# ISO 27001 and Right Fit For Risk (RFFR) - issues to avoid

As ISO 27001 is a very flexible framework it can be used in a variety of industries and sizes of organisations. This makes it vital to ensure it suits YOUR organisation's requirements from the begining. If you are using the ISO 27001 certification to meet the department's RFFR program or as tender evidence, you need to ensure it meets these requirements.

It is vital to understand that although RFFR closely aligns with ISO 27001 it is not a standard ISO 27001 certification. RFFR can be thought of as "ISO 27001 Plus" because it extends the standard's generic process by:

- requiring Providers consider a significantly broader set of potential security controls (the combination of ISO 27001 Annex A and Australian Government Information Security Manual (ISM) controls applicable to OFFICIAL information). ISO 27001 encourages organisations to consider and include relevant industry specific security controls in their ISMS.
- identifying Core Expectation areas, and associated ISM controls, that all Providers are expected to implement.

In March 2021, these extensions were codified as a formal ISO 27001 Scheme known as the DESE ISMS Scheme. Providers can be certified against this scheme to demonstrate that they have implemented an Information Security Management System (ISMS) which conforms with the requirements of the ISO 27001 standard, and which also reflects the departments RFFR requirements.

Providers may still choose to be certified against ISO 27001, but in doing so they must take steps to ensure their Certifying Body clearly understands that the certification approach must recognise and validate a Statement of Applicability (SoA) document that includes significantly more (and more specific) security controls than they may be used to seeing. The Certifying Body will need to adjust their "standard" certification estimate to account for the need to review and validate the implementation of these controls. This is most accurately done if the Provider can first supply a SoA that clearly identifies which controls have been selected for inclusion in the ISMS, and which controls have been deemed "not applicable".

It is critical that Providers get their ISMS scope and SoA right from the start, as it drives the rest of the ISO 27001 / DESE ISMS Scheme certification process.

Organisations can also use this certification more broadly by including any other security requirements (for example, State government security requirements) into their Information Security Management System (ISMS) and SoA for certification.

This document aims to assist providers avoid missteps we have seen to date to make this a smooth process. They have been categorised into:

- details included in your ISMS
- completeness of the SoA
- completeness of the scope
- address Right Fit For Risk (RFFR) Core Expectations

# Details included in your ISMS

## Socialise your ISMS to ensure everything you need is included

The purpose of your ISMS is to help uplift the security maturity of your whole organisation – not just to meet the department's requirements. Sponsors should ensure that this objective is understood by all business areas so that the ISMS can be designed to respond to all their security requirements and obligations.

**ISMS Scope:** A critical element of designing the ISMS is defining its scope. Documenting the ISMS Scope is a specific requirement of ISO 27001 Clause 4 and this is best done collaboratively across your business. Share your draft scope widely within your organisation to ensure that it accurately reflects:

- legal and contractual obligations relevant to security
- stakeholders with an interest in your organisation's security, and their specific needs and expectations
- the context of your organisation including its structure, services provided, key roles, physical locations, key ICT systems and a description of the information stored, processed or transmitted that requires a degree of protection
- your subcontractors and any third party service providers that could access (or adversely impact) your systems and the important information they store or process.

**Statement of Applicability (SoA):** The second critical artefact that defines your ISMS is the SoA. While ISO 27001 provides a "bare minimum" security controls model at Annex A to the standard, it also states that organisations should add any industry-specific security controls that it considers are appropriate to mitigate risks.

For providers delivering services on behalf of the Australian Government and handling OFFICIAL or OFFICIAL:Sensitive information (as defined in the Protective Security Policy Framework), this means due consideration of security controls contained in the ISM.

It also means that providers should ensure appropriate security controls are included in their ISMS to respond to unique security requirements within their contractual agreements. For example, the department's deeds contain requirements relating to data sovereignty that require specific controls regarding the physical location of data centres and infrastructure supporting cloud services. Controls designed to ensure these requirements are met should be included in the SoA (and should be identified as applicable to the ISMS).

Broad socialisation of your ISMS at the design stage can help ensure such requirements are captured in the ISMS Scope, reflected in the organisation's security risk assessment, and that appropriate security controls can be included in the SoA and ultimately implemented.

The Digital Partnership Office offers a service to review your ISMS scope and SoA prior to official submission, to confirm it is on track to meet RFFR requirements.

# Completeness of the SoA

## Be sure to demonstrate your consideration of ISM controls in the SoA

By considering only the normative Annex A controls from the standard, the level of detail required by the ISM and the accreditation letters relating to third party employment systems or certified cloud products can be overlooked. The accreditation requirement is an ISO 27001 Assessment Report which aligns with the ISM. If this is not done initially, organisations risk the need to rework their documents and have the ISO certifying body return to cover the revised scope, SoA and implemented controls.


If the starting point – the SoA – has missed controls, the resultant audit cannot be fit for the purpose of our accreditation. Ensure that all Official ISM controls are included in the SoA in accordance with:

- clause 6.1.3 (b) – the ISM is the "additional source" mentioned by the standard, and 6.1.3 (c) – noting the control objectives and the controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed to protect and manage your business.

