Document Reference:		Effective Date:	24/03/2024
Document Name:	Security Gap Analysis Report	Expiry Date:	24/3/2025

Cybersecurity Gap Analysis Report

SIT374 Team Project A

Redback Operations

Document Owner:	Daniel McAulay	Last Modified By:	Daniel McAulay
Next Review Date:	1/8/2024	Last Modified on:	24/03/2024

Version	Modified By	Approver	Date	Changes made
V0.2	Daniel McAulay	Daniel McAulay	24/03/2024	Document Creation

Table of Contents

Executive Summary

This report highlights the current state of our IT and cybersecurity infrastructure, identifies key gaps in policies and procedures, and provides recommendations for enhancing our security posture. It addresses the need for a comprehensive Information Security Management System and outlines specific areas where existing policies lack depth or are entirely missing.

The purpose of this gap analysis is to assess Redback Operation's current IT and cybersecurity policies against industry best practices and common security principles. Our focus has been on evaluating the overall robustness of our security policies and procedures across multiple layers of defence.

Current State Analysis

IT Infrastructure & Technology Summary

Currently all documentation references Google Cloud Platform. Redback Operations is currently undergoing a transitionary period of deploying on-premise & additional cloud-based assets, such as Microsoft Azure. Due to this transitional state, technical debt exists that Redback Operations needs to address to reduce risk & security gaps.

In this current transitional state, a complete gap analysis of technical policies & controls is difficult to conduct. Therefore, this report focuses primarily on high-level security policy.

Cybersecurity Posture

Our cybersecurity measures a limited range of policies, tools, and controls. Despite the limited existing measures, lack of a clear ISMS and security governance strategy, there are significant gaps in our security posture. Using defence in depth layers as a metric to measure security, there are significant gaps based on policy depth and coverage.

Regulatory and Industry Framework Compliance Overview

Currently, Redback Operations adheres to the Australian Privacy Act. Comprehensive documentation exists that references the Australian Privacy Principles, which must be adhered to across the company for all initiatives that both Information Technology and Operational Technology related.

While minor references to the Essential 8 Framework is referenced across Redback Operations security guidelines, there is no real implemented industry security frameworks such as NIST, CIS or ASD ISM that are adhered to in the environment. The overall

assessment is Redback Operations adheres to a limited set of incomplete or minor custom policies, resulting in low cyber maturity.

Gap Analysis

Policy, Procedure & Control Gaps for Redback Operations

Redback Operations faces exposure due to the absence of core IT and IT Security policies. Addressing these vulnerabilities is important for the security and operational efficiency of the company.

The core fundamental finding of this gap analysis report is the lack of a comprehensive Information Security Management System (ISMS).

The absence of formal policies across various domains of IT and cybersecurity has been identified as a critical vulnerability. While additional standards, policies, procedures & guidelines will be required to improve cyber maturity, the policies outlined in this document are fundamental to the development of any ISMS and have been considered as a priority to be developed.

The following sections outline the policy gaps that have been identified, along with suggested subjects each policy should cover:

Data Classification & Data Loss Prevention

Gap Analysis Finding:

No policy exists.

Policy Objective & Summary:

To mitigate risks associated with unauthorized data access and loss, ensuring the integrity and confidentiality of sensitive information.

Key Subjects:

- Definition of data categories & sensitivity controls (public, internal, confidential, and highly confidential).
- Define standards for data handling, storage, and transmission based on classification.
- Procedures for data loss prevention, including technological and process-based controls.
    - Keep content agnostic to controls and not technology.

- Roles and responsibilities for data management and protection.
    - Can also be defined as Data Mapping & Ownership.
- Enhancement and integration with existing Data Breach reporting mechanisms.

Cloud Security (Microsoft Azure)

Gap Analysis Finding:

No policy exists.

Policy Objective & Summary:

To define standards and controls to be utilized for cloud-based assets. Policy design must cover risk mitigation for cloud-based environments against potential threats, referencing established frameworks and platform strategies.

Key Subjects:

- Security responsibilities of the cloud provider versus the organization.
- Security policy and frameworks for deploying assets securely to Azure.
    - May include deployment strategies, security tooling, network topologies & individual security controls.
- Access control and identity management for cloud services.
- Secure development practices for cloud-based applications.

Endpoint Security

Gap Analysis Finding:

Some minor policy coverage exists, primarily references the Essential 8 Framework. Policy lacks depth such as maturity levels or methodology to achieve framework adherence.

