CandiClie Intern Assignment Report

Data Security, Incident Response, Compliance & Vulnerability Assessment

Pseudo-Report

Report For: SolviTech Solutions

Author: Aryan Parashar

aryanmayoor@gmail.com

Introduction to SolviTech Solutions

Solvitech Solutions operates several pieces of sensitive information pertaining to IT, HR, digital marketing, and business consulting. This includes personally identifiable information: details about the clients, records of employees, and application data of applicants. The Company also processes the payment and financial details of the customers, including but not limited to credit card number, invoices, and transaction history. Further, proprietary business information belonging to the Clients or jointly owned with the Company, comprising business strategy, intellectual property, and other confidential reports, is also handled. Solvitech has digital marketing data, project deliverables, and cloud-hosted data that are managed for clients; these include database and access tokens. The most critical risks are data breaches, insider threats, phishing attacks, and compliance violations. Consequences may be in the form of identity theft, fraud, and non-compliance, such as under the GDPR, PCI-DSS, and HIPAA.

Important Compliance Audits for SolviTech

{Checklists Available on Gdrive}

Link: Supplementary Material (Click Here)

1. ISO/IEC 27001 Audit Checklist for SolviTech Solutions
2. ISO 27017 Audit Checklist for SolviTech Solutions
3. GDPR Audit Checklist for SolviTech Solutions
4. PCI DSS Audit Checklist for SolviTech Solutions
5. SOC 2 Audit Checklist for SolviTech Solutions
6. Indian PDPB 2019 Audit Checklist for SolviTech Solutions
7. Indian ITA 2000 Audit Checklist for SolviTech Solutions
8. CCPA Audit Checklist for SolviTech Solutions
9. NIST Data Security Framework Audit Checklist for SolviTech Solutions

Audit Results – **Non-conformities**

(Based upon Commonly Found Missing Parameters)

1. ISO/IEC 27001 Audit Negations

1.1. Uncontrolled Documentation of ISMS
1.2. Lack of Comprehensive Risk Assessment
1.3. Weak Incident Response (IRP) and Business Continuity Plan(BCP)
1.4. Inadequate Encryption
1.5. Neglected Patch Management Processes
1.6. Untimely VAPT and Audits

2. ISO 27017 Audit Negations

2.1. Unclear cloud roles and responsibilities
2.2. Weak cloud access control
2.3. Inconsistent monitoring and logging
2.4. Lack of cloud incident response plan

3. GDPR Audit Negations

3.1. Insufficient data subject consent
3.2. Unlawful data transfers
3.3. Inadequate data breach response
3.4. Failure to maintain Record of Processing Activities (RoPA)

4. PCI DSS Audit Negations

4.1. Unencrypted payment data
4.2. Weak access controls
4.3. Lack of vulnerability management program
4.4. No two-factor authentication (2FA)

5. SOC 2 Audit Negations

5.1. Unclear security policies
5.2. Inconsistent system monitoring
5.3. Lack of change management process
5.4. No user access reviews

6. Indian PDPB 2019 Audit Negations

6.1. No user consent mechanism
6.2. Non-compliance with data localization
6.3. No grievance redressal mechanism
6.4. Insecure processing of sensitive data

7. Indian ITA 2000 Audit Negations

7.1. Non-compliance with data security standards
7.2. Unreported data breaches
7.3. Lack of IT Act compliance awareness

8. CCPA Audit Checklist Negations

8.1. Failure to honor consumer rights
8.2. No privacy policy disclosures
8.3. Non-compliance with "Do Not Sell" requests
8.4. Incomplete data inventory

9. NIST Data Security Framework Audit Negations

9.1. Lack of risk assessment process
9.2. Weak identity and access management
9.3. Incomplete incident response plan
9.4. No continuous monitoring

Vulnerability Assessment and Threat Vectors

1. Unencrypted Payment Data (PCI DSS)

1.1. **Impact:** High – Exposes sensitive payment information, leading to potential financial fraud and reputational damage.

1.2. **Likelihood:** High – Given the rise in cyber-attacks targeting financial data.

