Australian Government

Department of Education, Skills and Employment

Using ISO 27001 to meet your RFFR accreditation requirements

Overview

This document highlights the differences between an industry standard ISO 27001 and what the department needs to be able to assess your ICT environment as part of the Right Fit For Risk (RFFR) approach to accreditation.

The ISO 27001 is a very flexible framework which can be used in a variety of industries and sizes of organisations. Organisations use it by incorporating the requirements of their industry into the controls they will be certifying.

For providers working with government data, that means incorporating the Australian Government Information Security Manual (ISM) controls into the scope of your certification. You can find the latest version at www.cyber.gov.au/ism.

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.

Background

The Digital Partnership Office website includes details of RFFR's extensions to the usual ISO 27001 certification requirements, including details of the department's core expectations of providers. If you have not already read these, download and review these documents before moving on.

Before jumping into evaluating your ISO 27001 status

At this point, it is assumed that providers have already submitted the RFFR Questionnaire. Completing the questionnaire and spending time with the department in reviewing your responses will have highlighted key areas. This will help to concentrate your initial focus and bring about a better understanding of the department's requirements.

Providers should:

- ✓ **SPONSOR**: identify a sponsor within your organisation to support your journey towards ISO 27001 certification. Documentation on this step is already available on the Learning Centre.

- ✓ **SCOPE**: determine the scope of your certification requirements. What are you certifying? Consider stakeholders, physical boundaries, legal requirements, business activities, personnel and logical boundaries (data). By establishing the scope you will be able to define and document your information security management system (ISMS) for your business. The department has published a Scope template on the Digital Partnership Office's website for optional use by Providers.

- ✓ **GAP ANALYSIS**: perform a gap assessment to identify areas requiring focus. This will allow you time to fix non-compliances and to plan improvements before the certification audit. The department have published a SoA template on the Digital Partnership Office's website to assist with the gap assessment. Please also refer to the document "Gap Analysis vs Risk Assessment" for useful details.

- ✓ **STATEMENT OF APPLICABILITY (SoA)**: This is the central document in your ISMS. It links your requirements to the organisation's risks and the applied treatments to the risks. Your SoA will be one of the central documents used by your certification auditor. Please refer to the document "ISO 27001 Importance of the SoA" for useful details. The department have also published a SoA template on the Digital Partnership Office's website for optional use by Providers.

What is an Information Security Management System (ISMS)?

An ISMS is an organisational approach to managing its security. It comprises people, physical locations, ICT systems, policies and procedures for systematically managing the security of an organisation's sensitive data. An ISMS helps organisations to manage risk and ensure business continuity by preventing, detecting and limiting the impact of a security breach. It values people and processes, as well as technology, to mitigate risk.

Why is an ISMS Important?

Your ISMS is a holistic approach to IT security which acknowledges the inter-relationship between these elements and the benefits gained when all three work together. An ISMS can help co-ordinate all your security efforts (physical, personnel, ICT systems and insecurity) coherently, consistently and cost-effectively. With the additional benefit of having everything in one place.

It is important that the ISMS is an integrated part of your organisation's processes and overall management structure. Your organisation's documents are not just for an auditor to read. Management's endorsement and the sponsor's circulation of the ISMS will show staff your commitment and support for this new concept. It will help people understand what is expected of them and why it is important for them to implement it.

What is in my ISMS and who is going to use it?

Your ISMS needs to cover your important information, people, physical and logical assets. What is important to the success of your business (And therefore requires protection) should of course include everything you require to deliver and manage services under your deeds with the department..but are there other aspects of your business that require security? By including all your security requirements in one place, it is harder to overlook the important details. This ensures that all staff are aware of information security and consider it in the design of processes, information systems and controls. It provides a systematic approach to manage risks and enables staff and management to make well-informed decisions on security investments.

The requirements set out in the ISO 27001 standard are generic and are intended to be applicable to all organisations, regardless of type, size or nature. The international standard, ISO27001, specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS within the context of your organisation.

