GRC Team Gap Analysis Report

SIT378 Team Project B

*Redback Operations*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Modified By | Approver | Date | Changes Made |
| V0.1 | Jamison Begley |  | 24/07/2024 | Document Creation |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table Of Contents

[Executive Summary 4](#_Toc172811049)

[Current State Analysis 4](#_Toc172811050)

[IT Infrastructure Summary 4](#_Toc172811051)

[Cybersecurity Posture 4](#_Toc172811052)

[Regulatory and Industry Framework Compliance Overview 4](#_Toc172811053)

[Gap Analysis 5](#_Toc172811054)

[Policy, Procedure & Control Gaps for Redback Operations 5](#_Toc172811055)

[User Awareness Training 5](#_Toc172811056)

[Policy & Procedure Implementation Plans for Redback Operations 5](#_Toc172811057)

[Data Classification & Data Loss Prevention 6](#_Toc172811058)

[Cryptography Policy 6](#_Toc172811059)

[Endpoint Security 6](#_Toc172811060)

[External Attack Surface Management 7](#_Toc172811061)

[Monitoring & Log Analytics 7](#_Toc172811062)

[Server Security Policy 8](#_Toc172811063)

[User Awareness Training 8](#_Toc172811064)

[Recommendations 9](#_Toc172811065)

[Strategic Recommendations 9](#_Toc172811066)

[Implementation Plan 9](#_Toc172811067)

[Conclusion 9](#_Toc172811068)

# Executive Summary

This report highlights the current state of our IT and cybersecurity infrastructure in relation to the company’s GRC Team. It identifies key gaps in policies, procedures, implementation plans, and offers recommendations to strengthen our security posture. It emphasizes the need for improvement of our Information Security Management Systems, and identifies where policies need to be adjusted, and implementation plans created.

This gap analysis aims to evaluate Redback Operations’ current IT and cybersecurity policies and plans against industry-level security principles. We have concentrated on assessing the overall effectiveness of our security policies, procedures and plans across different layers of defense.

# Current State Analysis

## IT Infrastructure Summary

Currently all documentation can be accessed through the Redback Operations, Github, Docusaurs, or teams’ channels. Though the documentation is accessible to the public, only those involved and working with Redback Operations have access to the raw files that are used.

## Cybersecurity Posture

Compared to the previous GAP Analysis, our cybersecurity posture is now in a greater position, as it now measures a complex range of ISMS policies and procedures on how to govern the safety and functionality of our workplace.

Though there is a significant gap in the depth of some of the policies, and there is a lack of implementation/deployment plans for these policies and procedures.

## Regulatory and Industry Framework Compliance Overview

Redback Operations still adhere to the Australian Privacy Act. All documentation created exists in reference to the Australian Privacy Principles.

Though there are a range of policies and procedures at Redback Operations, there is a gap in deployment/implementation plans for these, so it cannot be guaranteed that these policies and procedures are being complied to, which may result in poor cyber safety.

# Gap Analysis

## Policy, Procedure & Control Gaps for Redback Operations

In response to the most recent Gap Analysis report, a range of ISMS policies were designed to address security concerns and vulnerabilities that Redback Operations may face.

Despite all policies being created, they are subject to be developed further. An example of this being the User Awareness Training Policy/Content. It is better to have more detailed and lengthy training, ensuring to cover all areas of awareness education for safety.

### User Awareness Training

**Gap Analysis Finding:**

No company-wide training content exists which oversees security awareness – despite there being cybersecurity–specific user awareness training. Though the current cybersecurity-awareness training can be edited and changed to a company-wide focus, by adding more general training points, such as password protection, and general system health and safety.

**Objective Summary:** To develop a comprehensive, yet easy to understand training program to educate employees on how to accurately identify and respond to cybersecurity threats.

**Key Subjects:**

* Secure practices for email, web browsing, and device usage.
* Password management and multi-factor authentication.
* Reporting procedures for suspicious activities or incidents.
* Constant system updates to patch for vulnerabilities
* Understanding Routes for Help (Needs to be modified to be company-wide)

## Policy & Procedure Implementation Plans for Redback Operations

Now that the ISMS Policy, Procedure & Control documents have been created, a more practical approach can be taken in the creation of deployment/implementation plans of each of these policies.

**Objective:** To develop deployment/implementation plans for ISMS policies and procedures that are easy to understand, safe to implement, consider cost effectiveness and do not pose any direct threat to the company.

