Australian Government
Department of Education, Skills and Employment

ISO 27001 Risk assessment and treatment

V2.0 May 2022

ISO 27001 risk assessment and treatment

This document is intended to provide a high level overview of the concept of risk assessment and treatment in an ISO 27001 context. As ISO 27001 is being used globally, there are significant preparatory resources which are easily accessible to providers at little or no cost. There is an audit and certification body infrastructure that can be used to obtain assistance implementing ISO 27001 initially, and when ready, to gain certification.

This document is not intended to duplicate the existing body of knowledge.

What is risk assessment and treatment?

Risk assessment is probably the most complex part of an ISO 27001 implementation. Assessing and treating your risks is the most important step at the beginning of any information security project. It sets the foundations for managing information security in your organisation.

Why is it so important? The main process when implementing ISO 27001 is to identify the assets requiring protection; consider the threats that could occur to their confidentiality, integrity or availability; assess the likelihood and consequence of each risk to each asset, and then find the most appropriate ways to prevent, detect or respond to each risk (ie treat your risks).

Although risk assessment and treatment can be complex, it can be broken down into the following basic steps:

1. Develop your risk assessment methodology for consistency

Rules need to be defined that describe how to risk management is conducted in your business so your entire organisation does it the same way. This ensures outcomes from different risk assessments in different parts of the business can be compared. The biggest practical problem with risk assessment is that different parts of your organisation might perform it slightly differently. It is also important to define upfront what an acceptable level of risk is. Consider the guidance in ISO31000 as a baseline approach.

2. Identify and assess your risks

Once the rules are defined the next step is to start identifying which potential problems could arise. List all your businesses assets including information, systems and other things important to your business that require protection, then consider the threats and vulnerabilities related to each of those assets. Assess the impact and likelihood for each combination of asset and threat or vulnerability to give the associated level of risk to your business.

3. Implement risk treatments

Not all risks are equal. Focus on the most important risks to your business, those which are unacceptable.

There are four ways to mitigate an unacceptable risk:

1. Apply security controls (from ISO 27001 Annex A and from the Information Security Manual (ISM) or additional sources) to decrease the risk's likelihood or consequences until the risk is acceptably low.
2. Transfer some of the impact to another party – such as by purchasing an insurance policy. Note that this will not change the likelihood of this risk event occurring. It will simply reduce the dollar cost of responding to the event.
3. Avoid the risk by stopping an activity that is too risky, or by doing it in a completely different fashion.
4. Accept the risk – this might be appropriate where the cost of mitigating the risk would be higher than the damage itself.

Take your building as an example of an asset. There is a risk your building will burn down in a fire. You could:

1. install a fire alarm and sprinkler system to suppress the fire and alert the fire brigade to come to your assistance
2. buy a fire insurance policy. Note this would result in the insurance company giving you money to rebuild, it does not change the likelihood that the fire happens
3. rebuild in a material that doesn't burn, which is likely to be more expensive
4. accept the risk of losing your building to fire

4. Document the results in your Risk Assessment Report

This step entails documenting the results of your organisation's decisions so far. Your Risk Assessment Report can easily be checked periodically in the future to make sure it still reflects your situation.

5. Create your Statement of Applicability

Your Statement of Applicability shows all the possible security controls that you have considered in response to the risks you have identified. It identifies which controls have been selected for inclusion in your ISMS (or not selected) and the rationale for each decision. It also lists the current implementation status and expected implementation date for every control that has been selected for inclusion in the ISMS (see step 6 below).

This document is very important because your certification auditor will use it as their main guide for their work. It is also critical to the department's accreditation decision and forms part of your RFFR milestone 2 and milestone 3 submissions.

6. Create your Risk Treatment Plan

The purpose of the risk treatment plan is to define exactly who is going to implement each control, in which timeframe, with which budget, etc.

There is a myth about ISO 27001 that it is focused entirely on IT. IT alone cannot protect information. The ISO 27001 framework considers your business as a whole, covering areas such as physical security, personnel security, supplier security and a range of other business security areas.

There are many different ways to implement controls. They can focus on any combination of people, processes and technology. Your Risk Treatment Plan documents how your organisation will implement your plan and leave only acceptable risks. The output from your risk treatment plan can be efficiently documented in the SoA, describing which controls will be implemented, by who, and when.