GRC Analyst Project: IT Governance Assessment Using COBIT Framework

As a Governance, Risk, and Compliance (GRC) Analyst, I was engaged by a medium-sized financial institution that was facing difficulties in aligning IT initiatives with its strategic business objectives. To address this challenge, I led a comprehensive IT governance assessment using the COBIT framework, aiming to evaluate governance maturity and drive stronger IT-business alignment.

1. Identifying Key Business Objectives

To begin, I conducted interviews with executive leadership, line-of-business managers, and IT stakeholders. I also reviewed the organization's strategic plan and operational KPIs. The following business objectives were prioritized:

- Strengthen digital banking services to improve customer engagement.
- Ensure compliance with financial regulations (e.g., GLBA, FFIEC).
- Improve IT service delivery and reduce operational downtime.
- Enhance data security and risk management practices.
- Optimize technology investment returns through better portfolio management.

Deliverable: A Business-IT Objectives Alignment Matrix, mapping strategic goals to IT functions and dependencies.

2. Assessing IT Governance with COBIT Domains

Using COBIT 2019's Governance and Management Objectives, I performed a structured assessment of the current IT governance state, focusing on five core domains:

EDM (Evaluate, Direct and Monitor)

- Identified limited executive oversight and lack of performance tracking on IT value delivery.
- Found that IT strategy was not formally reviewed against business goals.

APO (Align, Plan and Organize)

- IT lacked a formal enterprise architecture plan.

- No standardized approach for evaluating and prioritizing IT investments.

BAI (Build, Acquire and Implement)

- Projects were inconsistently managed, with frequent scope creep and delays.

- Change management processes were ad hoc.

DSS (Deliver, Service and Support)

- Found gaps in service level agreements (SLAs) and incident response planning.

- Business continuity procedures did not fully address IT dependencies.

MEA (Monitor, Evaluate and Assess)

- Compliance monitoring existed but was siloed and lacked integration into IT planning.

- Risk assessments were performed irregularly and not used in decision-making.

Deliverable: A COBIT Governance Maturity Heatmap illustrating strengths and areas for improvement (rated from Level 1 – Incomplete to Level 5 – Optimized).

3. Recommendations for IT-Business Alignment

I developed tailored recommendations to align IT strategy with business goals while improving governance maturity:

Governance Enhancements:

- Establish an IT Governance Board with executive oversight and cross-functional representation.

- Align IT performance metrics (KPIs) with business outcomes such as customer experience, service uptime, and compliance.

Strategic & Operational Improvements:

- Implement a Project Portfolio Management (PPM) process to prioritize IT projects based on business value.
- Introduce formal enterprise architecture planning to support scalable, secure systems.

Risk & Compliance Integration:

- Automate compliance tracking and align policies with COBIT's MEA objectives.
- Embed IT risk assessments into quarterly governance reviews.

Deliverable: A COBIT-Aligned Governance Roadmap with a phased implementation plan and recommended quick wins (e.g., create an IT value scorecard, formalize change management process).

4. Presentation to Senior Management

To communicate the findings and recommendations effectively, I created an executive-level presentation that included:

- A summary of business pain points and IT misalignments.
- The COBIT governance maturity heatmap and domain-level insights.
- Strategic governance recommendations linked to business benefits.
- A 12-month roadmap with milestones, responsible parties, and expected outcomes.

Deliverable: A concise and visual PowerPoint deck tailored for board-level review and buy-in.

Outcome

- The institution adopted my roadmap and formed a permanent IT Governance Committee.
- IT project delays were reduced by 30% through improved prioritization and accountability.
- Regulatory readiness improved through structured compliance integration.

- Executive leadership gained greater visibility and confidence in the IT function.