GRC and Compliance Framework Summary

Summary of Major Cybersecurity Governance and Compliance Frameworks

Prepared by: Beryl Amondi Opara

NIST (National Institute of Standards and Technology)

The NIST Cybersecurity Framework (CSF) provides organizations with a structured approach to managing and reducing cybersecurity risk. It is built around five core functions: Identify, Protect, Detect, Respond, and Recover. NIST emphasizes continuous improvement and is widely used across government and private sectors.

ISO/IEC 27001

ISO 27001 is an international standard for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). It focuses on risk assessment, control implementation, and management commitment to maintaining confidentiality, integrity, and availability of data.

GDPR (General Data Protection Regulation)

GDPR is the European Union's regulation on data privacy and protection. It enforces strict guidelines on how organizations handle personal data, ensuring transparency, accountability, and consent from individuals. Key principles include data minimization, lawful processing, and the right to be forgotten.

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA is a U.S. regulation that protects the privacy and security of healthcare information. It mandates safeguards for electronic protected health information (ePHI), including administrative, physical, and technical controls to ensure patient data confidentiality and integrity.

COBIT (Control Objectives for Information and Related Technologies)

COBIT provides a governance framework that helps organizations manage and align IT goals with business objectives. It focuses on risk management, performance measurement, and process control, ensuring IT delivers value while maintaining compliance.

PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS applies to organizations that handle cardholder data. It sets security standards for processing, storing, and transmitting credit card information, requiring strong access controls, network monitoring, encryption, and regular vulnerability assessments.

This summary highlights the core principles of key cybersecurity governance and compliance frameworks. Each framework plays a vital role in ensuring organizations maintain data security,

privacy, and regulatory alignment.