ISO 27001 – Gap analysis v risk assessment

V2. May 2022

Gap analysis versus risk assessment

A gap analysis can sometimes be confused with a risk assessment. Both can be helpful in identifying shortcomings in your organisation's information security posture. However, from an ISO 27001 perspective, they are quite different.

What is an ISO 27001 risk assessment?

Under ISO 27001 clause 6, a risk assessment is required to underpin the design of an Information Security Management System (ISMS). Completing a risk assessment is a crucial step in designing your ISMS because it shows where security controls are needed to help reduce the likelihood or consequences of security risks faced by your business.

Providers should identify the assets that require a level of security protection – for example, program-related data, personal information, commercially sensitive information, critical premises and systems, and so on. Then, apply a systematic approach to identify, understand and assess security risks that threaten the confidentiality, integrity and availability of these assets. Last, Providers should review ISO 27001 Annex A and the Australian Government Information Security Manual to identify possible security controls that could be implemented to reduce the likelihood or consequences of each risk to acceptably low levels.

The results of your risk assessment determine the nature of your information security responses.

What is an ISO 27001 gap analysis?

A gap analysis is an assessment of what you already have in place versus what you still need to do. The gap analysis should consider two main arms:

1. Identify current gaps in terms of **conforming with the requirements of the ISO 27001 standard**. ISO 27001 contains detailed requirements for any ISMS including the need to document a scope, assess and respond to risks, assign leadership roles, deploy adequate resources, operate the ISMS, evaluate performance over time and implement measures to help continuous improvement. These and other requirements are set out in clauses 4-10 of the ISO 27001 standard. Providers need to ensure that their ISMS reflects these requirements.

    - For Category 1 Providers, the current level of conformance with ISO 27001 and identified gaps will be verified in the independent Certifying Body's "Stage 1" and "Stage 2" assessment reports that form part of the Provider's milestone 2 (design) and milestone 3 (implementation) submissions respectively.

- Category 2A providers are required to self-assess their ISO 27001 conformance gaps and include details in their ISMS Self-assessment report included in the Provider's milestone 2 (design) and milestone 3 (implementation) submissions to the Department.

It is important to recognise a significant number of gaps are often identified in the design phase of the ISMS, which equates to RFFR's Milestone 2. It is important to identify these gaps during the design phase of the ISMS, so that Providers can carry out plans to address them in the implementation phase. These are expected to have been addressed during the ISMS implementation phase and there should be no (or few) gaps remaining at the point of the Provider's Milestone 3 submission.

2. Identify the current gaps in terms of **confirming where security controls are already in place, and where further action will be needed** to implement security controls either required by RFFR (core expectation areas) or which are otherwise appropriate to address the Provider's security risks. ISO 27001's Cl.6.1.3 (d) requires organisations to determine "…whether [necessary controls] are implemented or not." This could be met by identifying a binary implementation status (implemented/not implemented), although many Providers see benefit in tracking the implementation status of each required security control on a more progressive scale. Doing so recognises that even a partially implemented control can provide a degree of protection. For example, a control's implementation status could be one of the following:
    - 0 – control is not implemented nor planned (control is not relevant to the Provider's ISMS)
    - 1 – control is planned but not implemented
    - 2 – control is partially implemented, but full benefits cannot yet be expected
    - 3 – control is implemented but measurement, review and improvement processes are not performed
    - 4 – control is implemented and measurement, review and improvement processes are regularly performed.

    Again, it is important to recognise that during the ISMS design phase, and at RFFR Milestone 2, large numbers of relevant security controls will not be in place. However, identifying these gaps allows Providers to carry out plans to address them in the implementation phase. There should be no (or few) gaps remaining in the implementation of relevant security controls at the point of the Provider's Milestone 3 submission.

The department has published a **self-assessment report template** and a **Statement of Applicability template** that may assist Providers with documenting both these elements of their gap analysis. These are available through the Digital Partnership Office website.