COLLECTION OF CYBERSECURITY ASSESSMENT REPORT TEMPLATES WITH EXAMPLES AND SIMULATIONS

**BY IZZMIER IZZUDDIN**

## LIST OF COMMON CYBERSECURITY ASSESSMENTS

1. **Vulnerability Assessment**: Identiﬁes and evaluates security vulnerabilities in systems, applications, and networks. Tools like Nessus, Ǫualys, and OpenVAS are often used.
2. **Penetration Testing**: Simulates real-world attacks to ﬁnd and exploit vulnerabilities in systems. It helps in understanding the eFectiveness of existing security measures. Tools include Metasploit and Burp Suite.
3. **Risk Assessment**: Analyses potential risks to an organisation’s information assets, including likelihood and impact. It involves identifying critical assets, assessing threats, and determining vulnerabilities.
4. **Security Audit**: A comprehensive review of an organisation’s security policies, procedures, and controls to ensure compliance with standards and regulations. It often involves examining logs, documentation, and conﬁgurations.
5. **Compliance Assessment**: Evaluates adherence to regulatory requirements and industry standards such as GDPR, HIPAA, or PCI-DSS. It ensures that policies and controls meet legal and industry-speciﬁc standards.

**EXAMPLES AND SIMULATIONS**



# VULNERABILITY ASSESSMENT REPORT – DE LIGT SOLUTION

## PREPARED BY IZZMIER IZZUDDIN

### Table of Contents

1. **Executive Summary**

### Scope of Work

1. **Assessment Methodology**

### Summary of Findings

1. **Detailed Findings**

### Risk Assessment

1. **Recommendations**

### Conclusion

1. **Appendices**

### Executive Summary

The vulnerability assessment conducted for De Ligt Solutions identiﬁed several security gaps within the organisation’s infrastructure. This report outlines the vulnerabilities discovered and provides recommendations to mitigate the associated risks.

### Key Findings:

* + **Critical Vulnerabilities:** 3

### High-Risk Vulnerabilities: 4

* + **Medium-Risk Vulnerabilities:** 7

### Low-Risk Vulnerabilities: 12

The assessment uncovered critical vulnerabilities that could be exploited by attackers to gain unauthorised access to sensitive systems and data.

### Scope of Work Objectives:

* + Identify vulnerabilities in the external and internal network of De Ligt Solutions.
  + Evaluate the security posture of web applications and internal servers.
  + Provide actionable recommendations to mitigate identiﬁed risks.

### In-Scope Assets:

* + **External Network:** 203.0.113.1 - 203.0.113.50
  + **Internal Network:** 10.0.0.1 - 10.0.0.200
  + **Web Applications:** [www.deligtsolutions.com,](http://www.deligtsolutions.com/) intranet.deligtsolutions.com
  + **Databases:** SǪL Server, MongoDB

### Out-of-Scope:

* + Physical security assessments
  + Social engineering attacks on employees

### Assessment Methodology

The vulnerability assessment followed these steps:

1. **Reconnaissance:** Passive and active information gathering.
2. **Vulnerability Scanning:** Automated scanning using tools like Nessus, OpenVAS, and Nexpose.
3. **Manual Veriﬁcation:** Manual testing to conﬁrm vulnerabilities.
4. **Risk Analysis:** Evaluating the impact and likelihood of each vulnerability.
5. **Reporting:** Documenting the ﬁndings and providing remediation steps.

### Summary of Findings Critical Vulnerabilities:

* 1. **Remote Code Execution in Web Application**
     + **Description:** A critical ﬂaw was found in the web application that allows remote attackers to execute arbitrary code.
     + **Impact:** Potential full control over the application server.
     + **Recommendation:** Apply security patches immediately.

### SǪL Injection on Login Page

* + - **Description:** The login page of the internal web portal is vulnerable to SǪL injection.
    - **Impact:** Unauthorised access to sensitive user credentials.
    - **Recommendation:** Implement input validation and parameterised queries.

### Unrestricted File Upload

* + - **Description:** The web application allows unrestricted ﬁle uploads without proper validation.
    - **Impact:** Potential upload of malicious ﬁles leading to server compromise.
    - **Recommendation:** Restrict ﬁle types and implement proper validation.