1.3. Mitigation Steps:

1.3.1. Implement end-to-end encryption for all payment data.

1.3.2. Ensure Payment Card Industry (PCI) standards are strictly followed.

1.3.3. Regularly audit and test encryption protocols for potential weaknesses.

2. Weak Access Controls (SOC 2, PCI DSS, ISO 27017)

2.1. **Impact**: High – Inadequate access controls can lead to unauthorized data access, internal fraud, or cyber-attacks.

2.2. **Likelihood:** Medium – Without robust identity management, this vulnerability is a common point of exploitation.

2.3. Mitigation Steps:

2.3.1. Implement role-based access controls (RBAC) across systems.

2.3.2. Deploy two-factor authentication (2FA) for all sensitive accounts.

2.3.3. Regularly review and audit user access permissions to critical systems.

3. Insufficient Incident Response Plan (ISO 27017, NIST)

3.1. **Impact:** High – Lack of a formal response could delay containment and recovery, exacerbating a breach's impact.

3.2. **Likelihood:** Medium – Incident occurrence is likely, especially if preventative measures aren't in place.

3.3. Mitigation Steps:

3.3.1. Develop and document a comprehensive incident response plan (IRP).

3.3.2. Conduct regular incident response drills and simulations.

3.3.3. Establish a clear reporting and escalation process for incidents.

4. Failure to Honor Consumer Rights (GDPR, CCPA)

4.1. **Impact:** High – Non-compliance can result in severe legal penalties, especially for violations involving personal data.

4.2. **Likelihood:** High – With strict privacy regulations, violations could easily occur due to oversight or system limitations.

4.3. Mitigation Steps:

4.3.1. Ensure systems are in place to handle data access, deletion, and opt-out requests from consumers.

4.3.2. Regularly update privacy policies to reflect current practices.

4.3.3. Perform internal audits to verify compliance with GDPR and CCPA requirements.

5. Unreported Data Breaches (Indian ITA 2000, PDPB 2019)

5.1. **Impact:** High – Failure to report breaches can lead to heavy fines, loss of trust, and further regulatory action.

5.2. **Likelihood**: Medium – Likely due to inadequate monitoring and breach detection systems.

5.3. Mitigation Steps:

5.3.1. Implement breach detection and monitoring systems.

5.3.2. Establish clear guidelines for breach reporting and notification to authorities.

5.3.3. Conduct regular security awareness training to help identify potential breaches early.

6. Lack of Risk Assessment Process (NIST)

6.1. **Impact:** Medium – Inadequate risk assessment could result in failure to identify and mitigate emerging threats.

6.2. **Likelihood:** Medium – Without proper assessment, vulnerabilities can accumulate over time.

6.3. Mitigation Steps:

6.3.1. Conduct regular risk assessments following NIST guidelines.

6.3.2. Utilize vulnerability scanning tools to regularly evaluate system security.

6.3.3. Develop a risk management framework and assign responsibilities to key staff.

7. Inadequate Cloud Security Measures (ISO 27017)

7.1. **Impact:** High – Weak cloud security can lead to data leaks, unauthorized access, and compliance violations.

7.2. **Likelihood**: Medium – Increasing use of cloud services raises the risk without adequate controls.

7.3. Mitigation Steps:

7.3.1. Implement strong encryption and multi-factor authentication for cloud access.

7.3.2. Ensure proper logging and monitoring of cloud-based systems.

7.3.3. Review and update cloud security policies regularly, particularly regarding shared responsibility.

8. Non-compliance with Data Localization (PDPB 2019)

8.1. **Impact**: Medium – Can lead to regulatory fines and legal penalties.

8.2. **Likelihood:** Low – Less likely if the company doesn't handle large-scale cross-border data transfers.

8.3. Mitigation Steps:

8.3.1. Implement localized data storage solutions in compliance with local laws.

8.3.2. Ensure all data storage and processing adheres to regional requirements.

8.3.3. Establish partnerships with compliant data centers within required jurisdictions.

Data Security Implementation Plan

In order to improve data security, reduce potential hazards, and resolve the vulnerabilities found in the audit results, the following thorough implementation strategy is suggested:

1. Data Encryption and Secure Communication Channels

1.1. **Objective:** Ensure that sensitive data is kept encrypted both at rest and in transit to avoid unauthorized access and breaches.

1.2. Recommendations :

1.2.1. **End-to-End Encryption:** Encrypt all sensitive data using Industry-standard algorithms like AES 256 for encryption of data at rest and TLS 1.3 or above for data in transit. The encryption requirements for the payment-related data must be aligned with the requirements set by the PCI-DSS on encryption.

