Cybersecurity Compliance & Regulation Cheatsheet

A quick reference guide to navigating cybersecurity compliance and regulations, covering key frameworks, laws, and best practices to help organizations maintain a strong security posture and avoid penalties.

Key Compliance Frameworks

NIST Cybersecurity Framework (CSF)

Description: A voluntary framework primarily for US-based organizations to manage and reduce cybersecurity risks based on business needs and resources.

Key Functions:

- **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Benefits: Risk-based approach, adaptable to various organization sizes and industries, promotes a common language for cybersecurity risk management.

ISO 27001

Description: An international standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).

Key Components:

- Risk Assessment: Identify, analyze, and evaluate information security risks.
- Risk Treatment: Select and implement appropriate risk mitigation measures.
- Continual Improvement: Regularly monitor, review, and improve the ISMS.

Benefits: Globally recognized, provides a structured approach to information security, enhances credibility and trust with stakeholders.

SOC 2

Description: A reporting framework developed by the AICPA for service organizations to demonstrate controls over security, availability, processing integrity, confidentiality, and privacy of customer data.

Trust Services Criteria:

- Security: Protection of information and systems.
- Availability: System availability for operation and use.
- Processing Integrity: System processing is complete, accurate, timely, and authorized.
- Confidentiality: Protection of confidential information.
- Privacy: Handling of personal information.

Benefits: Demonstrates strong data protection practices to customers, particularly important for SaaS providers and cloud-based services.

Key Cybersecurity Regulations

GDPR (General Data Protection Regulation)

Description: European Union (EU) law on data protection and privacy for all individuals within the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA.

Key Requirements:

- Lawful basis for processing personal data (e.g., consent, contract).
- Data minimization: Collect only necessary data.
- Purpose limitation: Process data only for specified purposes.
- Data security: Implement appropriate technical and organizational measures.
- Data subject rights: Right to access, rectify, erase, restrict processing, data portability, and object.

Penalties: Up to €20 million or 4% of annual global turnover, whichever is higher.

CCPA/CPRA (California Consumer Privacy Act/California Privacy Rights Act)

Description: California state law that grants consumers various rights over their personal information, including the right to know, the right to delete, and the right to opt-out of the sale of their personal information.

Key Requirements:

- Transparency: Provide clear notice about data collection practices.
- Consumer rights: Honor consumer requests to access, delete, and opt-out of sale.
- Data security: Implement reasonable security measures to protect personal information.

Penalties: Up to $7,500 per violation.

HIPAA (Health Insurance Portability and Accountability Act)

Description: US law that provides data privacy and security provisions for safeguarding medical information.

Key Components:

- Privacy Rule: Protects individuals' medical records and other personal health information.
- Security Rule: Requires covered entities to implement administrative, physical, and technical safeguards to protect electronic protected health information (ePHI).
- Breach Notification Rule: Requires covered entities to notify affected individuals, HHS, and the media in the event of a breach of unsecured ePHI.

Penalties: Vary based on the severity and extent of the violation, ranging from $100 to $50,000 per violation, with a maximum penalty of $1.5 million per year for each violation category.

Essential Cybersecurity Practices for Compliance

Risk Management

Conduct Regular Risk Assessments: Identify, analyze, and evaluate potential threats and vulnerabilities to your organization's assets and data.

Implement Risk Mitigation Measures: Develop and implement controls to reduce the likelihood and impact of identified risks, such as security policies, procedures, and technologies.

Monitor and Review Risks: Continuously monitor and review your risk management program to ensure its effectiveness and adapt to changing threats and business needs.

Data Security

Implement Data Encryption: Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.

Control Access to Data: Implement strong access controls to limit access to sensitive data to authorized personnel only.

Regularly Back Up Data: Back up data regularly and store backups in a secure location to ensure data availability in the event of a disaster or security incident.

Data Loss Prevention (DLP): Deploy DLP solutions to prevent sensitive data from leaving the organization's control.

Incident Response

Develop an Incident Response Plan: Create a comprehensive plan that outlines the steps to take in the event of a security incident, including identification, containment, eradication, recovery, and lessons learned.

Test and Update the Plan Regularly: Conduct regular tabletop exercises and simulations to test the effectiveness of the incident response plan and update it as needed.

Establish Reporting Procedures: Define clear reporting procedures for employees to report suspected security incidents.

Maintaining Compliance

Documentation

Maintain Accurate Records: Keep detailed records of all security policies, procedures, risk assessments, incident responses, and compliance activities.

Document Changes: Document any changes to your security controls or processes to maintain an audit trail and ensure accountability.

Retention Policies: Implement data retention policies to adhere to legal and regulatory requirements.

Training and Awareness

Conduct Regular Security Awareness Training: Provide ongoing training to employees on cybersecurity best practices, phishing awareness, and data protection.

Role-Based Training: Tailor training programs to specific roles and responsibilities within the organization.

Testing and Evaluation: Test employee knowledge through quizzes and simulations to measure the effectiveness of the training program.

Audits and Assessments

Conduct Regular Internal Audits: Perform internal audits to assess the effectiveness of your security controls and identify areas for improvement.

Engage External Auditors: Engage external auditors to conduct independent assessments of your compliance with relevant regulations and frameworks.

Address Audit Findings: Develop and implement corrective action plans to address any findings from internal or external audits.