Cybersecurity Governance, Risk and Compliance

Mini-Capstone Project

Nguyen Duong

1. Common Security-Control Requirements Across HIPAA, PCI-DSS, and SOC2/SOC3

a. Firewall Implementation

Description: Firewalls serve as a barrier between trusted internal networks and untrusted external networks, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.

Risks of Non-Implementation: Without firewalls, systems are vulnerable to unauthorized access, malware, and data breaches.

Penalty:

- HIPAA: Fines range from $100 to $50,000 per violation, with a maximum annual penalty of $1.5 million.
- PCI-DSS: Non-compliance may lead to penalties from $5,000 to $100,000 per month and revocation of payment processing privileges.
- SOC2: Failure to implement firewalls may result in a qualified or adverse audit opinion.

Implementation Benefits:

- Blocks unauthorized access and filters harmful traffic.
- Enforces internal usage rules and access controls.
- Logs activity and sends alerts for suspicious behavior.
- Supports regulatory adherence and provides audit evidence.

Legal Issues:

- Failing to use firewalls may be seen as negligence in a breach.
- Increases risk of fines and regulatory actions.
- Breaches may require public disclosure, harming reputation.

Cloud Considerations:

- Use security groups or cloud-native firewalls to manage cloud traffic.
- Poorly set rules can expose services to the internet.
- Isolates critical systems within cloud environments.
- Easily scales and integrates with cloud automation and monitoring tools.

b. Access Control Mechanisms

Description: Access controls ensure that only authorized individuals can access specific systems and data.

Risks of Non-Implementation: Can result in insider threats, unauthorized data access, and breaches.

Penalty Clauses:

- HIPAA: Penalties similar to firewall violations.
- PCI-DSS: Fines and increased scrutiny.
- SOC2: Negative audit outcomes and reputational damage.

Implementation Benefits: Ensures accountability and supports least privilege principles.

Legal Issues: Failure to restrict access can violate confidentiality and data protection laws.

Cloud Considerations: Use Identity and Access Management (IAM) to enforce access policies in the cloud.

c. Encryption of Data at Rest and in Transit

Description: Converts data into a coded format unreadable without decryption keys.

Risks of Non-Implementation: Data may be intercepted or stolen during transmission or while stored.

Penalty Clauses:

- HIPAA: Unencrypted PHI breaches can lead to mandatory notifications and fines.
- PCI-DSS: Storing unencrypted cardholder data is a direct violation.
- SOC2: Encryption is essential for data privacy assurance.

Implementation Benefits:

- Restricts access to sensitive data, minimizing exposure.
- Tracks user actions and enforces responsibility.
- Ensures users access only what they need to perform their duties.
- Simplifies compliance and audit reporting.

Legal Issues:

- Uncontrolled access may breach HIPAA, GDPR, or CCPA.
- It can result in lawsuits, fines, and regulatory penalties if sensitive data is exposed.

Cloud Considerations:

- Use cloud-native tools like AWS IAM or Azure AD to assign and enforce permissions.

- Define detailed access policies by service, action, and resource.
  Review IAM logs regularly to detect unusual activity or access patterns.

d. Regular Security Audits and Monitoring

Description: Involves periodic assessment of systems for vulnerabilities and compliance adherence.

Risks of Non-Implementation: Vulnerabilities may go undetected and be exploited.

Penalty Clauses:

- HIPAA: Risk assessments are mandatory and audited.
- PCI-DSS: Regular system testing is required.
- SOC2: Audits are essential for trust principles.

Implementation Benefits:

- Identifies and mitigates security gaps early.
- Improves system visibility and strengthens security posture.
- Demonstrates compliance during external audits.
- Enables trend analysis to support proactive defense strategies.

Legal Issues:

- Lack of monitoring may be considered negligence if a breach occurs.
- Failure to audit regularly can result in legal actions and fines under regulatory frameworks.

Cloud Considerations:

- Use services like AWS CloudTrail, Azure Monitor, or GCP Logging for continuous tracking.
- Integrate logs into SIEM tools for centralized monitoring.
- Automate compliance reporting to ensure visibility and accountability.

e. Incident Response Planning

Description: Defines how organizations detect, respond to, and recover from security incidents.