It is anticipated that your ISMS will be scaled in accordance with the needs of your organisation.

Next steps

The next steps are:

1. document your scope
2. define and document your SoA
3. document and implement your ISMS.

If you choose to submit your scope and SoA to the department for feedback before your ISO 27001 stage 1 audit, please use the Security Compliance Support mailbox on SecurityComplianceSupport@dese.gov.au . Feedback will be given in the order that submissions are received.

Frequently Asked Questions

Is submission of our organisation's scoping document and SoA required before engaging the auditor?

No, review by the department is not mandatory.

In keeping with the old adage – measure twice and cut once – the Digital Partnership Office (DPO) can review your organisation's scope and SoA and give you feedback against our accreditation requirements prior to commencing the Stage 1 audit. To get the most benefit from this exercise it is worthwhile spending the time to make sure you are completely comfortable with your scope and SoA before you share them with us.

We have had some SoAs submitted which have not demonstrated consideration of ISM sourced security controls (or the other peculiarities of the way their business interacts with the department) alongside the ISO 27001 Annex A controls. They were based on simply the normative ISO 27001 Annex A controls. Fortunately we were able to highlight this omission before their auditors were involved and avoid a costly re-audit.

It is better to get it right initially than having to ask your auditor to return to do additional work.

Does the department require an IRAP assessor to be involved for the ISO 27001? Can an IRAP assessor give an ISO 27001 certificate?

ISO 27001 auditors are not ISM specialists so they are relying on your organisation to apply the ISM in the context of your organisation and document it within your SoA. Using the department's SoA template (ISO to ISM map) will assist your organisation to document this. While the use of an IRAP assessor may assist your organisation, the department does not require an IRAP assessor to be involved.

An IRAP assessor may also have expertise in relation to ISO 27001, but they are separate areas of expertise with separate qualification and experience requirements to be able to legally issue certificates.

JAS-ANZ is the accreditation authority for ISO 27001 certification bodies in Australia and New Zealand.

Your Scope

How to define the ISMS scope

The main purpose of setting the ISMS scope is to define which assets you intend to protect. Identify what information is important to the operation of your business and what is beyond your control. It does not matter whether this information is stored within your company offices or in the cloud. It does not matter whether this information is accessed from your local network or remotely. Also identify and describe the ICT systems and other assets that you require in order to carry out your business (including service delivery and management under your deeds with the department). These all require protection and should be within the scope of the ISMS.

A documented scope is also important when you are ready for certification. It is an expliucit requirement of ISO 27001 Cl.4. The certifying body will check whether all the elements of the ISMS work well within your scope. The business areas or systems that are not included in your scope will not be checked.

When defining the scope, consider:

- the external and internal issues referred to in *ISO27001 clause 4.1*
    - for example, the need to meet tender requirements to operate
- the need and expectations of interested parties referred to in *ISO27001 clause 4.2*
    - for example, who are the types of interested parties, different departments, types of job seekers require different aspects to be considered. Note the department's explicit requirements for RFFR accreditation and describe what that actually means, as if a third party unfamiliar with RFFR was reading the scope and needed to understand this need and expectation.
- interfaces and dependencies between what is within the ISMS scope and the outside world
    - for example, interaction with other systems and other parties outside the boundary of the ISMS, use of a centralised IT or HR team and processes.
    - Dependencies are any processes relied upon that are outside the scope of your organisation's ISMS. If your organisation restricts the scope of your ISMS to cover only part of your business, the processes which are external to your scope are treated as unrelated. It does not matter that they are internal to your broader business.
    - Interfaces are the ways your in-scope business interact with the world outside of that scope. Consider how your people, processes and technology within your scope interact with those outside of it.

Limiting your Scope

If your entire business is not to be covered by your ISMS scope, it may be restricted by:

- processes
- sections
- locations
- exclusions.

