4 Scoping

This chapter outlines what is meant by scope and how to decide the scope for an ISMS. It forms part of Stage 2 – Planning, assessment and evaluation in the Toolkit Route map.

Key topics

- **How scope can mean something different depending on the context**
- **How to successfully define the scope of an ISMS**
- **What to consider when scoping outsourced/third-party services**

4.1 Introduction

Scoping is a critical part of planning the roll-out and implementation of an information security management system (ISMS). An organisation is often sub-divided into smaller ISMS scopes (e.g. an ISMS relating to a particular project, service, audit or policy etc). In either case, the scope determines the boundaries and applicability of information security management and controls. Scope will be shaped by:

- the business of an organisation
- the needs and expectations of relevant interested parties
- the organisational structures that are currently in place.

It is important to correctly define and agree scope with the relevant senior stakeholders at the outset, so as to manage expectations, agree in advance what is (and is not) to be achieved, and ensure that applicable security requirements for relevant systems are identified and implemented.

4.2 Different scopes

An organisation will typically have multiple scopes relating to information security. For example, the overall scope for information security is likely to be considered as the entire organisation. However, in most Higher Education environments it would be difficult to tackle the whole organisation in one go. Similarly, it would be an almost impossible task to certify the entire organisation against a standard such as ISO/IEC 27001 or PCI DSS. Thus the organisation should consider having multiple, smaller, scopes, each of which is tailored to the protections required for the information it encompasses. For example, the scope of a PCI DSS audit is determined by protecting only payment cardholder data.

The scope of an ISMS should take account of the organisational objectives, structure, location, assets, technology and/or people involved in the delivery of those objectives.

Starting with a reduced scope (as opposed to trying to tackle too much too quickly) may also increase the chances of success, and of achieving the objectives of the ISMS in a reasonable time.

Examples of scopes include:

- scope of an ISMS for the purposes of ISO/IEC 27001 certification
- scope to which a policy applies
- system components potentially affecting the security of cardholder data for PCI DSS compliance
- scope of an audit
- scope of specific information security projects and services
- scope of responsibility in contractual agreements.

4.3 How to define the scope of an ISMS

4.3.1 Identify what needs to be protected

One of the first questions to ask is “what needs to be protected”? It is likely that there will be many information assets that need to be protected in order to support the organisation in achieving its business objectives. It is important to understand which of these the organisation considers to be most important, and so a risk-based, prioritised approach should be taken to scoping. In order to establish that assets are actually worth protecting, the organisation should justify why each asset requires protecting.

The scope of an ISMS may initially be defined to include only specific processes, services, systems or particular departments. Success stories can then be presented as a business case for expanding the scope of the ISMS, or creating another, separate scope with different requirements and protections.

In order to make the scope entirely clear, especially to third parties, it is a useful exercise to identify what is not in scope (e.g. the activities of the HR department).

Either way, the scope should clearly define what is being included, based on the business objectives and information assets to be protected, and it should be clear that anything else is out of scope.

4.3.2 Understand the organisation

The scope of an ISMS should take advantage of the organisational, management and governance structures that currently exist. The person(s) tasked with managing information security across an organisation should therefore begin by identifying relevant structures, and any constraints set by the structures that currently exist. If there is no governance currently in place then progress will be limited when trying to identify requirements and risk, and implementing security controls across the entire organisation. The scope of any initial work may therefore be to implement an appropriate management and governance framework (see Chapter 2, Information security governance).

Where the scope of an ISMS is defined by the need to protect a particular asset (e.g. cardholder data) or delivery of an objective (e.g. certification against ISO/IEC 27001) then it is important to first understand system components and structure involved in the delivery of relevant services. This may include, for example, obtaining system diagrams showing data stores and flows and relevant IT systems. Personnel involved in managing and delivering all system components will then likely be considered “in scope”.

4.3.3 Ensure endorsement of scope

The scope of an ISMS, policy, project or audit etc. should be endorsed and formally agreed by the relevant senior stakeholders (top management), to manage expectations and clearly define the objectives that will be delivered. Failure to correctly identify and formally agree the scope in this way is likely to lead to unclear objectives, difficulties in measuring progress and ultimately decrease the chances of success.

For those managing information security, it is important to consider the boundaries of control and authority. If, for example, the security of services or systems in a particular department are beyond the control or authority of the owners of the ISMS, they should not be included in the scope.

In the context of an audit, agreeing which systems are in scope may be particularly important so as to ensure that it is clear which systems the auditor is authorised to access and under what circumstances. Failure to obtain such authorisation in advance could even lead to a breach of law (such as the Computer Misuse Act 1990).

