LusoBank GRC Implementation Case Study

Overview:

This GRC simulation focuses on implementing an ISO/IEC 27001:2022-aligned Information Security Management System (ISMS) for LusoBank S.A., a fictional retail bank based in Portugal.

Objective:

To strengthen governance, manage cyber risks, and ensure compliance with key regulations:

- ISO/IEC 27001:2022
- GDPR (Portugal & EU)
- NIS2 Directive
- Banco de Portugal guidance
- EBA ICT security guidelines

Implementation Phases:

1. Policy Creation:

Developed a formal ISMS Policy, Security Objectives, and a governance model involving executive management.

2. Asset & Risk Analysis:

Created an Asset Register covering cloud and on-prem systems, SWIFT infrastructure, and customer data.

Identified key risks such as phishing attacks, insider threats, third-party risks, and system outages.

3. Risk Treatment:

Used a Risk Register to track risk ratings and apply controls like:

- MFA and RBAC

- Awareness training

- Data backup policies

- Vendor assessments

4. Compliance Mapping:

Mapped ISO/IEC 27001:2022 controls to current practices.

Included GDPR alignment for Articles 5, 25, 32, and 35 with references to the Data Protection Officer.

5. Dashboarding:

Developed a visual risk matrix showing treatment status, open risks, and overall security posture.

Outcome:

LusoBank now has a documented, auditable framework for cybersecurity governance.

It aligns with industry standards and positions the bank for successful audits and regulatory reviews.

Prepared by: GRC Analyst (Simulation Project)

Date: July 31, 2025