The problem when the ISMS scope is not your whole organisation is that the ISMS must have interfaces to the "outside" world. The outside world are not only your clients, partners, suppliers etc, but also your organisation's internal business areas, systems, people and processes that are not within the ISMS scope. A business area which is not within the scope needs to be treated in the same way as any external supplier and

suitable security measures must be put in place to prevent, detect and respond to security incidents that may occur at the boundary between the ISMS and these out of scope business areas (eg. responding to risks that sensitive data or systems could be accessed by a person in an out of scope business area).

Think about the interfaces and dependencies to determine whether the scope is sufficient. If your proposed scope is set too tightly, the interfaces and dependencies may make it impossible in practice.

If there is no interface, it cannot be separated. For example two business areas in separate rooms have the door between them as an interface so it is possible to segregate them physically. However, if they are in the same room, segregation would not be possible. If the employees both within and outside the scope use the same local network (with no segregation) and have access to various network services (eg printers), then there is no way to control the information flow to only inside the scope. They could not be separated.

Consider the situation where a business areas within your scope is using the services of your purchasing area, which is outside your scope. The in-scope business areas should perform a risk assessment of your purchasing area to identify if there are any risks for the information for which they are responsible. Moreover, those two business areas should sign terms and conditions between them for the services provided.

Why is this necessary? Your auditor must certify that within your scope you are able to handle the information in a secure way, they cannot check any of your business areas outside the scope. The only way to handle such a situation is to treat such business areas as if they were external companies.

Providing employment services within a larger business

If providing employment services is only part of your business, consider the business implications if your entire business is not covered within the scope of your ISMS. Compare the cost and benefit of covering your entire business by the ISO 27001 certificate with the cost and benefit of a reduced certificate scope.

Consider the implications of creating an artificial wall to ring fence parts of your business. Do you have a separate business that delivers the employment services in a way that you can restrict any impact from your broader business? If you choose to focus on only your employment services business, your organisation will need to put into place artificial processes and controls to ring fence that business.

Consider whether you rely on the same physical walls to restrict access to your office. Manage people using the same HR processes across your entire business. Manage IT using the same people and processes with the same network and instance of Active Directory to manage your entire business. The cost and disruption to your organisation's usual business processes increases the more integrated your business processes and controls are across your entire organisation.

Compare the cost of the controls with the cost of a data breach or data corruption – what would be the cost to your organisation if job seekers are not paid or are physically harmed? What about your organisation's reputation? Future business opportunities?

There is guidance freely available on the internet regarding how to set the scope of the ISO 27001 certification. This is a decision where your sponsor and business unit leaders will need to be heavily involved.

Documenting your scope

Your scope can be clearly defined in a couple of pages. There are template documents available to help formalise the scope decisions and formally document the results. The department does not require the use of any specific template. However an example scope template is available through the DPO website which can be modified to allow providers to work through the scoping decisions to best support your business and the ISMS journey.

Typical headings used, supplemented with the core expectation areas from the *Right Fit For Risk Overview*, include:

- purpose of the scope document
- interested parties, their security needs and expectations
- processes and services – including which of the department's programs are covered
- organisational units or business areas
- assumptions, dependencies and constraints
- locations and physical boundaries – addresses, floorplans, physical security considerations
- logical boundaries – data flow diagrams, network security considerations
- supply chain management (third party risk management)
- exclusions from the scope
- roles and responsibilities
- Overview information describing the organisation's current and future state in relation to the RFFR Core Expectation areas including
    - the ACSC's Essential Eight strategies to mitigate cybersecurity incidents
    - restricted access controls – identification, authentications and authorisation; privileged access; event logging and auditing
    - information security risk management
    - information security monitoring – vulnerability management, change management
    - managing cybersecurity incidents – detection, reporting and managing
    - Personnel security - onboarding and security awareness.

These headings are set out in the example template, located on the DPO Website.

Context of your organisation for ISMS purposes

Your organisation will have already identified the department's accreditation requirements in accordance with clause 4.2(b), which includes consideration of ISM-sourced controls and implementing controls to support the RFFR Core Expectation areas as a minimum.