## Secure use of cloud services accredited by the Digital Transformation Authority (DTA) and Third Party Employment and Skills (TPES) systems accredited by the department

**Be sure to consider the factors highlighted in the certification report when securing your cloud service**

Providers readily identify whenever a cloud service they use is government certified. However, they often have not obtained a copy of the independent certifier's certification report nor assessed their interaction points with the products used. Therefore, those providers were not able to benefit from the government's accreditation exercise to ensure that they were using the product safely and securely as intended. They left themselves exposed where controls and configurations within their own responsibility were not understood, documented and managed.



These cloud services are typically provided using a shared security model. This means that there are controls and configurations that your organisation needs to implement to use the service safely. For example, providers often remain responsible for authorising users of the system, granting them privileges, configuring event logging features and proactively reviewing event logs to identify potentially suspicious activity.

These and other customer obligations should be specified in the vendor's certification report and it is critical that Providers read the report to understand what their service provider will do, and what the Provider must do, to operate the service securely.

**Be sure to obtain sufficient assurance about the services you use**

Some Providers incorrectly believe that engaging a third party to manage and operate systems on their behalf means they are not responsible for these elements of security. In reality, a Provider always remains accountable for the standard of security that is applied in support of their business. Providers must implement oversight controls suitable to ensure that their subcontractors and other service providers are aware of, understand, implement and operate security controls that are appropriate to the nature and scope of their services.

This means a discussion with each of your service providers to review the set of ISO 27001 Annex A and ISM OFFICIAL controls and determine which are relevant to the service provider. Ideally these will be included in the agreement that you have with your service provider together with performance reporting obligations that generate confidence the security controls are being effectively operated on your behalf.

Your third party service providers may offer an ISO 27001 certificate, IRAP assessment or other independent certification as evidence that they operate securely. It is important to look at the scope and results of their Assessment Report to ensure that it covers the third party's controls relevant to the services, systems and sites that are relevant to you. Determine how your organisation can compensate for any non-conformities identified by their certifying auditor.

Providers also need to define, implement and operate a process to periodically ensure that your third party service providers continue to meet their security obligations to you.

## Completeness of the Scope

**Broader than technology controls to manage how your organisation delivers its services securely**

The Scope document tells the story of your ISMS by setting the context for your business, describing key services, locations, stakeholders, ICT systems/devices and ultimately the information that will be covered by your security management system.

Consider how your staff access the data they need to do their jobs – your corporate network and devices; any cloud services used; Wi-Fi used; video conferencing and IP telephony used; both in-house developed applications and non-in-house developed applications used. Where staff are using non-corporate owned devices, there are obligations to be considered regarding maintaining the security of those devices and what happens if the device is lost or when the person leaves. The ISM highlights obtaining a legal opinion before allowing staff to bring their own devices (BYOD) for this reason.

The scope should also describe how your organisation transfers information between ICT systems, storage locations and external stakeholders, and provide an overview of the main mechanisms you will use to ensure that sensitive information requiring protection does not spill over into systems and storage locations outside of the ISMS boundary to create an information security incident.

**Production data in a non-production environment**

An area that software developers who are not used to working in the government sector often overlook is in relation to test data.

If data that requires security protection is copied into testing or development environments (or used in any way in a non-production environment) the data must be protected using the same level of security as in the main operational ("production") environment.

# Addressing RFFR core expectations

## Level of Essential Eight maturity

The Core Expectations represent the most important group of security controls that Providers can implement to mitigate against targeted cyber intrusions. The Core expectations include controls to implement the Australian Cyber Security Centre's "essential eight" cyber security strategies.

It is important that Providers consider their threat profile and select a target maturity level for the essential eight. Large organisations and Australian Government departments are expected to target Maturity Level 3, while smaller organisations with less complex ICT environments and small holdings of sensitive data may decide to target Maturity Level 2 or 1.

Regardless of your target level, the department expects to see that you identify relevant controls as applicable to your ISMS and define a plan to implement them systematically over time. Providers must attain at least Maturity Level 1 at the point of their accreditation and are expected to uplift their maturity levels progressively from then on.

When determining your target maturity level you will need to understand the risk to your business and consider the likelihood of risks eventuating if you were to achieve each maturity level in turn. For instance privileged users often have the ability to bypass security controls. When privileged users are permitted to use their accounts to access email and the internet, these accounts could create far reaching damage if they were to be compromised by an adversary. If your organisation has not implemented application whitelisting, a malicious actor can exploit this to introduce malware to compromise the user's account even if antivirus software is installed. If local devices can attach removable drives, or cloud file storage or webmail services are not blocked, the compromised account could be used as conduits to extract your intellectual property and your holdings of personal data. Considering the potential impact that these events could have on your business operations and your ability to meet legal and contractual obligations, could lead you to target higher maturity levels in each Essential Eight strategy.