### High-Risk Vulnerabilities:

1. **Outdated SSL/TLS Protocols**
   * **Description:** The external web application uses outdated SSL/TLS protocols.
   * **Impact:** Increased risk of man-in-the-middle attacks.
   * **Recommendation:** Upgrade to the latest SSL/TLS protocols.

### Weak Passwords in User Accounts

* + **Description:** Several user accounts have weak passwords.
  + **Impact:** Increased risk of brute-force attacks.
  + **Recommendation:** Enforce strong password policies.

### Detailed Findings

* 1. **Remote Code Execution in Web Application**
     + **Vulnerability ID:** ABC-VULN-001
     + **Severity:** Critical
     + **A\ected System:** Web Application Server (203.0.113.25)
     + **Impact:** Full server compromise
     + **Recommendation:** Apply the latest security patches and review code for potential ﬂaws.

### SǪL Injection on Login Page

* + - **Vulnerability ID:** ABC-VULN-002
    - **Severity:** Critical
    - **A\ected System:** Internal Web Portal (10.0.0.15)
    - **Impact:** Unauthorised access to user credentials
    - **Recommendation:** Implement parameterised queries and input validation.

### Risk Assessment

The risk assessment matrix for identiﬁed vulnerabilities:

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability** | **Risk Level** | **Impact** | **Likelihood** |
| Remote Code Execution | Critical | High | High |
| SǪL Injection | Critical | High | High |
| Outdated SSL/TLS Protocols | High | Medium | Medium |
| Weak Passwords | High | Medium | Medium |
| ... | ... | ... | ... |

### Recommendations

* 1. **Patch Management:**
     + Ensure all systems are updated with the latest security patches.

### Password Policies:

* + - Enforce strong password policies, including the use of MFA.

### Web Application Security:

* + - Regularly review code and implement secure coding practices.

### SSL/TLS Upgrades:

* + - Upgrade to the latest SSL/TLS protocols and conﬁgurations.

### File Upload Restrictions:

* + - Implement strict validation and restrictions on ﬁle uploads.

### Conclusion

The vulnerability assessment has highlighted several critical and high-risk vulnerabilities within De Ligt Solutions' infrastructure. Immediate action is required to mitigate these risks and improve the overall security posture.

### Appendices

* **Appendix A:** Vulnerability Scanning Results
* **Appendix B:** Risk Assessment Methodology
* **Appendix C:** Tools Used for Assessment



# PENETRATION TESTING ASSESSMENT REPORT – MARTINEZ CORPORATION

## PREPARED BY IZZMIER IZZUDDIN

### Table of Contents

* 1. **Executive Summary**

### Scope of Work

* 1. **Methodology**

### Findings

* 1. **Risk Assessment**

### Recommendations

* 1. **Conclusion**

### Appendices

1. **Executive Summary**

The penetration test conducted for Martinez Corporation was aimed at identifying potential vulnerabilities in the company's external and internal networks. The test simulated real-world attacks to assess the eFectiveness of existing security controls.

### Key Findings:

* + **Critical Vulnerabilities:** 2

### High-Risk Vulnerabilities: 5

* + **Medium-Risk Vulnerabilities:** 8

### Low-Risk Vulnerabilities: 10

The overall security posture of Martinez Corporation is moderate, with several high-risk vulnerabilities that require immediate attention.

### Scope of Work Objectives:

* + Assess the security of Martinez Corporation’s external and internal networks.
  + Identify and exploit vulnerabilities to gain unauthorised access.
  + Evaluate the eFectiveness of existing security measures.

### In-Scope Targets:

* + **External IPs:** 192.168.1.1 - 192.168.1.50
  + **Internal Network:** 10.0.0.1 - 10.0.0.100
  + **Web Applications:** [www.martinezcorporation.com,](http://www.martinezcorporation.com/) portal.martinezcorporation.com

### Out-of-Scope:

* + Denial of Service (DoS) attacks
  + Social engineering attacks on employees

### Methodology

The penetration testing was conducted using the following phases:

1. **Reconnaissance:** Information gathering using tools like Nmap, Maltego, and Shodan.
2. **Scanning:** Network and port scanning to identify live hosts and open ports.
3. **Exploitation:** Attempting to exploit identiﬁed vulnerabilities using tools such as Metasploit and Burp Suite.
4. **Post-Exploitation:** Assessing the extent of compromise and the ability to maintain access.
5. **Reporting:** Documenting ﬁndings, risks, and recommendations.

