ISMS Policy Review

The scope of this review is to analyse the current ISMS (Information Security Management System) to ensure it is compliant with the ISO/IEC 27001 standard. A checklist was created which contained each requirement of an ISMS policy and used against the current policy to make sure it is compliant.

Each section is based off the number of requirements needed for an ISMS policy as told from ISO/IEC 27001. Sections may not contain notes as they are already compliant with the standard. The section structure of the current policy should also mimic this unless otherwise noted:

1. Scope

Is compliant with ISO/IEC 27001 standard? - YES

Scope is well written and fits the requirements needed. No work is needed for this section. But work outside of the ISMS policy might be needed to create policies for each of the assets listed in the scope. As some have policies and some do not

Policies that need to be created:

- Cloud security
- BYOD & MDM

2. Normative References

Is compliant with ISO/IEC 27001 standard? - NO

As stated in the policy, this section isn't applicable to Redback. Was only included to ensure section numbering was in line with ISO/IEC 27001. There is no way to improve on this as it would require a more detailed ISMS policy

3. Terms and Definitions

Is compliant with ISO/IEC 27001 standard? - NO

There are no references made to ISO/IEC 27000. It is unclear if there are terms used throughout the document that may need to be specified. This could be due to the detail of the policy that those references may not have been needed

4. Context of the Organisation

4.1 Understanding the organization and its context

Is compliant with ISO/IEC 27001 standard? – YES

4.2 Understanding the needs and expectations of interested parties

Is compliant with ISO/IEC 27001 standard? - YES

Needs more detail on which requirements will be addressed through the ISMS. Contains the needs and expectations of all interested parties but only list's them and doesn't go into detail about each one. This could be an area to improve on

4.3 Determining the scope of the information security management system

Is compliant with ISO/IEC 27001 standard? – YES

Does an excellent job of determining the scope. But needs to consider requirements referred to in 4.2 which there were none listed.

4.4 Information security management system

Is compliant with ISO/IEC 27001 standard? - YES

Well-written and fits the requirements. However, it refers to "section 12" which will have links to "appropriate" documentation/policies which can provide further explanation. Examining section 12, there are no links provided to said documentation and some of the assets mentioned don't have policies created for them

5. Leadership

5.1 Leadership and commitment

Is compliant with ISO/IEC 27001 standard? - NO

Needs more detail on how these policies will be implemented and be maintained. That could potentially be beyond the scope of the company and unit

5.2 Policy

Is compliant with ISO/IEC 27001 standard? - NO

Makes references to links to documents in section 12. As stated, there are no links to other policies present in that section. This will need to be rectified at some point as this is an important requirement that all documentation should be available

5.3 Organizational roles, responsibilities and authorities

Is compliant with ISO/IEC 27001 standard? – YES

6. Planning

6.1 Actions to address risks and opportunities

6.1.1 General

Is compliant with ISO/IEC 27001 standard? - YES

6.1.2 Information security risk assessment

Is compliant with ISO/IEC 27001 standard? - NO

This section states that a Risk analysis should be created alongside the ISMS. No analysis has been linked or created. Could this be something that can potentially be done?

6.1.3 Information security risk treatment

Is compliant with ISO/IEC 27001 standard? - NO

Same as above. No treatment has been linked or created

6.2 Information security objectives and planning to achieve them

Is compliant with ISO/IEC 27001 standard? - YES

Mislabelled as 6.1.4. Needs to be fixed to be in line with ISO/IEC 27001 standard. Potentially more detail is needed on how the company plans to achieve these objectives

6.3 Planning of changes

Is compliant with ISO/IEC 27001 standard? - NO

Not present in the document. Unknown if it fits with the scope of the unit

7. Support

7.1 Resources

Is compliant with ISO/IEC 27001 standard? - YES

As stated in the policy, Redback Operations doesn't have the same resources as a typical IT organisation. As all roles are split between students.

