Documenting your scope - Remove before use

Your scope can be clearly defined in a couple of pages. The department does not require the use of any specific template. This example template is available in the Learning Centre and may be used as the basis for working through the scoping decisions to best support your business and ISO 27001 journey.

Headings are provided as a recommendation of inclusion, italic text is guidance to be considered and should be removed.

Examples used are not definitive or exhaustive. Other information may be relevant to your circumstances.

Typical ISO27001 ISMS scope headings

1. Purpose of the scope document

Briefly explain the purpose of this scope document. Consider how it supports some of the ISO27001 clauses. The scope should act as a foundation and reference point for the rest of the Information Security Management System (ISMS).

Briefly explain the purpose of the ISMS. Consider the need to protect the confidentiality of sensitive information (to prevent intentional or accidental leaks), the need to maintain the integrity of your business information (to ensure accurate accounting and to ensure correct delivery of services), and the need to maintain the availability of your services (to ensure uninterrupted delivery of services to the public). State your legal, regulatory, and contractual obligations. For example (this list is only an example, you must consider what is applicable to your business):

- *Specify the RFFR requirements as per your Deed(s) (see the Department's Right Fit For Risk website and the Universal Guidelines accompanying the Deed)*
- *Protective Security Policy Framework*
- *Information Security Manual (ISM)*
- *Australian Privacy Act 1988*
- *Health Records Act 2001*
- *Children, Youth and Families Act 2005*
- *Charter of Human Rights and Responsibilities Act 2006*
- *Disability Act 2006*
- *Commission for Children and Young People Act 2012*
- *Mental Health Act 2014.*

2. Interested parties, their needs and expectations

Interested parties are your internal and external stakeholders. Consider people and organisations who expect you to maintain a level of information security (e.g. customers, partners, employees, business owners, etc.), and those whom you expect to maintain a level of information security (e.g. employees, service providers, etc.). State each stakeholder's security-related expectations and briefly describe the corresponding information or services that are expected to be secured.

Interested parties could include (this list is only an example):

- *Government departments, agencies, and regulators (state each one, e.g. Department of Education, Skills and Employment, Department of Social Services, State government entities)*
- *Customers (e.g. job seekers, participants, etc.)*
- *Other clients (e.g. referral recipients)*
- *Employees (e.g. senior leadership, system owners, IT managers, users, etc.)*
- *Shareholders or business owners*
- *Suppliers (e.g. internet service provider, IT service provider, cloud service providers, other business service providers, etc.)*
- *Media (e.g. consider the newsworthiness of suffering a data breach or interruption of service)*
- *Anyone else considered important for your business.*

It is important to note in this section that the Department of Employment, Skills and Education requires its providers to implement an Information Security Management System that conforms with the requirements of the ISO 27001 standard, which considers the inclusion of security controls sourced from the Australian Government Information Security Manual (ISM), and which includes, as a minimum, ISM-sourced controls supporting each of the RFFR Core Expectation areas. The department further requires any certification of the ISMS to include verification of not only the ISMS conformance with ISO 27001 requirements but also the implementation status of all selected controls (both controls sourced from ISO 27001 Annex A and controls sourced from ISM, and any other sources relevant to the Provider's business. The department has other explicit requirements relating to data sovereignty as specified in its contracts with the Provider. The Department has documented its requirements in the Provider's Deeds, associated guidelines, and on the Right Fit For Risk website.

3. Processes and services

State the services and business processes that will be covered by the ISMS. Consider government programs and the associated services provided under your own deed, as well as any you provide on behalf of other deed holders. Consider briefly describing how cases are managed from start to finish, how you interact with customers and other clients, how you obtain, handle, and store sensitive information, etc. This will help to identify the physical and logical boundaries later in this document.

4. Organisational units or business areas

List and briefly describe the organisational units or business areas that are involved with the in-scope processes and services. Consider providing an organisation chart that includes any sub-contracted entities and highlight the in-scope vs out-of-scope areas. For example, you may have a core business area that manages cases and provides services to clients, a corporate business area that provides internal services such as accounting, and an ICT business area that maintains the ICT infrastructure. The ICT area might include multiple sub-units, such as internal ICT management, an external ICT service provider, and multiple external cloud service providers. Ensure you briefly describe the services provided by each internal and external business area, including how they interact with each other (where applicable). You may declare some business areas out of scope if they are not required to deliver services to customers, do not handle sensitive data related to your services, and do not have the potential to access this data.

5. Assumptions, dependencies and constraints

State any assumptions, dependencies and constraints affecting your scope. Assumptions should only be made for things outside your control (e.g. you cannot assume that a service provider has sufficient security in place; you must obtain assurance for yourself, such as via a security report). For example:

- *You may be dependent on a contracted service provider to implement and manage certain security controls on your behalf*
- *You may be dependent on service providers (e.g. cloud service providers) to maintain equivalent security standards in their own systems*
- *Your ability to implement some controls may be constrained by existing contracts or budget limitations.*

6. Locations and physical boundaries

Refer to physical security core expectations in the Universal Guidelines and the Right Fit For Risk website.

State the full addresses of each physical location for which the in-scope services and business processes are conducted, and state which services or processes are conducted at each location. Ensure you include supporting business areas (e.g. if you operate your own servers, include their locations).

This should include floorplans for each location that show publicly accessible areas, working areas, and locations of ICT devices.