Objective: To protect all organizational devices against cyber threats, ensuring the security of data accessed and processed by these devices.

Key Subjects:

- Mandatory security software requirements (antivirus, firewall, etc.).
- Regular update and patch management procedures.
- Secure configuration standards for all endpoints.
- References to the Essential 8 Framework

Server Security & Hardening

Gap Analysis Finding:

Some minor policy coverage exists, primarily the Essential 8 Framework. Policy lacks depth such as maturity levels or methodology to achieve framework adherence.

Objective: To establish secure server operations, minimizing vulnerabilities through stringent security practices and hardening techniques.

Key Subjects:

- Hardening guidelines for operating systems and services.
- Patch management and vulnerability assessment schedule.
- Access control measures and use of secure administration protocols.
- Physical security measures for server environments.
- Monitoring and response strategies for server-related security events.
- Reference controls outlined in the Essential 8 Framework.

Encryption

Gap Analysis Finding:

Some content regarding this topic exists but is not detailed regarding encryption standards. Existing content is related to existing infrastructure only and is not a high-level policy or standard.

Objective: To ensure the confidentiality and integrity of data in transit and at rest through the application of strong encryption standards.

Key Subjects:

- Approved encryption algorithms and protocols.
- Key management lifecycle, including generation, storage, and destruction.
    - May include references to Certificate Authority Design/Hierarchy.
- Use cases for encryption (data at rest, data in transit, etc.).
- Encryption audit and verification procedures.

Monitoring & Log Analytics

Gap Analysis Finding:

Some minor content coverage exists. Existing content relates to Google Chronicle and is not detailed regarding Monitoring & Log Analytics in general. Existing content is related to GCP infrastructure and is not a high-level policy, standard or design.

Objective: To enable timely detection and response to security incidents through comprehensive monitoring and analysis of system logs.

Commented [DM1]: Existing Policy

Key Subjects:

- Log collection and management policy, covering what must be logged, log format, and retention.
- Real-time monitoring and alerting mechanisms.
- Common incident response scenarios & playbooks.
- References to common SOC (Security Operations Centre) design principles.

User Awareness Training

Gap Analysis Finding:

No training content exists which covers security awareness training.

Objective: To create and support a security-conscious culture within the organization, empowering employees to recognize and respond to cybersecurity threats.

Key Subjects:

- Overview of common cyber threats and attack vectors.
- Secure practices for email, web browsing, and device usage.
- Password management and multi-factor authentication.
- Reporting procedures for suspicious activities or incidents.
- Regular training schedule and policy compliance requirements.

External Attack Surface Management

Gap Analysis Finding:

No policy exists.

Objective: To identify, map, assess, and secure external-facing assets, reducing the risk of attacks exploiting these exposures.

Key Subjects:

- Inventory and classification of external-facing assets.
- Regular assessment procedures for identifying vulnerabilities.
- Remediation priorities and timelines for identified risks.
- Coordination with third parties for securing shared assets.
- Continuous improvement process for attack surface reduction.
- Policy compliance requirements for onboarding new assets.

BYOD & Mobile Device Management

Gap Analysis Finding:

No policy exists.

Objective: To establish control over personal devices used for work purposes, ensuring they meet organizational security standards.

Key Subjects:

- Security requirements and controls for personal devices accessing corporate resources.
- Device registration and compliance verification processes.
- Data separation and encryption on personal devices.
- Lost or stolen device response procedures.
- Privacy considerations for employees and the organization.

Technical Gaps

Due to platform changes and a lack of technical security tooling due to pending implementations, technical gaps are considered not applicable currently.

Recommendations

Strategic Recommendations

- Develop and implement comprehensive policies for each identified gap area, aligned with industry best practices and regulatory requirements.
- Establish a formal Information Security Management System to oversee policy implementation and compliance.
- Enhance user awareness training to cover critical cybersecurity threats and best practices.
- Implement technical measures to address identified vulnerabilities in network, server, and application security.
- Ensure Redback Operations ISMS is operational and actively used to guide the company towards maintaining a robust security posture.

Implementation Plan

The Redback Operations Infrastructure and Policy teams have already started addressing the gaps identified, including policy development, training programs, and technical security enhancements. Responsibilities are assigned to respective team members, with progress tracked via project management tools (Trello).

Conclusion

This gap analysis report underscores the urgent need for a comprehensive review and enhancement of Redback Operations IT and cybersecurity policies. By addressing the identified gaps, we can significantly improve our security posture and resilience against cyber threats.