4.3.4 Monitor and review

The scope of an ISMS, policy, audit or project is not static and may evolve over time as circumstances, threats, technologies and requirements develop. Therefore scoping is not something that should be done once at the beginning of a project and then forgotten about. Rather, scope should be monitored and reviewed at regular intervals and/or in the light of significant changes. In the event of an audit (be it for internal control or certification purposes) one of the first things an auditor should do is to review and assess the appropriateness of the scope. Factors that might affect/change the scope of an ISMS include:

- time dependencies: e.g. the scope of a particular ISMS and/or security project may only be applicable for a particular time period
- change in regulatory environment
- changes/updates to standards and/or third party requirements

- change in organisation (e.g. organisation structure changes)
- identification of non-conformities and/or incidents indicating incorrect scope
- overall maturity of ISMS (scope may increase over time)
- change in processes and practices (e.g. ceasing certain activities)
- outsourcing services.

4.4 Outsourcing and third parties

Outsourced: Any element that is not wholly controlled, managed, built, implemented and maintained by staff employed by the organisation.

Cloud services: A shared computer-based storage solution for data that is based in a virtualised computer environment. Cloud services can describe any shared environment, which can be provided both locally or outsourced.

All organisations will outsource some activities to third parties. Some third parties are taken so much for granted that, when questioned, staff do not remember them – e.g. the cleaning teams, waste removal contractors, and potentially accountants or auditors. Their activities may not be under scrutiny, yet they may have the highest levels of access.

There are many reasons why an organisation may want or need to outsource some (or all) of its IT provision. As information technology changes and evolves extremely quickly, it can be more cost-effective to outsource some of an organisation's IT solution, or to use cloud storage or services. Economies of scale means that large data warehouse-style storage facilities can offer cheap storage and extremely good availability. Externally hosted services may also provide specialist IT knowledge and support that is not available within the organisation.

If managed properly, outsourced IT or cloud technology carries no greater risk, and arguably less risk, than managing an in-house IT environment. However, poorly sourced or managed outsourcing, or inappropriate cloud provision, can be extremely risky.

4.4.1 Scoping considerations for cloud and outsourcing services

When cloud services are used, there can be multiple parties involved in the production of the overall service. For example, infrastructure and software services can be provided by different organisations.

Scoping in this context will involve having a clear understanding of the system components involved and the security responsibilities of each service provider. These security requirements should be included in any contractual agreements.

When outsourcing, it is vital to define the boundaries of applicability, responsibility and accountability.

Responsibility for implementing security may be outsourced, but the accountability cannot be, and so it is therefore important to understand the scope of an ISMS in this context. Put simply, when it comes to meeting certain security requirements, outsourced functions or processes will be in scope for an ISMS, but the suppliers are unlikely to be. It is up to the organisation to decide how it may be assured that services provided are of an appropriate standard.

For further information, the ICO has produced a guide on the use of cloud computing, and UCISA has a briefing paper on cloud computing.

4.4.2 Scope and third party contracts

Understanding an organisation's relationship with third parties is extremely important to ensure security for the business and the information that it holds, especially where information security may be put at risk by third party activities, even though their activities are not obviously related to information (e.g. cleaners).

When working with any third party, it is important for information security that the following are defined:

- Legal responsibility, accountability and insurance: all the parties' responsibilities must be detailed and understood. Running through a risk assessment process will uncover many areas where accountability needs to be defined. Disaster planning and incident response is also a good way of verifying that ownership and insurance responsibilities are correctly scoped.
- Access and authorisation: it is essential to make sure the rules and regulations for who can access what are clearly defined. If the organisation is allowing contractors into buildings, it should understand who has the keys or access codes; and who ensures the staff are trained and things are secure. Out of hours

office cleaning staff often have more physical access to an organisation than even the most trusted day staff. Access to IT systems and data should also be considered.

- Disclosure and privacy: the organisation should define and categorise the information that is being used and shared, and specify the applicable rules and regulations.
- Contract terms: The terms of contracts with third parties should be clearly defined to make sure that all parties are clear on the expectations of the work to be conducted, and sanctions or liabilities in the event of default are assigned.

4.4.3 Questions when outsourcing IT or using a cloud provider

When selecting a third party, questions such as the following should be considered:

- What data are going to be on the outsourced system? Do the data include any sensitive information, or have special requirements?
- What laws or regulations apply to the service provider who is supplying the IT provision? If it is a company outside of the EU, how will that interact with the requirements of the data which it will handle? Where will the data itself be stored?
- Who needs access to the IT solution? Is it something that needs a lot of physical involvement or does it not need any attention for many months?
- Are there restrictions on who administers the system? Who will the administrators be and who controls the access rights?
- Where is the system physically housed? Is the facility secured, who is it shared by, and who controls the access?
- Does the outsourced service provider themselves outsource any of their provision (e.g. off-site back-ups)? How do they manage the security controls which their third parties are handling?
- What service level is expected or provided? What levels of assurance for confidentiality, availability and integrity of data are there? Check the policies in place within your organisation.
- At the end of the business relationship, how will it be possible for the organisation’s information to be extracted from the third party environment in a usable form?
- What provisions (if any) are in place for compensating the organisation for the impact of a business continuity incident or disaster (e.g. loss or exposure of information)?