Briefly describe the physical security measures in place at each location. Consider the external features (e.g. locks, cameras, security patrols, etc.) and internal features (e.g. locked cabinets for network devices).

7. Logical boundaries

Document all ICT systems (including user devices, servers, network devices, VPN, cloud services, etc.) that are used by the in-scope services and business processes. This should include a diagram that shows all systems and external services as well as the flow of information between each system. For external services (e.g. cloud service provider), state the geographic location of the data centre. System connections and information flows are generally easier to understand in diagrams, particularly for those who are unfamiliar with your organisation.

8. Supply chain management (third party risk management)

Describe how you manage the risk of using third party services, including the use of artificial intelligence (AI) capabilities. Consider the risks to the confidentiality and integrity of information and the availability of your services when using a Third Party Employment System (TPES), cloud service providers, managed ICT service providers and other third parties that have the potential to impact in-scope information and services. Consider how you can be assured that your security requirements (e.g. RFFR requirements including data sovereignty) are being met by your service providers. Note that many cloud service providers publish their security reports and certifications online, while managed ICT service providers may need to be made aware of your security requirements. Refer to the three "management of third parties" downloadable resources on the Right Fit For Risk website.

For the use of AI, specify if your business uses any form of AI software or capability. If so, provide details about the software, how it is used as part of the in-scope processes and services, its integration with other systems, and what data it processes, stores, or communicates. Consider how this meet RFFR's data sovereignty requirements. When addressing any usage of AI, consider the below two guidelines for use of Generative AI as per the 'Interim guidance on government use of public generative AI tools':

- *Users should be able to explain, justify and take ownership of their advice and decisions.*
- *Assume any information users input into public generative AI tools could become public. Users should not input anything that could reveal classified, personal, or otherwise sensitive information into public Generative AI tools.*

9. Exclusions from the scope

State any parts of your business that are excluded from the scope of your ISMS. While some business areas may not be directly involved with the delivery of your services, consider the impact to your business if those areas were to suffer a data breach or interruption of service. Note that all systems that are connected to the in-scope network should remain in scope, as those systems may introduce vulnerabilities to the entire network.

10. Roles and responsibilities

Describe the key organisational security roles, the responsibilities of each, and who holds each role. This helps individuals understand what their roles and responsibilities are and allows for ISMS performance to be accurately reported to senior management.

Plans to address RFFR Core Expectation areas

Please demonstrate your appreciation of the RFFR Core Expectation areas and the requirement that controls supporting these must be present in your ISMS. Use the headings below to describe your current level of control in each area and your intent to implement additional security controls to address the RFFR Core Expectations.

11. Essential Eight strategies to mitigate cybersecurity incidents

Refer to cyber security core expectations in the Universal Guidelines and the Right Fit For Risk website. The latest maturity model is available at the Australian Cyber Security Centre (ACSC) website: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

For each strategy, assess your current maturity level based on the statements in the maturity model above, state the requirements that you currently meet, and state your target maturity level for each essential eight strategy. Consider presenting this section as a table.

Application control

What is being done to prevent the execution of unauthorised software?

Patch applications

What is being done to identify and mitigate known security vulnerabilities in application software?

Restrict Microsoft Office macros

What is being done to block untrusted macros?

User application hardening

What is being done to limit the potential for security vulnerabilities in user applications (focusing on application-specific security settings and removing unneeded functionality)?

Restrict administrative privileges

What is being done to limit actions taken by accounts with powerful access?

Patch operating systems

What is being done to identify and mitigate known security vulnerabilities in operating systems?

Multi-factor authentication

What is being done to protect against accounts being inappropriately accessed?

Regular backups

What is being done to maintain the availability of critical data and systems to allow your business to recover quickly if required?

12. Information security risk management

Refer to cyber security core expectations in the Universal Guidelines and the Right Fit For Risk website.

Briefly summarise the processes that are in place for identifying, assessing, and treating risks.

13. Information security monitoring

Refer to cyber security core expectations in the Universal Guidelines and the Right Fit For Risk website.

Vulnerability management

What monitoring practices are in place to identify, prioritise and respond to security risks?

Change management

What processes are in place for implementing routine and urgent system changes? How are unauthorised changes identified and managed?

14. Managing cybersecurity incidents

Refer to cyber security core expectations in the Universal Guidelines and the Right Fit For Risk website.

Detection

How are security incidents detected? How is data consolidated and analysed? Consider manual and automated processes involved.

Reporting and managing

How, and to whom, are security incidents reported? Consider all legal and contractual requirements. Who manages the response, repercussions, and future prevention? How is evidence preserved?

15. Restricted access controls

Refer to cyber security core expectations in the Universal Guidelines and the Right Fit For Risk website.

Identification, authentication and authorisation

What user identification and authentication practices are used to ensure access to systems (and data they process, store, or communicate) is controlled? How are they the same and different for user accounts, privileged accounts and service accounts?

Privileged access

How is privileged access restricted in both number of accounts and the functions these accounts can perform?

Event logging and auditing

Describe your event logging strategy. How are audits of event logs conducted? Are pro-active alerts used? Does your strategy reflect the data that is important to how you run your business – your crown jewels?

16. HR processes

Refer to personnel security core expectations in the Universal Guidelines and the Right Fit For Risk website.

What HR processes are associated with offering employment, on-going requirements to maintain employment, changing roles internally or exiting employment? Consider specialised position knowledge, competency or license (eg Working With Vulnerable People) requirements applicable to the States in which you operate.