### Data Classification & Data Loss Prevention

**Gap Analysis Finding:**

No deployment/implementation plan exists

**Objective Summary:** To develop an easy to implement, cost effective deployment plan for our Data Classification & Data Loss Prevention policies and procedures

**Key Subjects:**

* Re-define Data Classification levels
* Define Access Control levels
* Develop a “Redback Operations” page watermark
* Indicate encryption applications
* Explain how content inspection will be implemented
* Cost Effectiveness
* Ease of implementation
* Adherence to regulatory requirements

### Cryptography Policy

**Gap Analysis Finding:**

No deployment/implementation plan exists

**Objective Summary:** To develop an easy to implement, cost effective deployment plan for our Cryptography policies and procedures

**Key Subjects:**

* Re-define what encryption standards will be used
* Re-define classification levels
* Research encryption applications/programs that can be used
* Cost Effectiveness
* Ease of implementation
* Adherence to regulatory requirements

### Endpoint Security

**Gap Analysis Finding:**

No deployment/implementation plan exists

**Objective Summary:** To develop an easy to implement, cost effective deployment plan for our Endpoint security policies and procedures

**Key Subjects:**

* Re-define roles and responsibilities
* Research affordable, yet secure methods for storage (physical and digital)
* Redefine the need for awareness training
* Implementation of Least Privilege
* Cost Effectiveness
* Ease of implementation
* Adherence to regulatory requirements

### External Attack Surface Management

**Gap Analysis Finding:**

No deployment/implementation plan exists

**Objective Summary:** To develop an easy to implement, cost effective deployment plan for our External Attack Surface Management (EASM) policies and procedures

**Key Subjects:**

* Redefine policy adherence criteria
* Redefine roles and responsibilities
* Research protection services for:
  + Web-facing Applications and Services
  + Network Infrastructure
  + Cloud Services and Infrastructure
  + Email and Communication Servers
  + Remote Access Services
* Use EASM Policy (Methodology section) for areas to implement
* Cost Effectiveness
* Ease of implementation
* Adherence to regulatory requirements

### Monitoring & Log Analytics

**Gap Analysis Finding:**

No deployment/implementation plan exists

**Objective Summary:** To develop an easy to implement, cost effective deployment plan for our Monitoring & Log Analytics policies and procedures

**Key Subjects:**

* Research tools that can be used to collect and analyse log data
* Redefine key assets and data categories
* Redefine Roles and Responsibilities
* Ensure all digital assets are covered in deployment – explain how they will be covered
* Cost Effectiveness
* Ease of implementation
* Adherence to regulatory requirements

### Server Security Policy

**Gap Analysis Finding:**

No deployment/implementation plan exists

**Objective Summary:** To develop an easy to implement, cost effective deployment plan for our Server Security policies and procedures

**Key Subjects:**

* Redefine guidelines for:
  + Access Control
  + Data Protection
  + System Configuration
  + Patch Management
  + Security Monitoring
  + Incident Response
* Redefine key assets and data categories
* Redefine roles and responsibilities
* Refer to Server Security Policy (Strategic Overview & Controls section) for implementation strategies.
  + **Though these need to be built upon**
* Cost Effectiveness
* Ease of implementation
* Adherence to regulatory requirements

### User Awareness Training

**Gap Analysis Finding:**

Some cybersecurity-user related training exists. Though this needs to be broadened to company-wide training. This will be built upon through the previous section: “Policy, Procedure & Control Gaps for Redback Operations”.

**Key Subjects:**

* This content should be worked on through the course of the semester, adding more to it as more documentation is created, though it can only be completed once all deployment plans have been created, as information within these plans should be in the training content.
* Adherence to regulatory requirements

# Recommendations

### Strategic Recommendations

* Develop and begin to implement comprehensive, yet easy to understand deployment plans and strategies for each ISMS policy, maintaining adhering to regulatory requirements.
* Develop stronger and broader user awareness training content to oversee the entire company.
* Ensure that the developed ISMS policies are implemented and complied with.

# Implementation Plan

The Redback Operations GRC team will begin developing a range of material that directly addresses the gaps identified, including training programs, strengthening/redesigning of policies, and implementation/deployment plans. Roles and responsibilities will be either self-assigned or directed by our team leader, where all progress can be tracked via Microsoft Planner and through frequent team meetings.

# Conclusion

This gap analysis report outlines the critical need for a thorough review and enhancement of Redback Operations’ ISMS policies, paired with the need for creation of deployment plans, created in an easy to understand, and cost-effective manner. Addressing the gaps identified will cause a drastic improvement in our security posture as compliance to policies will be ensured with the implementation of deployment plans.