Risks of Non-Implementation: Delay in response increases data loss and operational impact.

Penalty Clauses:

- HIPAA: Late breach notifications attract larger fines.
- PCI-DSS: Incident response plans must be tested.
- SOC2: Incident management is a core requirement.

Implementation Benefits:

- Reduces the duration and scope of security incidents.
- Ensure clear roles and communication during a crisis.
- Builds customer and partner confidence through preparedness.
- Help meet regulatory and contractual obligations.

Legal Issues:

- Inadequate or undocumented incident handling may result in non-compliance penalties.
- Organizations can face lawsuits or loss of business for failing to protect sensitive data.

Cloud Considerations:

- Design response workflows that integrate cloud service provider procedures.
- Use automated alerts and playbooks for fast cloud-specific response.
- Maintain logs and evidence from cloud platforms for forensic analysis.

2. Common Data Requirements Across HIPAA, PCI-DSS, and SOC2/SOC3

a. Personally Identifiable Information (PII)

Frameworks: HIPAA, SOC2/SOC3
Data Fields:

- Full name
- Social Security Number (SSN)
- Driver's license or ID number
- Date of birth
- Address
- Email and phone number

Justification: PII is critical because it can be exploited for identity theft, fraud, and social engineering attacks. SOC2 includes it under the privacy trust principle, while HIPAA considers any PII linked to health records as Protected Health Information (PHI).

b. Protected Health Information (PHI)

Frameworks: HIPAA
Data Fields:

- Medical records
- Health insurance information

- Treatment history
- Biometric identifiers

Justification: HIPAA mandates strong safeguards for PHI. Even basic identifiers become PHI when linked to health conditions. Breaches involving PHI require public breach notification and can incur severe penalties.

c. Payment Card Information (PCI)

Frameworks: PCI-DSS
Data Fields:

- Primary Account Number (PAN)
- Cardholder name
- Expiration date
- CVV and service code

Justification: PCI-DSS defines how merchants and processors must handle credit card data securely. Improper storage or transmission of this information can lead to financial fraud, heavy fines, and loss of payment processing privileges.

3. Risk Register: Definition, Use, and Tool Comparison

A Risk Register is a centralized repository used to systematically document and manage risks within an organization. It typically includes critical elements such as a detailed description of each risk, its likelihood of occurrence, potential impact, assigned owner, mitigation strategies, and status tracking. The primary purpose of a risk register is to ensure that risks are captured, assessed, monitored, and treated in a transparent and consistent manner.

Usage of Risk Register

- Identify and classify risks according to their source, category, or impact area (e.g., operational, cybersecurity, regulatory).
- Assign ownership and accountability to specific individuals or teams responsible for managing the risk.
- Prioritize risks based on a scoring system (e.g., risk matrix) to guide the allocation of resources and define treatment plans.
- Support compliance and audit readiness by providing traceable documentation of risk management activities for regulators and auditors.

GRC Significance

- Continuous compliance by documenting evolving risks and control measures aligned with regulatory standards.

- Strategic IT governance through proactive decision making aligns with business objectives.
- Risk visibility across departments, enabling enterprise-wide collaboration and breaking down silos in risk management efforts.

Tool Comparison: SimpleRisk and Open Source Risk Engine

Feature	SimpleRisk	Open Source Risk Engine (ORE)
Purpose	GRC and IT security compliance	Quantitative enterprise risk modeling
Interface	Web-based dashboard	Technical, code-heavy interface
Customization	High with plugin support	Limited, needs programming skills
Reporting	Rich with graphs and export options	Analytics-focused, not visual
Integration	Integrates with SIEMs and ticketing	Limited third-party integrations
Best Fit	Mid-to-large businesses, IT risk	Financial services, modeling-heavy

4. Risk Assessments Using ORE

Top 10 Vulnerabilities (May 2023 – April 2024)

