**<redacted> threat and risk assessment Report**

# **Executive Summary**

Four key risks were identified that exceeded <REDACTED> moderate risk tolerance. These include flat network architecture, weak authentication mechanisms, inadequate incident response preparedness, and uncertainty regarding PCI DSS compliance. Each of these areas poses an immediate threat to business continuity, data privacy, and regulatory obligations.  
  
Recommendations have been provided to mitigate these risks and strengthen <REDACTED> cybersecurity posture.

Introduction

To establish the current risk exposure to <REDACTED> networks, systems, and information assets, <REDACTED>was engaged to undertake a cybersecurity risk assessment. This was performed via a review of the organisation’s Information Security Policy and an interview with <REDACTED>, <REDACTED> CISO.

Summary of Risk Assessment Methodology – See Appendix 1

Summary of Risks Identified

* Flat Network Architecture: All sensitive and non-sensitive data resides in a flat network, increasing the risk of lateral movement and unauthorized access.
* Single-Factor Authentication: Use of single-factor authentication across admin and user accounts leaves systems vulnerable to credential-based attacks.
* Inadequate Incident Response Preparedness: Lack of a documented IR plan, untested backups, and absence of tabletop exercises reduce <REDACTED> readiness to manage security incidents.
* Uncertainty Around PCI DSS Compliance: Lack of clarity regarding PCI DSS obligations poses regulatory and reputational risks, especially concerning customer payment data.

Summary of Proposed Risk Treatments

* Implement network segmentation and enforce role-based access to reduce exposure from flat architecture.
* Adopt multi-factor authentication (MFA) for all privileged and user accounts to mitigate credential compromise risks.
* Develop, document, and test an incident response plan, including backup restoration validation and tabletop simulations.
* Conduct a formal PCI DSS compliance review to clarify obligations, update documentation, and ensure alignment with data protection standards.

Scope and Risk Tolerance

The scope of this assessment was the <REDACTED> operational and business environment and all supporting ICT and information assets.

The risk appetite of <REDACTED> is **Moderate**; as such, all risks with an assessed rating exceeding this threshold require selection of one of the following treatments:

* Mitigate – Reduce the risk likelihood or impact by implementing additional controls, procedures, or safeguards.
* Transfer – Shift the risk to a third party, such as through outsourcing, insurance, or contractual arrangements.
* Accept – Acknowledge the risk and take no additional action, typically when it falls within risk appetite or mitigation is not cost-effective.
* Avoid – Eliminate the risk entirely by discontinuing the associated activity or changing the approach.

The selection of a proposed treatment is to be based on the efficacy of the treatment measured against the time, cost, resources and effort required for implementation.

# **Risk Assessment**

The following risks have been identified as part of this risk assessment in relation to <REDACTED> operations and services.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Risk identified/Statement** | **Existing Controls** | **Likelihood** | **Consequence** | **Risk** | **Proposed Treatment** | **Residual Likelihood** | **Residual Consequence** | **Residual Risk** |
| **R1** | Not segmenting the network increases the likelihood of unauthorized access and lateral movement across sensitive systems. | Flat network with centralized data and basic logging. | Likely | Major | Extreme | Mitigate – Implement VLAN-based network segmentation, role-based access controls, and internal firewall policies. (Ref: ISO/IEC 27001 A.13.1.1 – Network controls) | Possible | Moderate | Moderate |
| **R2** | Not implementing multi-factor authentication elevates the likelihood of unauthorized access due to compromised credentials. | Password complexity enforced only. | Likely | Major | Extreme | Mitigate – Enforce multi-factor authentication for all admin and user accounts. (Ref: ISO/IEC 27001 A.9.4.2 – Secure log-on procedures / A.9.4.3 – Password management system) | Unlikely | Moderate | Low |
| **R3** | Not documenting and testing the incident response plan elevates the consequence of an ineffective response during security incidents. | Logging enabled, DR/BCP exists but not tested, occasional workshops held. | Possible | Major | High | Mitigate – Develop and test a formal incident response plan, implement awareness training, and conduct regular tabletop exercises. (Ref: ISO/IEC 27001 A.16.1.1 – Responsibilities and procedures / A.17.1.3 – Information backup) | Unlikely | Moderate | Moderate |
| **R4** | Not confirming PCI DSS applicability elevates the risk of non-compliance and mishandling of customer payment data. | PANs are masked; payment processing outsourced. CISO unsure about PCI DSS applicability. | Possible | Major | High | Mitigate – Conduct a formal PCI DSS compliance assessment, document third-party roles, and update internal policies. (Ref: ISO/IEC 27001 A.18.1.4 – Privacy and protection of personally identifiable information) | Unlikely | Moderate | Moderate |

