Rick Abraham

My Company  Dallas, TX

Risk Assessment – Compliance Risks

Contents

[Introduction 2](#_Toc182584971)

[Purpose 2](#_Toc182584972)

[Scope 2](#_Toc182584973)

[Risk Identification 2](#_Toc182584974)

[Risk Analysis 3](#_Toc182584975)

[Mitigation Recommendations 3](#_Toc182584976)

[Employee Laptops 3](#_Toc182584977)

[Mobile Devices 3](#_Toc182584978)

[IoT Devices 4](#_Toc182584979)

[Unregistered Devices 4](#_Toc182584980)

[Wearables 4](#_Toc182584981)

[Monitoring and Review 4](#_Toc182584982)

[Frequency 4](#_Toc182584983)

[Daily 4](#_Toc182584984)

[Monthly 4](#_Toc182584985)

[Quarterly 4](#_Toc182584986)

[Bi-Annually 5](#_Toc182584987)

[Annually 5](#_Toc182584988)

[Incident Response 5](#_Toc182584989)

[Documentation and Compliance 5](#_Toc182584990)

Risk Assessment – Compliance Risks

# Introduction

Purpose: This risk assessment evaluates vulnerabilities and threats associated with non-compliance to regulatory frameworks (e.g., GDPR, HIPAA, PCI DSS) and industry standards (e.g., ISO 27001, NIST SP 800-53). It identifies risks, their impacts, and provides mitigation strategies to ensure legal and regulatory obligations are met.

Scope: Covers all organizational processes, systems, and third-party engagements that are subject to compliance requirements.

# Risk Identification

| **Asset** | **Threat** | **Vulnerability** | **Impact** | **Risk Rating** |
| --- | --- | --- | --- | --- |
| Personal Data (PII) | Unauthorized access or mishandling of personal data | Lack of encryption or access control | Fines, legal penalties, reputational damage | High |
| Payment Data (PCI) | Breach of credit card or payment information | Inadequate adherence to PCI DSS standards | Fraud, financial losses, compliance violations | High |
| Medical Data (PHI) | Non-compliance with HIPAA requirements | Unsecured storage or transmission of sensitive health data | Legal penalties, patient trust issues | High |
| Third-Party Processes | Vendors failing to meet contractual compliance terms | Lack of vendor risk assessments | Legal penalties, supply chain disruptions | Medium |
| Audit and Reporting | Failure to maintain accurate logs for audits | Insufficient logging or documentation | Regulatory non-compliance, operational fines | Medium |

# Risk Analysis

| **Asset** | **Likelihood** | **Impact Severity** | **Overall Risk Level** |
| --- | --- | --- | --- |
| Personal Data (PII) | High | High | Critical |
| Payment Data (PCI) | Medium | High | High |
| Medical Data (PHI) | Medium | High | High |
| Third-Party Processes | Medium | Medium | Moderate |
| Audit and Reporting | Medium | Medium | Moderate |

# Mitigation Recommendations

## Personal Data (PII)

* Encrypt all sensitive personal data at rest and in transit using strong encryption protocols (e.g., AES-256).
* Implement access control policies to restrict access to PII to authorized personnel only.
* Conduct regular training for employees on handling PII in compliance with GDPR and CCPA regulations.

## Payment Data (PCI)

* Enforce PCI DSS compliance by implementing secure payment gateways and regularly auditing payment systems.
* Deploy network segmentation to isolate payment systems from non-sensitive systems.
* Perform quarterly vulnerability scans and annual penetration tests on payment systems.

## Medical Data (PHI)

* Ensure compliance with HIPAA by encrypting all health-related data and securing access logs for auditability.
* Conduct regular risk assessments of systems handling PHI to identify gaps in compliance.
* Require Business Associate Agreements (BAAs) with third parties that process or store PHI.

## Third-Party Processes

* Perform vendor risk assessments before onboarding and regularly audit third-party compliance certifications.
* Include compliance clauses in vendor contracts, with penalties for non-compliance.
* Use continuous monitoring tools to track vendor activities related to sensitive data.

## Audit and Reporting

* Implement robust logging mechanisms to capture user activities, access events, and system changes.
* Automate compliance reporting to ensure timely submission to regulators and internal stakeholders.
* Maintain audit trails for at least the minimum period required by applicable regulations (e.g., GDPR, SOX).

# Monitoring and Review

Frequency

### Daily

* Monitor access logs for PII, PHI, and payment data to detect unauthorized activities.
* Validate alerts from security tools to ensure they align with regulatory requirements.

### Monthly

* Audit compliance with access control policies and ensure encryption is enabled across all sensitive data repositories.
* Review third-party reports and certifications to verify ongoing adherence to compliance standards.

### Quarterly

* Conduct internal compliance audits to ensure adherence to GDPR, HIPAA, PCI DSS, and other applicable regulations.
* Review audit logs for anomalies and ensure secure storage for audit trails.
* Test the effectiveness of compliance controls using simulated data handling exercises.

### Bi-Annually

* Perform regulatory readiness drills, focusing on GDPR, HIPAA, or PCI DSS-specific scenarios.
* Evaluate the effectiveness of compliance-related tools (e.g., DLP, access control systems) through simulations.

### Annually

* Reassess compliance risks based on new regulatory requirements, industry standards, or internal process changes.
* Update compliance policies and employee training programs to reflect changes in regulatory expectations.
* Conduct a compliance awareness campaign to educate employees and stakeholders about regulatory obligations.

Incident Response

* Establish a Compliance Incident Response Team (CIRT) trained to address violations and data breaches.
* Conduct annual response drills, focusing on regulatory breach notification requirements.
* Document all compliance-related incidents, including root causes, remediation actions, and regulatory reports.

Documentation and Compliance

* Maintain detailed logs of compliance activities, including audits, training, and vendor assessments.
* Document updates to policies, access controls, and encryption mechanisms to demonstrate continuous improvement.
* Ensure compliance with applicable regulations and standards, including:
  + NIST SP 800-53: AC-17 (Remote Access), SI-4 (Monitoring), and AU-12 (Audit Generation).
  + GDPR, HIPAA, PCI DSS, and ISO 27001 for specific data protection and audit requirements.