### Findings

**Critical Vulnerabilities:**

### SǪL Injection in Web Application Portal

* + - **Description:** The portal was vulnerable to SǪL Injection attacks, allowing unauthorised access to the database.
    - **Impact:** Full database compromise, including sensitive customer information.

### Exploitability: High

* + - **Recommendation:** Implement parameterised queries and input validation.

### Unpatched Remote Code Execution (RCE) Vulnerability

* + - **Description:** An unpatched RCE vulnerability in the internal server allowed remote attackers to execute arbitrary code.
    - **Impact:** Full control over the aFected server.

### Exploitability: High

* + - **Recommendation:** Apply the latest security patches.

### High-Risk Vulnerabilities:

1. **Weak Password Policies**
   * **Description:** Several user accounts were identiﬁed with weak passwords.
   * **Impact:** Increased risk of brute-force attacks.
   * **Exploitability:** Medium
   * **Recommendation:** Enforce strong password policies.

### Open Ports Without Proper Filtering

* + **Description:** Open ports on internal servers without proper ﬁltering mechanisms.
  + **Impact:** Potential entry points for attackers.
  + **Exploitability:** Medium
  + **Recommendation:** Implement strict ﬁrewall rules.

### Risk Assessment

The risk assessment for the identiﬁed vulnerabilities is categorised as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability** | **Risk Level** | **Impact** | **Exploitability** |
| SǪL Injection | Critical | High | High |
| Unpatched RCE | Critical | High | High |
| Weak Password Policies | High | Medium | Medium |
| Open Ports | High | Medium | Medium |
| ... | ... | ... | ... |

### Recommendations

* 1. **Patch Management:**
     + Regularly update all systems and apply the latest security patches.

### Password Policies:

* + - Enforce strong password policies and multi-factor authentication (MFA).

### Network Segmentation:

* + - Segment the network to limit the spread of attacks.

### Security Awareness Training:

* + - Conduct regular security awareness training for employees.

### Web Application Security:

* + - Implement secure coding practices and regular code reviews.

### Conclusion

The penetration test revealed critical and high-risk vulnerabilities that need immediate remediation. Implementing the recommended security measures will signiﬁcantly enhance the security posture of Martinez Corporation.

### Appendices

* **Appendix A:** Detailed Vulnerability Descriptions
* **Appendix B:** Tools and Techniques Used
* **Appendix C:** Raw Scan Data



# RISK ASSESSMENT REPORT – DALOT HEALTHCARE SERVICES

## PREPARED BY IZZMIER IZZUDDIN

### Table of Contents

* 1. **Executive Summary**

### Assessment Scope

* 1. **Assessment Methodology**

### Risk Identiﬁcation

* 1. **Risk Analysis**

### Risk Evaluation

* 1. **Risk Treatment Recommendations**

### Conclusion

* 1. **Appendices**

### Executive Summary

This risk assessment was conducted for Dalot Healthcare Services to identify potential threats, vulnerabilities, and the associated risks to the organisation's critical assets. The assessment aimed to provide a clear understanding of the risk landscape and oFer actionable recommendations to mitigate identiﬁed risks.

### Key Findings:

* + **High-Risk Areas:** 4

### Medium-Risk Areas: 5

* + **Low-Risk Areas:** 6

The assessment uncovered signiﬁcant risks related to data security, network vulnerabilities, and compliance with healthcare regulations.

### Assessment Scope Objectives:

* + Identify potential threats and vulnerabilities to ABC Healthcare Services' critical assets.
  + Analyse the impact and likelihood of identiﬁed risks.
  + Provide recommendations to mitigate or transfer risks.

### In-Scope Assets:

* + **Electronic Health Record (EHR) System**

### Medical Devices Network

* + **Patient Data Storage Systems**

### Network Infrastructure

* + **Email Communication Systems**
  + **Compliance Areas:** HIPAA, GDPR, HITECH

### Out-of-Scope:

* + Physical security of on-site data centres
  + Non-critical legacy systems

### Assessment Methodology

The risk assessment followed a structured approach, including:

1. **Risk Identiﬁcation:** Identifying potential threats and vulnerabilities.
2. **Risk Analysis:** Evaluating the likelihood and impact of each identiﬁed risk.
3. **Risk Evaluation:** Prioritising risks based on their severity.
4. **Risk Treatment:** Recommending mitigation strategies to reduce or transfer risks.