1.2.2. **Secure Communication Channels:** Encryption of SSL or TLS for all communications, both internal and external parts. The VPN must be implemented to allow remote access to the sensitive systems; this ensures that employees working offsite can have encrypted and secure connections.

1.2.3. **Key Management:** This includes best practices related to encryption key management, like the rotation of keys periodically and the storing of keys in a secure hardware security module.

2. Access Control and User Authentication

2.1. **Goal:** Limit access to confidential data only to persons with due authorization and enhance mechanisms related to user authentication.

2.2. Best Practices:

2.2.1. **Role-Based Access Control (RBAC**): RBAC would ensure that only those users explicitly permitted to have access to certain data are the ones allowed. This makes sure that an employee can only access data needed for a particular function or role. This reduces the insider threat within an organization. Review and audit roles periodically and perform updates to ensure permissions remain appropriate as roles change over time.

2.2.2. **Multi-Factor Authentication**: Enforce MFA on all systems, especially for those accounts with privileged access or that have access to sensitive data. Enact MFA for all remote access solutions, including VPN and cloud platforms, since passwords would create a single point of failure.

2.2.3. **Password Policies:** Enforce strong password policies that require passwords to meet complexity requirements for length, special characters, and numbers. Implement password expiration and rotation policies that require users to update passwords regularly. Consider the use of passwordless authentication methods, such as biometrics or security tokens, wherever viable for improved security.

3. Periodic Security Audits along with Staff Training

3.1. **Objective:** The security posture shall be kept proactive through continuous monitoring, auditing, and awareness programs.

3.2. Recommendations:

3.2.1. **Periodic Security Audits:** Ensure periodic security audits are carried out quarterly or annually to identify new vulnerabilities that further mitigate them. Tools to be used for this are vulnerability scanners, penetration testing, and compliance checks (ISO 27001, GDPR, PCI DSS). Implement continuous monitoring tools and provide real-time threat detection and incident response through tools such as the Security Incident and Event Monitoring system to immediately mitigate any emerging risk.

3.2.2. **Data Backup and Recovery Drills**: Establish enterprise-wide automatic backups of sensitive data. Such backups must be retained within highly secured and encrypted environments, both locally on-site and remotely off-site. This will help them conduct disaster recovery drills, allowing them to realize quick recovery of systems and data following a breach or incident resulting in data loss.

3.2.3. **Employee Awareness and Training**: By implementing a security awareness training for all employees highly focused on Phishing and social engineering prevention.

3.2.4. **Proper management of sensitive information**, including its disposal and encryption.

3.2.5. **Incident reporting process:** Phishing simulation on a regular basis to increase the ability of employees to identify cyber threats.

4. Incident Response and Breach Management

4.1. **Objective:** To have a well-structured framework in place for the detection, response, and recovery of security incidents.

4.2. Recommendations:

4.2.1. **Incident Response Plan:** Formulate and implement an IRP-a written plan for detailing the activities to be performed when there is a breach or cyber attack. Identify key persons with responsibilities and a communication plan to be used to notify stakeholders, clients, and regulatory authorities in case of a data breach.

4.2.2. **Data Breach Notification:** Comply with breach notification obligations issues about relevant regulations like GDPR, CCPA, and ITA 2000. Generally, disclose the breach to the affected persons concerned and the relevant regulator within the prescribed time limit.

4.2.3. **Post-Incident Activity:** After an incident, a proper post-incident activity for determining root causes and making the defenses better should be done. Update the incident response plan based on lessons learned.

5. Continuous Compliance and Governance

5.1. Objective: Security controls to be aligned with Industry Regulations and Best Practices

5.2. Recommendations:

5.2.1. **Compliance Management:** Review and update the security policy from time to time to make them compliant with ever-evolving standards such as ISO 27001, PCI DSS, GDPR, etc. Use automated compliance management software to achieve this task of continuous monitoring and compliance with regulatory requirements.

5.2.2. **Data Classification:** Apply a data classification scheme to identify sensitive data, such as confidential/restricted. This further extends control with regard to access and handling of information at high risk.