As the department will be relying on ISMS assessment / certification reports as the basis for making our accreditation decisions, please ensure your ISO 27001 certifying body is aware of the importance of validating all the controls that you have identified are applicable to your ISMS (including the ISM controls).

Currently all the department's programs are required to be within the scope of your ISO 27001 certificate. On engagement to deliver employment services, the department's core expectations of providers are that they:

- understand their operational risks
- have adequate controls in place to prevent identified risks
- be capable of responding to a data breach
- protect information assets as well as physical assets
- commit to continual improvement as cyber risks change and develop.

This is much broader than an IRAP assessment of a system. The ISO 27001 takes a holistic approach as IT alone cannot protect information and your business. This framework considers the business as a whole,

covering areas such as physical security and human resources management. Critically assessing these non-IT factors are important to getting the full benefit of this holistic business approach.

Your organisation will determine the boundaries and applicability of the information security management system to establish its scope. You will have already identified the department's accreditation scoping requirements in accordance with clause 4.3(b).

In determining your scope, you need to consider your interested parties and ensure compliance with all your organisation's legal and contractual requirements. While we cannot give an exhaustive list, we highlight that the department is an interested party and your organisation's deed with us is contains various contractual requirements that must be considered. Your deed refers to program data and related records. Keep in mind this is a broad requirement. In addition to the data you obtain from, or upload into departmental systems, also think about things like emails, calendar invitations and reports generated to manage your business.

For the avoidance of doubt, for providers this includes:

- your own ICT environment
- any Third Party IT systems that you use
- any cloud services that you use
- any interactions with Third Party Employment and Skills (TPES) systems that you use
- assurance mechanisms you use to gain confidence about the standards of security operated by your subcontractors and service providers.

To get the most benefit from this program, the department will be working closely with organisations to ensure your scope and SoA meets both the department's and your organisation's needs. Each provider's SoA will be unique. It is dependent on your ICT environment, use of systems, services, subcontractors and service providers, and how you manage your ecosystem.

While not necessary, the department's input into your scope and SoA may limit provider and auditor misunderstandings on documentation, processes and the audit effort required. It is better to get it right initially than having to ask your auditor to return to do additional work.

Use of a TPES

The centralised controls within an accredited TPES have gained accreditation directly with the department. The department's accreditation can be leveraged as a source of assurance that the TPES is capable of being used by Providers for specified Programs, in a secure manner. The DESE Programs and the features accredited are specified within the department's accreditation letter, which is available on the DPO website.

Interaction between your organisation's own environment and any accredited TPES used are within the scope of your own assurance to ensure all transfer points are appropriately safeguarded. These are the areas where your organisation has responsibility to implement and manage configurations and users. These responsibilities, details of any action plans the vendor has to address identified weaknesses, any excluded features and any other considerations are explained in the department's accreditation letter.

It is important that Providers access the accreditation letter and ensure that they understand any areas where their TPES use differs from the accredited configuration. Providers must also understand their own obligations for securing their instance of the TPES and ensure that appropriate controls responding to these "shared obligations" are included in the ISMS.

Use of a cloud service

The Australian Signals Directorate (ASD) historically made an assessment of the centralised controls within cloud services listed on their Certified Cloud Services List (CCSL). That list ceased in July 2020 and all ASD cloud certifications are now void.

Providers are wholly responsible for ensuring that the cloud services they choose to use are appropriately secure and meet the unique security requirements of their deeds with the department (including data sovereignty requirements). The ASD has published a range of guidance materials designed to assist the secure adoption of cloud services across government and industry, which is accessible through the ASD website at https://www.cyber.gov.au/acsc/view-all-content/programs/irap/asd-certified-cloud-services. It includes the following publications:

- Anatomy of a Cloud Assessment and Authorisation
- Cloud Assessment and Authorisation - Frequently Asked Questions
- Cloud Security Assessment Report Template
- Cloud Security Controls Matrix

Similar to use of a TPES, the interaction between your organisation's own environment and cloud services used are within the scope of your own assurance to ensure information assets are appropriately safeguarded. Even if a cloud service offers an independent certification as assurance of its security posture, it is important to understand the scope of the certification (and match it to your own usage), as well as understanding the customer specific responsibilities that exist where your organisation has responsibility to implement and manage controls.