4.4.4 Example: third parties and PCI DSS

A service provider may supply remote firewall management, or paper shredding, services to the organisation. The service provider themselves would not need to be PCI DSS compliant, but the service provided to the organisation should be compliant and would fall in scope for the PCI DSS assessment of the organisation.

Service providers can demonstrate PCI DSS “compliance” either by having their service included in the organisation’s assessment, or by undergoing an assessment themselves. In either case, the services provided that may affect the security of cardholder data must be considered to be in scope. It is the responsibility of the organisation to demonstrate compliance – rather than the service provider.

4.4.5 Example: outsourced scope in an HE environment

A large organisation is divided into distinct units that use different types of data and have different requirements for that data. The organisation is federated into many different smaller units that each require basic IT. The basic IT provision consists of desktop and file services for general information.

In one area of the organisation, IT is provided by an external company employed by the organisation. The units using this “group IT provision” treat it as outsourced provision and have service level agreements in place. The reason it is considered outsourced is that, when the scope was defined, the control of the system administration, access control, physical security and changes to the systems were out of the control of the individual units.

One of the units using the “group IT provision” requires a fully validated and highly secure database for one project. This is a very specialised system that neither the unit IT nor the “group IT provision” can provide on its own. The unit employs a third party software provider to build, maintain and support the database, but, because of the sensitivity of the data, it has been built on the servers and storage provided by the group IT provider, and is managed by the IT support personnel employed by the unit.

Every element of this outsourcing must be clearly understood to manage the scope:

- Where was the database physically housed?
- Who has access to each part of the system from software to hardware?
- What provides the integrity checking?
- What and who ensures availability?
- Who provides the assurance of confidentiality?
- What laws and regulations are involved in each part of the system?
- What countries are involved?
- What service level provision is required by each of the parties?
- What security controls need to be considered?

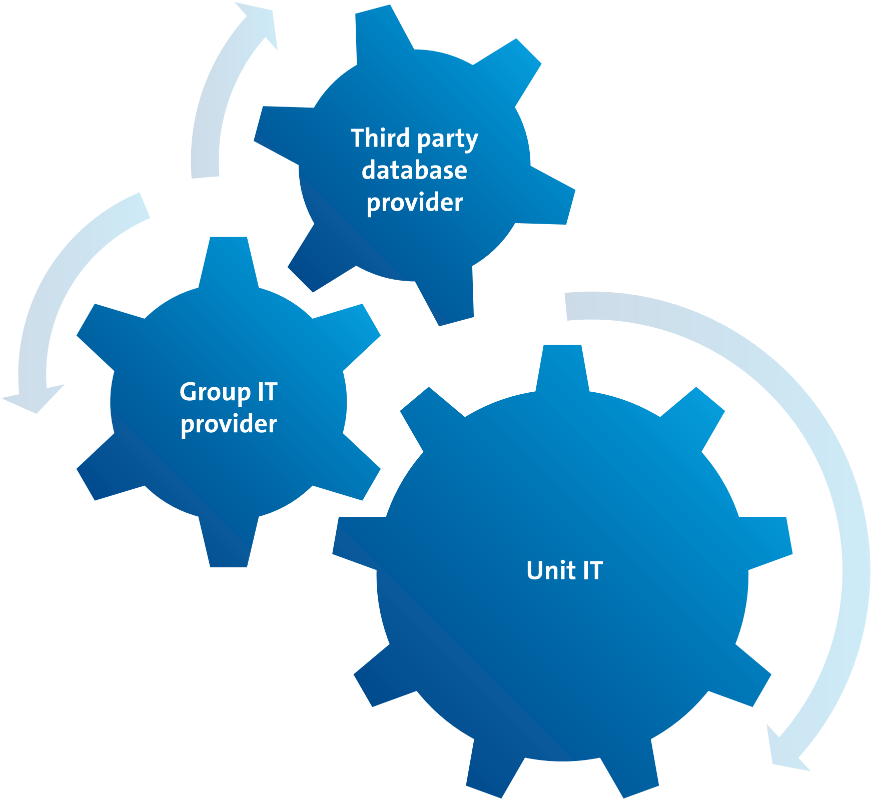

Figure 1: Illustrates the relationships detailed above.

Summary

- Successfully defining and agreeing the scope of an ISMS from the beginning is a critical success factor in the implementation of any ISMS – if the scope is wrong you will not know where you are going or when you got there!
- There are different scopes involved in implementing information security in an organisation, from high-level scopes covering the entire organisation, to the scope of a particular project or service
- Start small with one limited scope, demonstrate success and build from there
- Monitor and review, and if your scope is wrong then change it accordingly

Resources

Scope definition for a data safe haven – UCL, case study

Reading list

The Common Vulnerabilities and Exposures database:
www.ucisa.ac.uk/ismt18
https://cve.mitre.org/

UCISA briefing paper on cloud computing:
www.ucisa.ac.uk/ismt19
www.ucisa.ac.uk/publications/cloud.aspx

The Information Commissioner's Office's advice on choosing a cloud service provider:
www.ucisa.ac.uk/ismt20
https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf