Proven Process for Building an ISO 27001 Certifiable Information Security Management System (ISMS)

Pivot Point SECURITY

1 Understand Your Organization Context (Scope)

To develop an information security plan, it is critical to understand your organization, its business goals, and its information security expectations. **An easy way to think about this is to ask: What information do we need to protect? And what are the processes that act on that information?**

Understanding the processes requires you to understand and document the people, systems and hard assets (e.g., employees, contractors, vendors, hardware, software, physical offices, data centers, networks, etc.) that support these processes. **The easiest way to gather this information is via a sequence of interviews with an organizational cross-section of the right people.**

Put simply, scoping is about understanding everything that influences information related risk and associated risk management decisions.

2 Understand Your Current Information Security Controls

A big factor in any information security plan is, unsurprisingly, the strength and maturity of the current information security program.

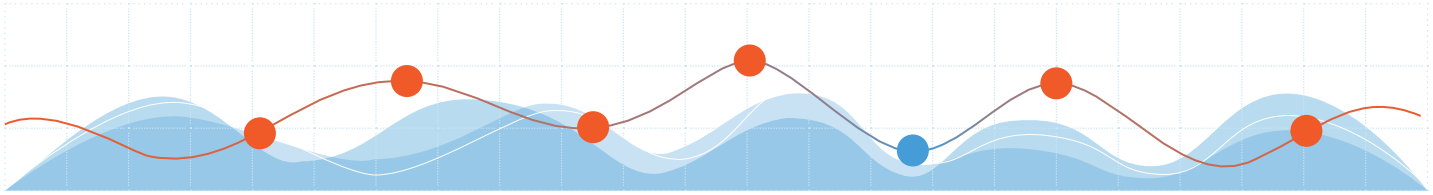
There is a lot of overlap between understanding this and understanding your organizational scope. We will gather this information during the scoping process as a "controls understanding/enumeration." The focus here is on understanding what information security controls are in place and the extent to which they are implemented and operated. It's not yet about "assessing" (passing judgement) as we won't yet understand your risk well enough to contextualize the assessment. Instead, it's about understanding/documenting what is being done currently.

The easiest way to gather this information is via artifact review (e.g., policies, standards, procedures, audit/assessment findings, penetration test results, incident reports, etc.) and discussions with your IT and information security staff.

Pivot Point SECURITY

3 Identify and Analyze Information Related Risk

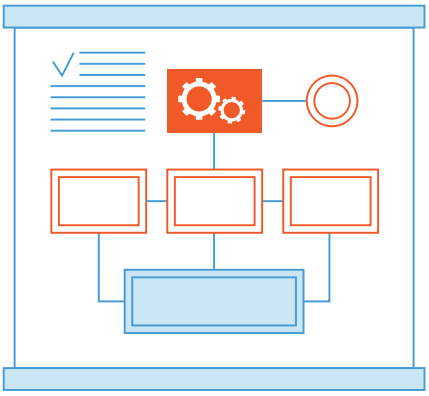
A key factor in any information security plan is the risks posed to your information assets and whether those risks are reduced to a level you are comfortable with. This process is often referred to as a **risk assessment**, which is comprised of risk identification and risk analysis.



During the previous two steps, we will have already identified a number of risks (despite the fact this was not yet our intent). **In this phase, the initial focus is on identifying all the additional risks to your organization's information related assets (risk identification).** Once we have a firm understanding of all the risks, we then assess (and document) which risks are currently being effectively managed by information security controls already in place, and which are not yet effectively managed (risk analysis). This involves consideration of the likelihood of a risk being realized, taking into account the current information security controls in place, along with the impact that risk realization would have on your organization.

In a nutshell, risk assessment is the process of identifying the universe of risks to your information assets and determining if/which of those risks necessitate improvements in your information security program.

4 Build a Risk Treatment Plan



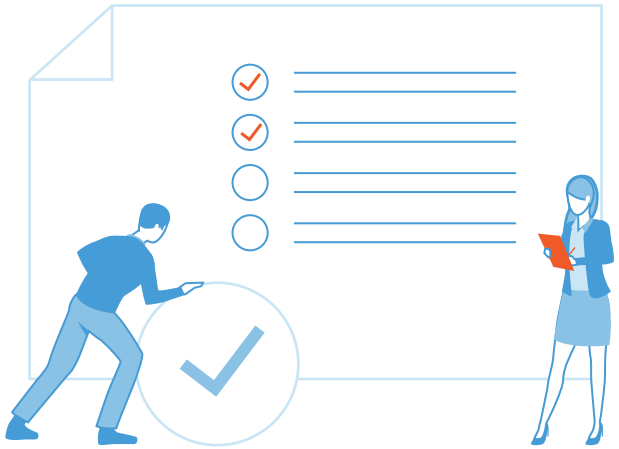
Once we understand which risks need to be addressed, we develop a plan to improve the security controls to reduce the risks to a level that the business is comfortable with (risk treatment). **That group of risk treatments (ideally approved by senior management) is generally referred to as a Risk Treatment Plan.** This is a simple, near-term, tactical Information Security Plan.

For many small to midsized organizations, this Risk Treatment Plan is all you will need until all risks of note are effectively managed. Longer-term, there may be some value in translating it to a more formal "strategic" plan that provides a longer-term vision for your information security program. Based on the above analysis and fact-finding, your information security plan will give you a prioritized view of planned improvements to more effectively manage risk in accordance with management's directive.

Proven Process for Building an ISO 27001 Certifiable Information Security Management System (ISMS)

Pivot Point SECURITY

5 Execute the Plan



A good plan prioritizes the necessary risk treatments based on **risk, level of effort, resourcing, and logical relationships** between different treatments.

Successful plan execution and operationalization positions you to verify the effectiveness of the existing and updated controls.

6 Internal Audit

A hallmark of **ISO 27001** is management "ensuring the suitability, adequacy, and effectiveness" of the ISMS.
A well-designed ISMS Internal Audit program is key to doing so. The goal of the Internal Audit is to identify what is working well and document what isn't and how it will be corrected (Corrective Action Plans (CAP)). Once complete, we work with management to review the results and formally approve the CAPs.

7 Certify the ISMS (the Plan's Operation)

The operation of your ISMS is formally certified by an ISO 27001 Registrar in a "Certification Audit."
Stage 1 of the audit is unusual in that it is purely focused on the design and operation of ISMS clauses 4-10. For that reason, ensuring that you are optimally prepped and or supported by an experienced **ISO 27001** implementer is key to a successful Stage 1. Assuming Stage 1 is successful, several weeks later the auditor will return for Stage 2, which concentrates on the design and operation of Annex A controls. Understanding the audit program, its link to your risk assessment, and the auditors background are keys to a smooth Stage 2.

ISO 27001 CERTIFIED

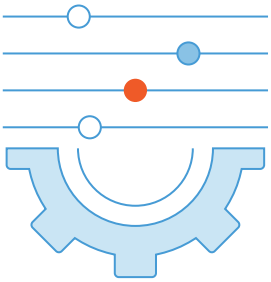
info@pivotpointsecurity.com

Proven Process for Building an ISO 27001 Certifiable Information Security Management System (ISMS)

Pivot Point SECURITY

8 Maintenance, Continuous Improvement and Recertification

Getting an imperfect ISMS certified is possible, but keeping it certified isn't! **ISO 27001** is about executing the ISMS, updating it to reflect changes in context, and continuously improving it. A well operationalized ISMS will make it easier to **adjust to ongoing changes in threats, technology, regulations, and client expectations** and have these changes logically cascade through the ISMS



Here are some artifacts you can expect to produce on your ISO 27001 journey

- Scope Statement
- Risk Assessment
- ISMS Objectives
- Security Metrics
- Policies/Standards/Procedures
- Statement of Applicability (SOA)
- ISMS Internal Audit Program

To start a conversation with one of our ISO 27001 experts, click here or please give us a call at

888-748-6876

info@pivotpointsecurity.com