Incident Response Checklist Playbook and Summary

[NIST Framework]

For the purpose of managing cybersecurity risks, including incident response, the National Institute of Standards and Technology (NIST) Cybersecurity Framework offers an organized method. The reaction aligns with the key tasks of NIST, which are Detect, Respond, Identify, Protect, and Recover.

1. Immediate Actions (Respond & Detect)

A. Detect and Analyze the Breach (Detect)

- Use security monitoring tools (SIEM, IDS/IPS) to identify suspicious activity or breaches.
- Analyze log data, alerts, and system reports to confirm the breach and determine its scope.
- Identify affected systems and compromised data (e.g., PII, payment information, business data).

B. Contain the Breach (Respond)

- Implement containment measures to limit the damage, such as disconnecting compromised systems.
- Use network segmentation or firewall rules to stop further lateral movement of attackers.
- Disable affected accounts or privileges if the breach involves credential compromise.

C. Preserve Evidence (Respond)

- Preserve system logs, security alerts, and relevant files for forensic investigation.
- Avoid modifying the affected systems to ensure proper evidence collection.
- Secure digital copies of all communications, alerts, and changes made during the incident.

---

2. Communication Protocols (Respond)

A. Internal Notification (Respond)

- Alert the Incident Response Team (IRT) and key stakeholders (IT, Legal, Management).
- Assign clear roles for handling the breach, including technical remediation and communication.

B. Regulatory and Legal Compliance (Respond)

- Notify regulatory authorities within the required time frame (e.g., GDPR 72-hour rule).
- Ensure compliance with data breach laws applicable to the company's industry or geography (e.g., HIPAA, PCI DSS).

C. External Communication (Respond)

- Communicate with affected clients, partners, and vendors, providing them with accurate information about the breach and how it may impact them.
- Share recommended actions (e.g., password resets, fraud monitoring) to mitigate further damage.
- Prepare a public statement if required, ensuring transparency and responsibility are emphasized.

---

3. Long-Term Recovery Strategies (Recover & Protect)

A. Remediation (Recover)

- Identify the root cause of the breach and immediately address vulnerabilities (e.g., patching systems, updating configurations, reviewing network access).
- Remove malicious code or backdoors installed by attackers and confirm systems are secure.
- Strengthen access control mechanisms by enforcing least privilege, multi-factor authentication (MFA), and role-based access control (RBAC).

B. Post-Incident Analysis (Recover)

- Conduct a comprehensive forensic analysis to understand how the breach occurred, the extent of the impact, and the timeline of events.
- Document the attack vector, methods used, and any missed detection points.
- Update the incident response plan based on lessons learned to improve future responses.

C. Monitoring and Continuous Improvement (Identify & Detect)

- Implement enhanced monitoring systems for real-time detection of suspicious activity.
- Conduct regular audits and vulnerability scans to identify and mitigate new threats.
- Utilize automated security solutions (e.g., IDS, EDR) for continuous monitoring and threat detection.

---

4. Long-Term Data Security (Protect & Recover)

A. Strengthening Security Policies and Training (Protect)

- Conduct regular employee training on phishing prevention, secure data handling, and recognizing suspicious activity.
- Update and enforce the company's data protection and incident response policies in line with industry best practices.

B. Improving Detection Capabilities (Detect)

- Implement advanced detection tools like Security Information and Event Management (SIEM) systems to detect anomalies and breaches.
- Use Endpoint Detection and Response (EDR) tools to continuously monitor endpoint activities and automatically respond to detected threats.

C. Recovery and Business Continuity Planning (Recover)

- Ensure robust backup and disaster recovery plans are in place, regularly tested, and include isolated backups.
- Perform a post-breach review of the business continuity plan, ensuring that critical operations can continue during recovery.
- Focus on long-term monitoring and patch management to ensure all systems are secured against similar future attacks.

✓ Mapping the NIST Framework:

Identify: Critical asset identification, integration of threat intelligence, and routine assessments.
Safeguard: Robust encryption, restricted access, and education.
Detect: Endpoint security, SIEM, and real-time monitoring.
React: Containment, regulatory communication, and incident reaction strategies.
Recover: Plans for cleanup, forensic examination, and recovery.

SolviTech Solutions may minimize harm and guarantee a speedy recovery by managing a data breach with organized and effective procedures by following the NIST framework.