Data Warehousing Team Audit Report

SIT374 Team Project A

*Redback Operations*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Modified By** | **Approver** | **Date** | **Changes made** |
| 1.0 | Jamison Begley |  | 9/9/24 | Document Creation |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

*​*

Contents

[Introduction 4](#_Toc176773374)

[Audit 4](#_Toc176773375)

[Policy Compliance 4](#_Toc176773376)

[Ethical Considerations and Requirements 6](#_Toc176773377)

[Governance 8](#_Toc176773378)

[Overall Findings and Recommendations 9](#_Toc176773379)

[Conclusion 10](#_Toc176773380)

*​*

*​*

*​*

*​*

*​*

​**​**

## Introduction

The Data Warehousing team audit took place on Friday, September 6, 2024 between auditor, Jamison Begley, and Team Leader, Kaylin Lucas-Griffin. The purpose of this audit was to assess the conformity of the data warehousing team to Redback Operations’ ISMS policies, ethical considerations, and general governance concerns.

Before the day of the audit, I conducted my own research on the team and their work to get a better understanding of what they do at Redback Operations, though I also created a separate document with a range of questions that are developed to confirm or deny my findings.

On the day of the audit, I began with asking a few questions related to their team, the first being: “What data, and what type of data is being stored”. To which the response was that the data being stored is a collection from each project, though it is only sample data, and they are generally in the format of .csv, and .json files. This information is stored on a Deakin VM, meaning that the data is completely offline (no cloud storage), but for the time being the team is happy with its storage capabilities.

## 

## Audit

The following text shows each audit point, compliance, observations, and action required if applicable.

### Policy Compliance

* 1. – Are the correct encryption methods being used for data in storage and transmission?

No, data is transmitted and stored in plaintext.

Action Required:

* Data transmission and storage needs to be in accordance with the company’s cryptography policy, which can be accessed on our company repos.
  1. – Are the related DLP Policies being adhered to?

No, Access Controls are not being adhered to as everyone as root access

No, Encryption is not being adhered to (according to 1.1).

No, Content Inspection is not being adhered to, though it was stated that some files undergo content inspection – this needs to be all files.

No, Regular Backups do not occur (it was stated that no backups occur).

Action Required:

* DLP Policies need to be adhered to by implementing relevant access controls (limiting who can access/modify the data).
* Encryption Policy needs to be adhered to (according to 1.1).
* All data must undergo content inspection when received from each project.
* Regular data backups must take place to ensure recovery of data if lost.
  1. – Are the related Data Classification Policies being adhered to?

Yes, the Data Classification Policies are being adhered to, and data is categorised accordingly.

Action Required:

* No action is required.
  1. – Have forms of physical security for data protection been implemented?

Yes, password protection has been implemented on the Deakin VM, protection data from physical interception.

Action Required:

* No action is required.
  1. – Have forms of digital security for data protection been implemented?

Yes, data is protected behind Deakin’s internet servers – individuals must be connected to the Deakin VM to access the data.

Action Required:

* No action is required.
  1. – Have EASM risks been identified?

No, the team is aware of potential risks and attacks, though there is no documentation of these potential risks.

Action Required:

* Documentation of potential External Attack Surface Management risks needs to be created – for more information access the EASM policy on our company’s repos.
  1. – Have all employees undergone the appropriate User Awareness Training?

No, the team was unaware of the “Cybersecurity User Awareness Training” document.

Action Required:

* Employees must read over the Cybersecurity User Awareness Training document so they can better understand what policies and procedures must be followed, and they can better their understanding of potential risks to their data.

### Ethical Considerations and Requirements

* 1. – Are all forms of data collection briefed with customers, and is consent gathered?

N/A – The team only stores the data; they do not collect it.

Action Required:

* No action is required.
  1. – Has all collected information and data been classified with data classification requirements?

Yes, in reference to 1.3, all data collected is categorised according to the Data Classification Policies.

Action Required:

* No action is required.
  1. – Is data anonymity used to protect the privacy of customers?

Yes, data anonymity is used for project 2 data, as this is the only project with personally identifiable information.

Action Required:

* No action is required.
  1. – Is the cryptography policy being adhered to?

No, in reference to 1.1, the cryptography is not being adhered to as all data is stored and transmitted in plaintext.

Action Required:

* In reference to 1.1, Data transmission and storage needs to be in accordance with the company’s cryptography policy, which can be accessed on our company repos.
  1. – Is data minimalization being put in place when collecting data?

Yes, only data that is relevant to Redback Operations’ company directive and goals is being collected.

Action Required:

* No action is required.
  1. – Are the relevant ISMS policies being adhered to when required?

No, the team is unaware of the policies, therefore they are not being adhered to.

Action Required:

* The team must conduct their own research and read through the ISMS policies to gain a better understanding of how to comply – this can be done through the User Awareness Training.

### Governance

* 1. – Is the tea, adhering to the company’s governance framework?

Yes, all data is used for the company’s goals and directive. Everything on the VM is within Redback’s scope of operations.

Action Required:

* No action is required.
  1. – Are team roles and responsibilities clearly defined and documented?

Yes, sub-teams are classified and documented, also known as the “Data Warehousing Solutions”.

Action Required:

* No action is required.
  1. – Is there a risk management plan in place?

No, there is no risk management plan in place, there is also no evidence of potential risks being identified.

Action Required:

* A document needs to be created outlining potential risks, and how to manage them.
  1. – Is there an incident response plan in place?

No, there is not an incident response plan in place, nor is there a document to list potential incident.

Action Required:

* An incident response plan, including potential incidents, their impact, and how to appropriately respond to them must be created.
  1. – Are incidents logged and reviewed for continuous improvement?

No, as there is no incident response plan, incidents are not logged and regularly reviewed for continuous improvement.

Action Required:

* An incident logging document must be created and updated in response to incidents whenever they occur.

## Overall Findings and Recommendations

This audit outlined various gaps in the Data Warehousing team’s ISMS policy compliance and general awareness, their compliance to ethical considerations and overall governance.

On the topic of policy compliance, the team needs to read through the ISMS policies on our company repos and adjust their working style accordingly, with main points of interest being encryption, data loss prevention, risk management and overall user training. The User Awareness Training should be treated as a high priority, as it will help employees gain a greater understanding of the practices that need to be in place to maintain a safe and secure environment for our data.

Relevant to ethical considerations and requirements, data confidentiality and integrity can only be guaranteed if the cryptography policy is understood and adhered to, as data should not be stored and transmitted in plaintext.

Finally, referring to the general governance points, there should be regular risk identification being documented, so the team can account for, and avoid any potential risks. Further, a risk management plan and incident response plan should be developed, alongside the logging of incidents to allow for continuous improvement to our security posture.

## Conclusion

After the audit, a few more questions were asked to gain a better understanding of the direction that the Data Warehousing team aims to take.

Kaylin ended by saying that he and his team “want to have governance and the correct security in place to be an elite team, and an elite project”. He wants their service to be a “self-service for employees”, and to have cloud storage and access to make it easier to “provide a service to the rest of the projects as somewhere that they can store and access their data”.