**APPENDIX 1: Risk Matrix and Risk, Likelihood & Consequence Ratings**

Risk Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk Matrix | | Consequence | | | | |
| **Negligible** | **Minor** | **Moderate** | **Major** | **Severe** |
| Likelihood | **Almost Certain** | Moderate | High | High | Extreme | Extreme |
| **Likely** | Low | Moderate | High | Extreme | Extreme |
| **Possible** | Low | Moderate | High | High | Extreme |
| **Unlikely** | Low | Low | Moderate | High | High |
| **Rare** | Low | Low | Low | Moderate | High |

Risk Ratings

|  |  |
| --- | --- |
| Risk Rating | Risk Definition |
| Extreme | The risk threatens the survival of the organisation if it eventuates.  An immediate response is required by executive management to mitigate existing risk to the organisation.  A proposed activity posing such a risk must not proceed without executive management sign-off and application of mitigating controls. |
| High | The risk threatens the continued operation of an organisational business unit or service.  A response is required by executive management to mitigate existing risk to the organisation.  A proposed activity posing such a risk must not proceed without application of mitigating controls. |
| Moderate | The risk threatens an organisational activity.  Controls that are in place must be confirmed to effectively mitigate existing risk, and the risk must be accepted by the risk owner.  Action is required at the business unit level to evaluate whether the level of risk posed by the proposed activity is within their risk appetite or apply additional controls. |
| Low | The risk is managed by Business as Usual (BAU) practices and procedures. |

Likelihood Ratings

|  |  |  |  |
| --- | --- | --- | --- |
| Likelihood | Chance | Frequency | Probability |
| Almost Certain | Is expected to occur in most circumstances. | Has occurred 9 or 10 times in the past 10 years in the organisation or circumstances are in train that will almost certainly cause it to happen. | >/=95% |
| Likely | Will probably occur in most circumstances. | Occurred more than 7 times over 10 years in the organisation or in other similar organisations or circumstances such that is likely to occur in the next year. | 65% - 95% |
| Possible | Might occur at some time. | Has occurred in this organisation more than 3 times in the past 10 years, or occurs regularly in similar organisations, or is considered to have a reasonable likelihood of occurring in the next few years. | 35% - 65% |
| Unlikely | Could occur at some time. | Has occurred 2 or 3 times in 10 years within the organisation or similar organisations. | 5% - 35% |
| Rare | May occur in exceptional circumstances | Has occurred or can reasonably be expected to occur only a few times in 100 years. | <5% |

Consequence Ratings

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Area of Impact | Negligible | Minor | Moderate | Major | Severe |
| Information | Compromise of information otherwise in the public domain. | Minor compromise of information sensitive to internal business unit interests. | Compromise of information important to the organisation’s operations. | Compromise of information critical to the organisation’s operations and competitive advantage. | Compromise of information covered by legal or regulatory obligations. |
| Operations | Minimal impact on non-core operations. The impact can be managed as part of Business as Usual (BAU) operations. | Some impact to organisational operations, such as delays or minor loss in Quality of Service (QoS). | Impact on the organisation resulting in degradation of performance which impacts targets. | Breakdown of key business activities leading to reduction in performance, such as service delays, revenue loss, client dissatisfaction, legal/regulatory breaches. | Protracted unavailability of key business activities. Survival of the organisation is threatened. |
| People | Minor injury or first aid treatment. | Injury requiring treatment by medical practitioner and/or loss time from workplace. | Major injury or hospitalisation. | Single death and/or multiple major injuries. | Multiple deaths. |
| Property | Minor damage of vandalism to asset. | Minor damage or loss of <5% of total assets. | Damage or loss of <20% of total assets. | Extensive damage or loss <50% of total assets | Destruction or complete loss of >50% of assets. |
| Financial | 1% of budget (organisational, business unit, or project budget, as applicable). | 2-5% of annual budget. | 5-10% of annual budget. | > 10% of annual budget. | > 30% of organisational or project budget. |
| Reputation | Local mention only which is quickly forgotten. Freedom to operate unaffected. | Adverse media coverage at a local or regional level.  Minor brand damage offset by public relations efforts. | Adverse media coverage at a local or regional level. Threat of prosecution or sanctions by authorities for breach of laws or regulations. | Adverse media coverage at a national level, and public, political, and media scrutiny. Brand damage and loss of customers. | National or International concern, Governmental inquiry. Sustained adverse national or international media scrutiny. Significant Brand damage and loss of customers. |
| Regulatory Compliance | Minor regulatory breach which is remediated through BAU activities. | Regulatory scrutiny and threats of sanctions or penalties. | Minor breach of laws or regulations, penalties applied to the organisation. | Breach of laws or regulations, sanctions or penalties applied to the organisation, enforceable undertakings applied to the organisation over a short period of time. | Significant breach of laws or regulations, major sanctions or penalties, enforceable undertakings over a number of years, prosecution of directors. |