Sri Lanka Institute of Information Technology

A picture containing text, clipart

Description automatically generated

Assignment Report 02

IE3102

**3. Specific document tools**

**Enterprise Standards for Information Security – IE3102**

**B.Sc. (Hons) in Information Technology**

**Student Details**

|  |  |
| --- | --- |
| **Student ID** | **Student Name** |
| IT22560094 | Ranasinghe R.A.D.T.M |

**Contents**

[**Specific Document Tools 4**](#_Toc179802482)

[**Statement of Applicability 4**](#_Toc179802483)

[**SOA documented tool 5**](#_Toc179802484)

[**Asset registry 6**](#_Toc179802485)

[**Asset Registry Documented tool 7**](#_Toc179802486)

[**RACI matrix 8**](#_Toc179802487)

[**RACI Matrix Documented tool 8**](#_Toc179802488)

[**Risk Register 9**](#_Toc179802489)

[**Risk Registry Documented tool 10**](#_Toc179802490)

[**References 11**](#_Toc179802491)

# Specific Document Tools

## Statement of Applicability

The list of information security measures you are implementing within your organization is included in the Statement of Applicability (SoA) [1] The list of controls is directly extracted from Annex A of ISO 27002, which is a standard that is based on ISO 27001 [1]. Statement of Applicability is a crucial component of your ISO 27001 accreditation.

How to construct a Statement of Applicability (SoA) for ISO 27001:

1. Purchase a copy of ISO 27002:2022.
2. Create a spreadsheet in Microsoft Excel.
3. Create an entry in the Statement of Applicability Spreadsheet for each ISO 27002 control.
4. Provide proof that the restriction applies to you.
5. List the controls that don't apply to you.
6. Continually examine whether the controls are appropriate.
7. Preserve the ISO 27001 control review meeting notes.

## SOA documented tool

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Asset registry

The register of all objects that store, transfer, or process data is known as the physical asset register. Data asset registration is also necessary. It's important to note a few important details concerning assets [2].

We'll need to write down some fundamental details like serial numbers and asset owners. Following that, we'll examine the data that the devices process as well as its classifications, criticality, and other factors.

The ISO 27001 standard does not specify which information must be included in the asset inventory; in addition to the asset's name and owner, you are free to include other pertinent details like the item's category, location, notes, etc [2].

We consider all devices, even those that are frequently overlooked by users, like switches, routers, wireless access points, and removable media.

The person who oversees the ISO 27001 implementation project typically builds the asset register. Typically, this is the Chief Information Security Officer, who gathers all the data and ensures that the inventory is maintained.

## Asset Registry Documented tool

A screen shot of a computer

Description automatically generated

A black and white grid

Description automatically generated

## RACI matrix

ISO 27001 RACI matrix basic concepts

* Responsible: The people who carry out the necessary work to finish the mission.
* Accountable: Indicates the person who will be ultimately responsible for the outcomes of an activity and who will assign the work to the people who will carry it out.
* Consulted: Those who sought to be heard regarding the relevant action and with whom there is two-way communication are referred to.
* Informed: Indicates people who requested to be kept informed of the activity's progress and with whom there is only one-way communication.

Where to document the RACI matrix

The project sponsor oversees securing top management support, and the RACI matrix can be documented separately or as part of a project plan. The schedule, budget, and communication plan for the project, among other project documents, should provide specific information regarding these duties. A single "R" denotes the performance of an operational part of the activity, while roles indicated as "A/R" denote responsibility and management activities [3].

## RACI Matrix Documented tool

A screenshot of a computer

Description automatically generated

## Risk Register

Because ISO 27001 is a risk-based system, the level and inclusion of controls are determined by the amount of risk [4]. You record the risk in a risk register, assign it a risk score, and choose how you're going to handle it. Your residual risk is then calculated using the risk score you recorded following the change [4]. The management review team meeting includes the assignment of risks to owners and the tracking and management of action plans [4].

Risk management, the procedure for managing risks, and the risk register are simple [4]. They serve as the information security management system's building block [4].

Process of creating a risk register:

1. Make a two-tabbed Excel spreadsheet.
2. Mark up the document and insert a reference field.
3. Add a field for external references and describe the risk.
4. Add a field for assets including a Threat Field
5. Add a Field for Vulnerabilities and a field for outcomes
6. Include a CIA Field and Place a Current Control Field there
7. Add a Field of Impact and a Field of Likelihood
8. Construct a Risk Score Field and construct a Treatment Field
9. Add a Field for the Treatment Plan and add a field for the treatment owner.
10. Add a field for the treatment date and add a field for residual risk.

## Risk Registry Documented tool

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

# References

|  |  |
| --- | --- |
| [1] | "statement-of-applicability-iso-27001/," [Online]. Available: https://hightable.io/statement-of-applicability-iso-27001/. |
| [2] | D. Kosutic, "Asset management according to ISO 27001: How to handle an asset register / asset inventory," Advisera, 2023. [Online]. Available: https://advisera.com/27001academy/knowledgebase/how-to-handle-asset-register-asset-inventory-according-to-iso-27001/. |
| [3] | R. Leal, "RACI matrix for ISO 27001 implementation project," Advisera, 2018. [Online]. Available: https://advisera.com/27001academy/blog/2018/11/05/raci-matrix-for-iso-27001-implementation-project/. |
| [4] | "risk-register/," [Online]. Available: https://hightable.io/risk-register/. |