LAYERED ARCHITECTURE SOLUTION

Regulatory-Compliant Architecture: Business vs. Compliance

LAYER 3
REGULATORS/
AUDITORS

National Competent Authorities (KNF, CNB, MNB, BNR, ASF, etc.) / EBA / ECB / ESAs / GDPR DPAs

EU-wide DORA & GDPR enforcement alignment

Single source of truth expectation

Audit evidence & documentation

(Audit access **only to GRC)**

LAYER 2
GRC PLATFORM
(Independent Compliance Layer)

Independent from operations (required)
Policy library: DORA, GDPR, MiFID II / IDD, NIS 2, ESG (SFDR/CSRD)

Central risk & outsourcing registers (including third-party ICT providers)

GDPR artifacts — RoPA, DPIA, TIA repositories
Audit evidence store; Links to immutable archives

(OUR INTEGRATION LAYER - Custom Dev)

- ❏ APIs extract evidence from Salesforce
- ❏ Compliance metadata tagging
- ❏ Data transformation & formatting
- ❏ Real-time /batch sync

LAYER 1
OPERATIONAL SYSTEMS
(Business)

Salesforce FSC:
Data 360, KYC

Shield: Audit Trail, Event Monitoring

Integration Layer connects Salesforce to: Banking/Insurance (SAP, Avaloq);

Archive systems (OpenText, S3+Lock);

SIEM (Splunk, Sentinel)

BUSINESS USERS

KEY PRINCIPLE ✓ **Regulators interact ONLY with GRC layer** (not Salesforce) ✓ **GRC platform = independent compliance system of record** ✓ **Integration ensures evidence flows** from operations to oversight ✓ **Segregation of duties** satisfies **EU DORA and ECB independence requirements.**

Salesforce FSC runs the business, GRC platform demonstrates control. Our integration builds the trust bridge