Cybersecurity Compliance

Provider: IBM (Coursera)
Completion Date: April 8, 2025

Overview

This course introduced the key frameworks, standards, and regulatory requirements that shape modern cybersecurity programs. It emphasized the importance of governance, risk, and compliance (GRC) in protecting organizations and ensuring accountability. Through real-world case studies and control frameworks, the course connected compliance obligations with practical security implementation.

Key Topics Covered

- Governance, risk, and compliance (GRC) fundamentals
- Security frameworks: NIST Cybersecurity Framework, ISO/IEC 27001, and COBIT
- Industry-specific regulations: HIPAA, GDPR, PCI DSS, SOX
- Risk assessment, impact analysis, and mitigation strategies
- Security policies, procedures, and internal controls
- Audits, continuous monitoring, and reporting requirements
- Legal considerations: privacy law, intellectual property, and breach notification

Practical Applications

- Building policies and standards aligned with regulatory frameworks
- Conducting compliance gap assessments and audits
- Applying risk assessment methods to prioritize controls
- Mapping organizational processes to compliance obligations
- Communicating compliance requirements across technical and non-technical teams

Personal Reflection

This course strengthened my ability to connect legal and regulatory requirements with technical security practices. I developed confidence in interpreting frameworks, evaluating compliance risks, and supporting audits. These skills directly align with my career focus in GRC, where ensuring both accountability and security is essential.