Information security risk treatments

When determining all the controls that are necessary to implement the ISMS and respond to security risks (clause 6.1.3(b)), we draw your attention to the note "Organisations can design controls as required or identify them from any source." Your deed with the department includes compliance with the ISM.

The department have released a SoA template (ISO to ISM mapping document) to help make the exercise of identifying OFFICIAL controls with the ISM easier. This template is available on the DPO Website. Revised versions will be released periodically to reflect the changes made to the ISM through the year.

Subcontractors and consortiums

Lead providers

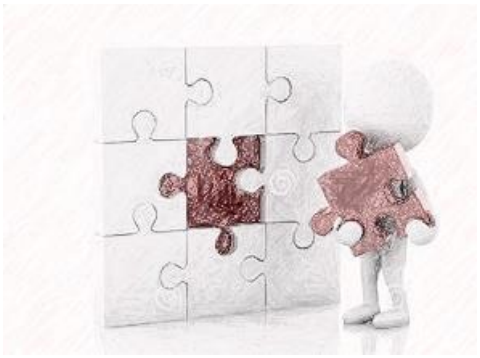
The organisation who is the deed signatory is legally and morally responsible for ensuring that the subcontractors used also comply with the security, privacy and data sovereignty requirements of your deed. If there is a weakness in an entity in your supply chain it poses a risk to your organisation. ISO 27001 addresses this risk with control objective A.15 (Supplier Relationships) and related ISM sourced controls. Don't leave a hole in your ISMS. There are a suite

of documents available on the DPO Website to assist in the management of third parties.

Where the department also has a deed with a subcontractor your organisation uses, that subcontractor will be pursuing the department's accreditation for their services under that deed. You may be able to obtain some degree of assurance through their RFFR accreditation. However, you need to consider the scope of your subcontractor's accreditation and whether the timing of their accreditation will meet your own needs. This is particularly relevant where you use a subcontractor who falls into a Category 2A or Category 2B provider classification because their milestone deliverables to the department may not fall due until a later date than your own submission is due.

There is the option to include subcontractors within the scope of your own audit and have your auditor test the controls in place at their sites too. Alternatively you could arrange a supplier audit – a second party audit – of their environment. Which approach is best for your organisation will be dependent on the specifics of your situation.

Subcontractors

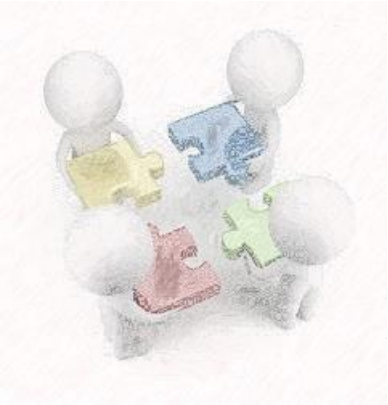


You are part of the bigger picture in the lead provider's compliance requirements. Your lead provider will be looking to you for assurance that you understand, have implemented, and will operate an effective standard of security over the life of your subcontracted services delivery.

Your lead provider will need to demonstrate their approach to managing supply chain security. This may require that you include certain security specific requirements in your subcontract, that you implement relevant security controls sourced from the ISM, and have a reliable method of assuring the lead provider that you continue to secure the information under your control to a standard that meets the lead provider's (and the departments) security requirements.

The department does not assess or accredit organisations that are not signatories to a deed.

Consortiums



Each organisation in the consortium is responsible for assuring their own environment. Lead providers should take an active role in communicating requirements to all members of the consortium.

Each organisation that is a signatory to the deed is considered a Provider in its own right and must seek RFFR accreditation. Only when all consortium members have achieved RFFR accreditation can the entire consortium be accredited.

It is important to remember that if there is an issue with one organisation's accreditation it will have an effect on the deed held and operated by all organisations.