CVE	Description	Impact	Rating
CVE-2023-34362	MOVEit Transfer SQL Injection flaw allowing unauthorized access and data theft.	Affected 2,700+ organizations and 93.3M individuals.	Critical
CVE-2024-3272	RCE vulnerabilities in D-Link NAS due to default admin accounts with no password.	Impacts 92,000+ global devices; enables remote control.	Critical
CVE-2024-27348	Apache HugeGraph-Server flaw enabling unauthenticated remote code execution.	Allows attackers full system access.	Critical
CVE-2024-49138	Windows CLFS driver vulnerability allowing local privilege escalation.	Grants attackers system-level privileges.	Critical

CVE-2024-2883	Use-after-free vulnerability in Chrome’s ANGLE component exploitable via malicious content.	Enables remote arbitrary code execution.	High
CVE-2024-22252	VMware USB controller flaw allowing guest-to-host code execution.	Compromises host from guest VMs.	High
CVE-2024-23225	iOS kernel memory protection bypass vulnerabilities.	Bypasses memory protections to gain kernel access.	High
CVE-2024-20337	Cisco Secure Client SAML injection leading to session hijacking.	Enables unauthorized access via injection attack.	High
CVE-2024-22127	SAP NetWeaver AS Java code injection flaw.	Compromises confidentiality, integrity, and availability.	High
CVE-2024-21334	Microsoft Open Management Infrastructure RCE vulnerability.	Remote code execution without authentication.	High

Top 10 Compliance Risks

Risk ID	Description	Compliance Area	Impact	Rating
R1	Failure to conduct periodic risk assessments.	HIPAA	Leads to undetected vulnerabilities and compliance gaps.	High
R2	Delayed data breach notifications (beyond 60-day rule).	HIPAA	Increases penalties, causes legal and reputational harm.	High
R3	Insufficient access controls to PHI.	HIPAA	Allows unauthorized access and data exposure.	High
R4	Storing cardholder data without encryption.	PCI-DSS	Increases risk of theft, fraud, and brand damage.	High

R5	Using weak or default authentication credentials.	PCI-DSS	Easily exploited by attackers to gain system access.	High
R6	Lack of regular vulnerability testing and scanning.	PCI-DSS	Leaves known vulnerabilities unpatched.	High
R7	No continuous monitoring of systems and logs.	SOC2	Delays incident detection and response.	High
R8	No documented or tested incident response plan.	SOC2	Causes confusion and delayed reaction during breaches.	High
R9	Poor data backup practices or absence of backup validation.	SOC2	Leads to irreversible data loss during incidents.	High
R10	No mandatory employee cybersecurity awareness training.	SOC2	Increases human errors and phishing susceptibility.	High

Risk Management Metrics

Metric Name	Definition	Justification
Mean Time to Detect	Average time taken to identify a security incident.	Shorter MTTD enables quicker containment of threats.
Mean Time to Respond	Average time taken to respond after detection.	Faster MTTR reduces damage and recovery costs.
Patch Management Efficiency	% of systems patched within policy time after a release.	Ensures vulnerabilities are fixed quickly.
Compliance Audit Success Rate	% of audits passed without significant findings.	Indicates maturity of compliance practices.
User Access Review Frequency	Regularity of reviewing user roles and access privileges.	Prevents excessive permissions and enforces least privilege.

Incident Recurrence Rate	How often the same type of incident reoccurs.	Measures the effectiveness of remediation and root-cause analysis.
Risk Exposure Score	Calculated score for potential loss per risk event.	Supports prioritization based on impact.
Training Completion Rate	% of employees who completed security training.	Reduces risk from human error and phishing.
Unpatched Vulnerability Count	Number of high/critical vulnerabilities not patched.	Identifies current exposure to known risks.
Data Backup Success Rate	% of successful backups over total scheduled backups.	Ensures business continuity and recovery capability.

5. References

- Folorunso, A., Wada, I., Samuel, B., & Mohammed, V. (2024). Security compliance and its implication for cybersecurity. World Journal of Advanced Research and Reviews.
- Mohammed, D. (2015). Cybersecurity compliance in the financial sector. Journal of Internet Banking and Commerce.
- National Institute of Standards and Technology. (2024). National Vulnerability Database. U.S. Department of Commerce.
- SimpleRisk. (2024). GRC Platform Documentation.
- GoodFirms. (2024). Best Open-Source Risk Management Tools Survey.