GRC Case Study (ISO/IEC 27001:2022)

Analyst: Samuel Jemal
Date: 31 October 2025
Role: SOC Analyst (Intern)

1. Executive Summary

The GRC (Governance, Risk, and Compliance) analysis, conducted on 31 October 2025, focused on ISO/IEC 27001:2022 implementation within a mid-sized enterprise environment. The goal was to assess compliance maturity, identify control gaps, and recommend actions for maintaining continuous alignment with information security standards.

2. Tools Used

- Splunk / ELK Stack – Log monitoring
- Wireshark – Network traffic inspection
- Sysmon – Endpoint event tracking
- MITRE ATT&CK; – Threat mapping

3. Findings

Control Area	Status	Recommendation
Access Control (A.9)	Partially Implemented	Introduce MFA for privileged accounts
Asset Management (A.8)	Compliant	Review quarterly asset inventory
Incident Management (A.16)	In Progress	Define escalation matrix and train staff
Risk Assessment (A.6)	Not Documented	Conduct annual risk assessment workshop

4. Recommendations

- Implement continuous monitoring dashboards for real-time visibility.
- Improve rule tuning for false positive reduction.
- Regularly train analysts on new detection methods.
- Adopt automation (SOAR) for faster alert triage.

5. Analyst Signature

Name: Samuel Jemal
Date: 31 October 2025
Role: SOC Analyst (Intern)