## Managing and reporting cyber security incidents and data breaches

**Missing reporting requirements**

Providers are subject to different reporting requirements depending on their varying legal obligations. There are circumstances where Providers may be required to report security incidents to a range of external parties including program participants, the Provider's executive, the department, the Australian Cyber Security Centre, the Office of the Australian Information Commissioner, the organisation's ISO 27001 certifying body, the media or the police. Identifying the parties that should be notified of a cyber security incident and

planning when and how each would be notified is an important aspect of security incident management that can be overlooked by private sector organisations.

Even if a Provider uses an outsourced ICT service provider, cloud service or TPES the responsibility to report data breaches remains with the Provider. An organisation can outsource processes, but cannot outsource responsibilities or legal obligations. The department has released a suite of documents to assist providers to manage their third parties. These are available on the Digital Partnership Office website.

Providers may require specific contractual terms and service level agreements with their service providers to ensure prompt reporting of cyber security incidents and data breaches to enable them to meet their reporting obligations. There are reporting timeframes relevant to "notifiable breaches" under Australian Privacy law and the European Union's General Data Protection Regulations (GDPR) applicable to data relating to European citizens.

It is important to remember that security does not necessarily mean privacy. Privacy is a possible outcome of security, but it is possible to have a privacy violation without a security breach.

Before an event happens, take the time to calmly determine who is authorised to respond to cyber security incidents and data breaches – and how. This will benefit your organisation both in your ability to promptly respond, and in not causing confusion in your messaging.

## Event logging and auditing

**Not taking the time to develop pro-active alerts based on your business risks and needs**

Event logs can be generated to record all activities. The value from this comes in sorting through the haystack to quickly find things that look like a needle. If event logs are not audited (reviewed), nothing can be learned and cyber intrusions or malicious activities cannot be identified. On the other hand, it is equally important to ensure that event logs can be readily filtered to exclude informational events and records of everyday activities that don't assist with the identification of possible security incidents. Restricting the activities that can be performed with privileged accounts also assists with this.

To give focus, identify your organisation's crown jewels (most sensitive data, most important systems etc) and high risk activities that threaten their confidentiality, integrity or availability. Build alerts that can identify if these activities ever occur. For example, what event logs would indicate if system administrators were accessing important systems in the middle of the night? Are database contents being exported from key systems and transferred outside the organisation? Are there high volumes of failed login attempts? Are user accounts being added and removed from powerful access roles or groups without authorisation? There is guidance in the ISM regarding possible events that should eb logged in relation to operating systems, databases, websites etc. although the set of possible events to be recorded and monitored will be unique to your organisation and the possible threats that you face.

The time taken to target event alerts will be rewarded by timely identification of security incidents enabling an effective response. Promptly identifying the incident can allow your organisation to minimise the harm involved.

Consider how long logs need to be kept to facilitate this audit process. If they are deleted too quickly, your organisation may not be able to identify inappropriate activities performed. The logs may also be needed for a court case or a Royal Commission hearing.

## Data sovereignty

**Not restricting privileged access to foreign nationals**

Providers need to consider whether the individuals they employ are Australian citizens, permanent residents, or have a right to work in Australia. For most roles, this is sufficient. However, where a person has privileged access to systems or data, it is critical that they are Australian citizens of permanent residents to ensure an appropriate connection with Australia. This is equally important where a Provider has given privileged access to systems or data to a service provider.

**Not validating that data in products and tools used cannot be stored, sent or accessed from offshore**

This is a critical term within the provider deed that needs to be positively addressed. If adopted, the requirement for privileged users to be Australian citizens or permanent residents will typically also be addressed in most cases.

Most providers specifically contract with the cloud services vendor to ensure that the service they are consuming is hosted and supported from onshore only. It is the use of communication and collaboration tools where providers have generally been caught out.

Also consider other ICT services that store or process "program-related" data. For example, an organisations finance system may keep records of payments made for items to assist job seekers secure a job, which are then claimed back from the Employment Fund.

Some organisations have chosen to use an offshore system to support their non-government business. If this is relevant to your organisation, check that your scope is set so that the interactions with the business area using the offshore system is outside the scope of your ISO 27001 for accreditation, and check to ensure that appropriate preventive and detective mechanisms are in place regarding the risk that sensitive information be transported outside the ISMS scope into these other systems. Refer to *Using ISO 27001 to meet your RFFR accreditation requirement* for more details about the importance of controlling the interfaces, like the physical walls and the logical walls provided by your network and firewalls to segregate the business areas.

## Physical security and working remotely

Physical security measures were typically understood and actively being addressed. Providers have taken on board the high level comments around working remotely in relation to RFFR physical security core expectations as described on the Digital Partnership Office website and contained within Deed guidelines.

# Next steps

Consider the areas highlighted above where other providers have experienced missteps, in conjunction with the other documents available on the Digital Partnership Office website. Ensure your ISO 27001 sponsor is heavily involved setting the scope, developing the SoA and drafting the ISMS.