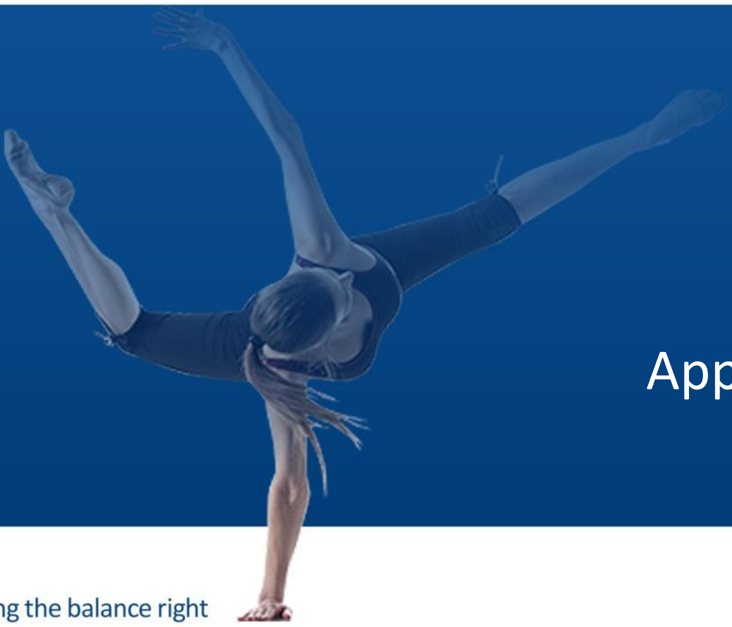
URM

ULTIMA RISK MANAGEMENT

Ensuring Your ISMS Scope is Appropriate for ISO 27001:2013



Getting the balance right

URM Viewpoint

1.0 Background

The importance of setting an appropriate information security management system (ISMS) scope has always been recognised as a key starting point in any ISO 27001 certification project. With the introduction of ISO 27001:2013 however, establishing an appropriate and meaningful scoping statement has become even more important. The purpose of this document from Ultima Risk Management Ltd (URM) is to outline some of the issues that have been encountered with historic ISO 27001 scopes, as well as providing its perspective on the scoping requirements of the updated Standard.

Since ISO 27001 was first introduced, a number of organisations have adopted a limited scope rather than certifying the whole organisation. The reasons why organisations would set a limited scope are numerous. It may be part of a phased approach where a 'pilot' scope is adopted as a first step or it may be a division or function of the organisation where confidentiality, integrity and availability of information is deemed to be of particular importance. Alternatively, the definition of the scope may have been influenced by an organisation's clients i.e. those functions which a client or clients are particularly interested in. All of these reasons are perfectly valid and there are many recognised benefits to starting off with a limited scope that is manageable and achievable, then building on the scope as confidence/skills/resources increase and as the organisation realises the many and varied benefits that certification brings.

However, there have also been instances under ISO 27001:2005 where some organisations have taken advantage of the limited scope option to certify part of the organisation that is not a significant contributor to key organisational outputs or is not satisfying the organisational purpose. In addition, where there is little top management involvement in a limited scope certification, this often results in conflicts of priority as the ISMS is seen as something 'X' department does in isolation, rather than it being embedded into the organisational culture and operation. With the introduction of ISO 27001:2013 however, a lot more consideration needs to be given to limited scope certifications and alignment with organisational objectives and the needs of interested parties.

2.0 Why is Scoping Different with ISO 27001:2013?

With ISO 27001:2013, a very strong emphasis is placed on the need to ensure that the ISMS is integrated into the organisation's processes and that the ISMS is compatible with and supports the strategic direction of the organisation. Alongside this, there is now a much greater focus on top management leadership and commitment to ensure that the ISMS does not operate in isolation to the rest of the organisation and that information security is fully embedded and considered organisation wide.

These changes of emphasis do not necessarily mean that a limited scope is no longer an option; however what it does mean is that there are things which need to be identified and established. Firstly, the department or function that makes up the limited scope would need to be of sufficient size to be deemed an 'organisation' or 'entity' in its own right delivering meaningful services. Also, in order to demonstrate senior/top management commitment and leadership, there would need to be at least one senior person actively involved within the scope who has accountability. In addition, there should be clear expectations defined for the limited scope's interested parties. Some of these elements (such as interested parties) were implied within ISO 27001:2005 but were not made explicit.

In the following sections, there will be a focus on Clause 4 of ISO 27001:2013 'Context of the Organization' and what this actually means to organisations that have an ISMS with a limited scope. However, as the information gathered during Clause 4 feeds into Clause 6.1 'Actions to address risks and opportunities', this may represent an opportunity for organisations to validate limited scopes by assessing whether significant information security risks to the organisation are covered within the in-scope department.

Understanding the organization and its context (4.1)

An organisation needs to determine the external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its ISMS.

Let us consider, as an example, the IT department of Company ABC, where the purpose of the department is to provide IT services to internal users only and where Company ABC is involved in manufacturing and provides no IT services to its clients. In this instance, under ISO 27001:2013 would the IT department represent an acceptable scope? We have already identified that the IT department needs to play a key role in assisting Company ABC achieve its purpose and needs to be of sufficient size to be classified as an 'organisation' delivering meaningful services, to be deemed a valid scope.