### Risk Identiﬁcation

* 1. **Identiﬁed Threats:**
     + **Cyber Attacks:** Targeted attacks on the EHR system and network infrastructure.
     + **Data Breaches:** Unauthorised access to sensitive patient information.
     + **Insider Threats:** Malicious or accidental actions by employees leading to data loss or breaches.
     + **Regulatory Non-Compliance:** Failure to comply with HIPAA, GDPR, or HITECH regulations.

### Identiﬁed Vulnerabilities:

* + - **Unpatched Software:** Critical systems running outdated and unpatched software.
    - **Weak Access Controls:** Inadequate access control mechanisms for sensitive data.
    - **Lack of Encryption:** Unencrypted data at rest and in transit.
    - **Insu\icient Employee Training:** Lack of security awareness training for staF.

### Risk Analysis

The identiﬁed risks were analysed based on their likelihood and impact:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk ID** | **Risk Description** | **Likelihood** | **Impact** | **Risk Level** |
| R-001 | Unpatched EHR System Vulnerability | High | High | High |
| R-002 | Unencrypted Patient Data | Medium | High | High |
| R-003 | Phishing Attacks on Email System | High | Medium | Medium |
| R-004 | Insider Threat from Lack of Employee Training | Medium | Medium | Medium |
| R-005 | Regulatory Non-Compliance (HIPAA) | Low | High | Medium |
| R-006 | Outdated Medical Device Firmware | Medium | High | High |
| R-007 | Inadequate Network Segmentation | High | Medium | Medium |
| R-008 | Lack of Multi-Factor Authentication (MFA) | High | High | High |

### Risk Evaluation Risk Prioritisation:

The risks were prioritised based on their risk levels, with high-risk areas requiring immediate attention.

### High-Risk Areas:

1. **Unpatched EHR System Vulnerability (R-001)**

### Unencrypted Patient Data (R-002)

1. **Outdated Medical Device Firmware (R-006)**

### Lack of Multi-Factor Authentication (MFA) (R-008) Medium-Risk Areas:

1. **Phishing Attacks on Email System (R-003)**

### Insider Threat from Lack of Employee Training (R-004)

1. **Regulatory Non-Compliance (HIPAA) (R-005)**

### Inadequate Network Segmentation (R-007) Low-Risk Areas:

* Risks that have been identiﬁed as low priority but still need to be monitored regularly.

### Risk Treatment Recommendations High-Risk Areas:

1. **Unpatched EHR System Vulnerability (R-001):**
   * **Recommendation:** Implement a regular patch management process to ensure all systems are up-to-date.
   * **Timeline:** Immediate (1-2 weeks)

### Unencrypted Patient Data (R-002):

* + **Recommendation:** Encrypt all patient data at rest and in transit using strong encryption protocols.
  + **Timeline:** High Priority (2-4 weeks)

### Outdated Medical Device Firmware (R-006):

* + **Recommendation:** Regularly update ﬁrmware on all medical devices and ensure compatibility with security protocols.
  + **Timeline:** Immediate (1-2 weeks)

### Lack of Multi-Factor Authentication (MFA) (R-008):

* + **Recommendation:** Implement MFA across all critical systems, especially for administrative access.
  + **Timeline:** High Priority (2-4 weeks)

### Medium-Risk Areas:

1. **Phishing Attacks on Email System (R-003):**
   * **Recommendation:** Implement email ﬁltering and security awareness training for employees.
   * **Timeline:** Medium Priority (4-6 weeks)

### Insider Threat from Lack of Employee Training (R-004):

* + **Recommendation:** Develop and conduct regular security awareness training for all employees.
  + **Timeline:** Medium Priority (4-6 weeks)

### Regulatory Non-Compliance (HIPAA) (R-005):

* + **Recommendation:** Review and update compliance policies, and conduct regular audits.
  + **Timeline:** Medium Priority (4-6 weeks)

### Inadequate Network Segmentation (R-007):

* + **Recommendation:** Implement proper network segmentation to isolate critical systems from less secure areas.
  + **Timeline:** Medium Priority (4-6 weeks)

### Conclusion

The risk assessment has highlighted several critical areas that require immediate attention. By implementing the recommended risk treatment strategies, Dalot Healthcare Services can signiﬁcantly reduce its risk exposure and ensure compliance with relevant regulations.

