werden **read-only** referenziert, GRC-API-Keys sind eng gescoped. In Dokumente betten Sie **Mermaid-Diagramme** und die **Live-Netzwerk-Topologie** ein. Reports gehen als LaTeX-gesetzte PDFs raus. Jede Änderung wird **append-only, per DB-Trigger gegen Ändern und Löschen geschützt** protokolliert.

GRC, das weiß, was es schützt. Compliance auf lebenden Daten.
Sehen Sie COD live in Ihrer Umgebung, ohne Vertriebsdruck.

extoco.de • extocode GmbH