If the IT department meets the 'organisation' criteria, it then needs to determine the external and internal issues relevant solely to its own department e.g. the structure and roles within the department, availability of reliable qualified and competent workforce, stability of work force, service expectations from other departments within Company ABC (service level agreements, operating level agreements), legal and regulatory issues, and any Company ABC client expectations, which the IT department is subject to.

However, if Company ABC's internal and external issues affect the IT department e.g. if Company ABC's customer demographics may impact on the IT equipment maintenance windows or the technology which the IT department need to support, then it will be necessary to determine internal and external issues company wide.

If Company ABC has already identified internal and external issues for the whole company and the IT department knows which ones are relevant to it, then the IT department can use this information. However, if this assessment has not been conducted, then a decision will need to be made whether it is meaningful to the company for internal and external issues to only be considered for the IT department or would it be more appropriate to include the whole company. Remember, these issues feed into addressing risks and opportunities. Also, the identified company-wide internal and external issues could be a basis for justifying why a limited scope is appropriate.

Understanding the needs and expectations of interested parties (4.2)

Within this sub clause, the 'organisation' needs to determine interested parties that are relevant to the ISMS and the requirements of those interested parties with regard to information security. Interested parties include legal, regulatory and contractual requirements.

Using the IT department again as the 'organisation', it would need to determine the requirements from its customers, i.e. users within Company ABC. For users within Company ABC to provide this information to the IT department, they would need to know what legal, regulatory and contractual requirements Company ABC must adhere to e.g. information classification, information handling, backup and recovery requirements, business continuity arrangements etc. Often in reality though, organisations ask IT departments to tell them what they should do. In this case, the IT department could provide its clients (other departments) with details of its service offering which would then put the emphasis on those departments to agree/reject/negotiate an appropriate service offering. The IT department needs to ensure that the service offering includes all information security controls that are applicable to what it offers its clients not just the technical controls.

An effective approach of capturing this information is to conduct an internal workshop with 'interested parties'.

Determining the scope of the ISMS (4.3)

Organisations are also required to determine the boundaries and applicability of the ISMS to establish its scope. This requirement should be satisfied by considering those elements identified in

4.1 and 4.2, as well as the interfaces and dependencies between activities performed by the organisation and those that are performed by other organisations.

When the ISMS scope is not the whole organisation, the department or function within scope will have interfaces to the ‘outside’ world, with the ‘outside’ world being not only clients, suppliers, partners etc., but also other organisational departments that are not within scope. As such, a department which is not within the scope of the ISMS should be treated in the same way as an external supplier, or as a client, if they are receiving a service from the department within scope. The level of service should be determined through internal documents that would serve as ‘agreements’ e.g. policies, procedures, operating or service level agreements that confirm the in-scope department’s obligations.

The requirements involved with the ‘outside’ world have not changed in the ISO 27001:2013 but need to be fully understood to ensure that the scope remains appropriate and that other requirements of ISO 27001:2013 are implemented appropriately.

Information security management system (4.4)

As with all management system standards there is a requirement to establish, implement, maintain and continually improve the ISMS. As part of this process, the scope should continually be assessed to determine whether it remains suitable to the purpose of the organisation.

3.0 Implications for Organisations Setting an ISO 27001:2013 Compliant ISMS Scope

So what is within scope?

When undertaking audits on behalf of its clients, URM has previously come across a number of organisations which seem to blur the lines of what is within scope and what is not in scope, especially with regards to information. The new requirements place a clear, unambiguous need to detail the scope which will prevent ‘blurring’.

If we look back at the IT department of Company ABC as an example, information that would be within scope of their ISMS is everything created, owned or controlled by the IT department as well as any information entrusted to them by its interested parties. The IT department would need to ensure the information entrusted to them is protected in line with the needs and expectations of the relevant interested parties.

So what does an organisation need to think about when considering a limited ISMS scope?

7 Questions for Organisations with a Limited ISMS Scope

- Could your limited scope department or function be deemed to be an ‘organisation’ in its own right within the requirements of the new Standard?
- Is there a sufficient, demonstrable management commitment within scope?
- Can the boundaries, interfaces and dependencies be defined?
- Is it possible to ensure that processes undertaken by the ‘outside’ world are managed and controlled?
- Does the scope have top management representation and involvement?
- Are there defined expectations of the limited scope’s interested parties?
- Within the scoping statement, is there a justification for what is within scope and what is excluded from scope?

If the answer to the above questions is ‘yes’, then a limited scope is likely to be acceptable to the organisation’s certification body.

Summary

Scoping the ISMS is an important strategic decision that should be made by the organisation's top management. Where a limited scope is adopted, information security and business strategies should be aligned to reduce the likelihood of unmanaged information security risks existing or developing in the other parts of the organisation. The decision to adopt a limited scope needs to be taken with the knowledge that there will be a requirement to apply security controls at the perimeter of the ISMS, including some within the organisation, since the rest of organisation is the 'outside' world.

Top management is also required to demonstrate its leadership and commitment to the ISMS, irrespective of the size of the scope. These requirements can be achieved through communicating the importance of effective information security management, directing and supporting individuals to contribute to the effectiveness of the ISMS and supporting other management roles to demonstrate their leadership.

In addition, top management is required to establish information security objectives at different functions and levels, which are consistent with the organisation's information security policy and are aligned with the business objectives and are measureable (where practicable).