### Appendices

* **Appendix A:** Risk Assessment Checklist
* **Appendix B:** Compliance Matrix
* **Appendix C:** Tools and Techniques Used



# SECURITY AUDIT REPORT – SERVICES SHAW FINANCIAL SERVICES

## PREPARED BY IZZMIER IZZUDDIN

### Table of Contents

1. **Executive Summary**

### Audit Scope

1. **Audit Methodology**

### Summary of Findings

1. **Detailed Findings**

### Compliance Review

1. **Risk Analysis**

### Recommendations

1. **Conclusion**

### Appendices

1. **Executive Summary**

The security audit for Shaw Financial Services was conducted to evaluate the organisation's adherence to industry best practices and compliance with relevant regulations. The audit uncovered several areas that require immediate attention to strengthen the overall security posture and ensure compliance with standards like ISO 27001 and PCI-DSS.

### Key Findings:

* + **Non-compliance Issues:** 5

### High-Risk Areas: 3

* + **Medium-Risk Areas:** 6

### Low-Risk Areas: 9

The audit revealed gaps in access control, data encryption, and incident response processes.

### Audit Scope Objectives:

* + Assess the security controls in place to protect sensitive ﬁnancial data.
  + Evaluate compliance with ISO 27001, PCI-DSS, and other relevant standards.
  + Identify gaps and recommend corrective actions to address identiﬁed risks.

### In-Scope Assets:

* + **Data Centres:** Main Data Centre, Backup Data Centre
  + **Network Infrastructure:** Firewalls, Routers, Switches
  + **Critical Systems:** Core Banking System, Payment Processing System
  + **Endpoints:** Employee Workstations, Laptops
  + **Applications:** Online Banking Portal, Internal CRM
  + **Compliance Areas:** Access Control, Data Encryption, Incident Response

### Out-of-Scope:

* + Physical security at branch locations
  + Non-critical legacy systems

### Audit Methodology

The audit was conducted in the following phases:

1. **Planning:** Understanding the scope, objectives, and necessary resources for the audit.
2. **Pre-Audit Information Gathering:** Collecting policies, procedures, and previous audit reports.
3. **Audit Execution:** On-site inspections, interviews with key personnel, and review of technical controls.
4. **Testing and Validation:** Simulating potential attacks, vulnerability scanning, and policy reviews.
5. **Reporting:** Documenting ﬁndings, risks, and recommendations.

### Summary of Findings High-Risk Areas:

* 1. **Lack of Multi-Factor Authentication (MFA) for Online Banking Portal**
     + **Impact:** Increased risk of unauthorised access to customer accounts.
     + **Recommendation:** Implement MFA for all customer and administrative access.

### Unencrypted Sensitive Data

* + - **Impact:** Exposure of sensitive ﬁnancial data in case of a breach.
    - **Recommendation:** Encrypt all sensitive data both at rest and in transit.

### Insu\icient Incident Response Plan

* + - **Impact:** Delayed response to security incidents, leading to potential data breaches.
    - **Recommendation:** Develop and implement a comprehensive incident response plan.

### Medium-Risk Areas:

1. **Outdated Firewall Rules**
   * **Impact:** Increased risk of network breaches.
   * **Recommendation:** Regularly review and update ﬁrewall rules.

### Weak Password Policies

* + **Impact:** Increased likelihood of successful brute-force attacks.
  + **Recommendation:** Enforce strong password policies and implement password expiration.

### Detailed Findings

* 1. **Lack of Multi-Factor Authentication (MFA)**
     + **Finding ID:** ABC-AUDIT-001
     + **Severity:** High
     + **Description:** The online banking portal does not require MFA, exposing it to potential unauthorised access.
     + **Impact:** Unauthorised access to customer accounts could lead to signiﬁcant ﬁnancial losses.
     + **Recommendation:** Implement MFA for all customer and administrative access.

### Unencrypted Sensitive Data

* + - **Finding ID:** ABC-AUDIT-002
    - **Severity:** High
    - **Description:** Sensitive ﬁnancial data is stored unencrypted in the database.
    - **Impact:** Exposure of sensitive data in case of a breach.
    - **Recommendation:** Implement encryption for all sensitive data at rest and in transit.

### Compliance Review ISO 27001 Compliance:

* **Non-Compliance:** Lack of documented incident response plan, insuFicient access controls.
* **Recommendation:** Develop a detailed incident response plan and review access control policies.

### PCI-DSS Compliance:

* **Non-Compliance:** Unencrypted cardholder data, inadequate network segmentation.
* **Recommendation:** Encrypt all cardholder data and implement proper network segmentation.

### Risk Analysis

The risk assessment matrix for identiﬁed issues:

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **Risk Level** | **Impact** | **Likelihood** |
| Lack of Multi-Factor Authentication | High | High | High |
| Unencrypted Sensitive Data | High | High | Medium |
| InsuFicient Incident Response Plan | High | Medium | Medium |
| Outdated Firewall Rules | Medium | Medium | Medium |
| Weak Password Policies | Medium | Medium | Medium |
| ... | ... | ... | ... |

### Recommendations

* 1. **Implement Multi-Factor Authentication (MFA):**
     + Ensure MFA is mandatory for all user access to critical systems and applications.

### Encrypt Sensitive Data:

* + - Apply encryption to all sensitive data both at rest and in transit.

### Revise and Implement an Incident Response Plan:

* + - Develop a comprehensive incident response plan and conduct regular training and simulations.

### Review and Update Firewall Rules:

* + - Regularly review and update ﬁrewall conﬁgurations to protect against the latest threats.

### Strengthen Password Policies:

* + - Enforce the use of strong passwords, including length, complexity, and expiration policies.

### Conclusion

The security audit identiﬁed several critical and high-risk issues within Shaw Financial Services' infrastructure. Addressing these issues promptly is crucial to reducing the risk of data breaches and ensuring compliance with relevant regulations.

### Appendices

* **Appendix A:** Audit Checklist
* **Appendix B:** Compliance Matrix
* **Appendix C:** Tools and Techniques Used



# COMPLIANCE ASSESSMENT REPORT – ONANA FINANCIAL SERVICES

## PREPARED BY IZZMIER IZZUDDIN

### Table of Contents

* 1. **Executive Summary**

### Assessment Scope

* 1. **Regulatory Requirements**

### Assessment Methodology

* 1. **Compliance Findings**

### Compliance Gaps

* 1. **Recommendations**

### Conclusion

* 1. **Appendices**

### Executive Summary

The compliance assessment was conducted for Onana Financial Services to evaluate the organisation's adherence to relevant regulatory requirements, including PCI DSS, GDPR, and SOX. The goal was to identify areas of non-compliance and provide recommendations to address these gaps.

### Key Findings:

* + **Total Compliance Areas Evaluated:** 15

### Fully Compliant Areas: 10

* + **Partially Compliant Areas:** 3

### Non-Compliant Areas: 2

The assessment revealed critical gaps in data protection and access control measures that need immediate attention to ensure compliance.

### Assessment Scope Objectives:

* + Evaluate Onana Financial Services ' compliance with PCI DSS, GDPR, and SOX regulations.
  + Identify areas of non-compliance and assess the impact of these gaps.
  + Provide actionable recommendations to achieve full compliance.

### In-Scope Compliance Areas:

* + **Payment Card Industry Data Security Standard (PCI DSS)**

### General Data Protection Regulation (GDPR)

* + **Sarbanes-Oxley Act (SOX) Out-of-Scope:**
  + Physical security of branch oFices
  + Non-critical legacy ﬁnancial systems

### Regulatory Requirements

* 1. **PCI DSS:**
     + **Requirement 1:** Install and maintain a ﬁrewall conﬁguration to protect cardholder data.
     + **Requirement 3:** Protect stored cardholder data.
     + **Requirement 5:** Use and regularly update anti-virus software or programs.

### GDPR:

* + - **Article 5:** Principles relating to processing of personal data.
    - **Article 32:** Security of processing.
    - **Article 33:** Notiﬁcation of a personal data breach to the supervisory authority.

### SOX:

* + - **Section 302:** Corporate responsibility for ﬁnancial reports.
    - **Section 404:** Management assessment of internal controls.

### Assessment Methodology

The compliance assessment followed a structured approach:

1. **Documentation Review:** Analysis of existing policies, procedures, and compliance documentation.
2. **Interviews:** Conducted interviews with key stakeholders responsible for compliance.
3. **Technical Assessment:** Veriﬁcation of technical controls and conﬁgurations against regulatory requirements.
4. **Gap Analysis:** Identiﬁcation of gaps in compliance and evaluation of their impact.

### Compliance Findings

* 1. **Fully Compliant Areas:**
     + **PCI DSS Requirement 5:** Anti-virus software is up-to-date and actively monitored.
     + **GDPR Article 32:** Encryption of personal data in transit and at rest.
     + **SOX Section 302:** Corporate responsibility measures are in place, with regular management reviews.

### Partially Compliant Areas:

* + - **PCI DSS Requirement 1:** Firewall conﬁgurations are mostly compliant, but logging and monitoring are inadequate.
    - **GDPR Article 33:** Breach notiﬁcation procedures exist but lack deﬁned timelines and responsibilities.
    - **SOX Section 404:** Internal controls are documented but lack regular testing and review.

### Non-Compliant Areas:

* + - **PCI DSS Requirement 3:** Inadequate protection of stored cardholder data, with some data stored unencrypted.
    - **GDPR Article 5:** Data retention policies are not consistently applied across all departments.

### Compliance Gaps

* 1. **High-Risk Non-Compliance:**

### PCI DSS Requirement 3:

* + **Gap:** Cardholder data stored without encryption in certain databases.
  + **Impact:** High risk of data breach and non-compliance ﬁnes.
  + **Recommendation:** Implement encryption for all stored cardholder data immediately.

### GDPR Article 5:

* + **Gap:** Inconsistent data retention policies leading to potential over- retention of personal data.
  + **Impact:** Non-compliance with GDPR's data minimisation principle.
  + **Recommendation:** Standardise data retention policies and ensure they are applied consistently across the organisation.

### Medium-Risk Non-Compliance:

1. **PCI DSS Requirement 1:**
   * **Gap:** Firewall logs are not regularly monitored, leading to potential undetected breaches.
   * **Impact:** Medium risk of undetected security incidents.
   * **Recommendation:** Enhance ﬁrewall logging and establish a regular monitoring process.

### GDPR Article 33:

* + **Gap:** Lack of clear timelines and responsibilities in breach notiﬁcation procedures.
  + **Impact:** Medium risk of delayed breach reporting.
  + **Recommendation:** Deﬁne clear timelines and assign speciﬁc responsibilities for breach notiﬁcations.

### SOX Section 404:

* + **Gap:** Infrequent testing and review of internal controls.
  + **Impact:** Medium risk of internal control failures.
  + **Recommendation:** Establish a regular schedule for testing and reviewing internal controls.

### Recommendations High-Risk Areas:

1. **PCI DSS Requirement 3:**
   * **Action:** Encrypt all stored cardholder data using strong encryption algorithms.
   * **Timeline:** Immediate (1-2 weeks)

### GDPR Article 5:

* + **Action:** Review and standardise data retention policies across all departments.
  + **Timeline:** High Priority (2-4 weeks)

### Medium-Risk Areas:

1. **PCI DSS Requirement 1:**
   * **Action:** Implement continuous ﬁrewall log monitoring and alerting.
   * **Timeline:** Medium Priority (4-6 weeks)

### GDPR Article 33:

* + **Action:** Update breach notiﬁcation procedures with clear timelines and responsibilities.
  + **Timeline:** Medium Priority (4-6 weeks)

### SOX Section 404:

* + **Action:** Develop and implement a regular internal control testing schedule.
  + **Timeline:** Medium Priority (4-6 weeks)

### Conclusion

The compliance assessment has identiﬁed critical gaps that require immediate action to ensure Onana Financial Services ' adherence to regulatory requirements. By implementing the recommended actions, the organisation can achieve full compliance and reduce the risk of penalties and security breaches.

### Appendices

* + - **Appendix A:** Compliance Checklist
    - **Appendix B:** Interview Notes
    - **Appendix C:** Tools and Techniques Used