7.2 Competence

Is compliant with ISO/IEC 27001 standard? - YES

States that training maybe required to bring Staff and students are working within the ISMS. Would it be worth creating training documents or videos to cover all bases?

7.3 Awareness

Is compliant with ISO/IEC 27001 standard? - YES

All documentation that has been created is available on the website and is accessible to all

7.4 Communication

Is compliant with ISO/IEC 27001 standard? - YES

7.5 Documented Information

7.5.1 General

Is compliant with ISO/IEC 27001 standard? - YES

Mislabelled as Section 8.1 in the current policy. Is meant to be 7.5.1 to fit the standard

7.5.2 Creating and Updating

Is compliant with ISO/IEC 27001 standard? - YES

Mislabelled as Section 8.2 in the current policy. Is meant to be 7.5.2 to fit the standard

7.5.3 Control of Documented Information

Is compliant with ISO/IEC 27001 standard? - YES

Mislabelled as Section 8.3 in the current policy. Is meant to be 7.5.3 to fit the standard

8. Operation

8.1 Operational planning and control

Is compliant with ISO/IEC 27001 standard? - YES

Mislabelled as Section 9.1 in the current policy. Is meant to be 8.1 to fit the standard

8.2 Information security risk assessment

Is compliant with ISO/IEC 27001 standard? - NO

Not present in the current policy. As with 6.1.2, the risk assessment hasn't been linked or created

8.3 Information security risk treatment

Is compliant with ISO/IEC 27001 standard? - NO

Not present in the current policy. As with 6.1.3, the risk treatment hasn't been linked or created

9. Performance Evaluation

9.1 Monitoring, measurement, analysis and evaluation

Is compliant with ISO/IEC 27001 standard? - YES

Labelled as Section 10.1 in the current policy. Needs to be renamed to 9.1 to be in line with ISO/IEC 27001 standard

9.2 Internal Audit

9.2.1 General

Is compliant with ISO/IEC 27001 standard? - YES

Shares the same as the previous requirement. Mislabelled as 10.2. Needs to be renamed to 9.2.1 to be in line with ISO/IEC 27001 standard

9.2.2 Internal Audit programme

Is compliant with ISO/IEC 27001 standard? - NO

Not present in current policy. However, this could be due to the size of the company

9.3 Management review

9.3.1 General

Is compliant with ISO/IEC 27001 standard? - YES

Mislabelled as 10.3. Needs to be renamed to 9.3.1 to be in line with ISO/IEC 27001 standard

9.3.2 Management review inputs

Is compliant with ISO/IEC 27001 standard? - NO

Not present in current policy. However, may not be applicable to Redback Operations as it doesn't have a typical management structure and as such the guidelines set in the standard would not be applied. But it does state that company goals and policies should be reviewed when necessary

9.3.3 Management review results

Is compliant with ISO/IEC 27001 standard? - NO

As stated for 9.3.2, a management review isn't applicable to Redback Operations

10. Improvement

10.1 Continual Improvement

Is compliant with ISO/IEC 27001 standard? - YES

More detail is potentially needed to specify how the company will do this. Mislabelled as Section 11.2 in the current policy. Needs to be renamed to 10.1 to be in line with ISO/IEC 27001 standard

10.2 Nonconformity and corrective action

Is compliant with ISO/IEC 27001 standard? - YES

Mislabelled as Section 11.1. Needs to be renamed to 10.2 to be in line with ISO/IEC 27001 standard

Summary

The current policy is on the right track to being ISO/IEC 27001 certified. However, there are some sections that either don't exist or require more detail to be compliant. The overall requirement structure was mostly adhered to, but all the later sections have the wrong numbering structure and as such made it difficult to keep track of each requirement. As mentioned throughout this review, Section 12 is supposed to have links to other policies that are referenced in the policy but there are no links present currently. This needs to be addressed. There also needs to be policies created for some of the assets mentioned in the scope (those are listed in its respective section).