



Your Guide to ISO 27001

ISO 27001 is a valuable way to identify, mitigate and monitor your company's information security risk.

This standard is designed to help you manage the security of your services, data, intellectual property or any information entrusted to you by a third party.

Unlike other popular compliance efforts, the main focus of the ISO 27001 standard is the design, implementation and maintenance of a company's information security management system (ISMS). The ISMS is a collection of your company's policies, procedures, people and controls to address information security relative to its defined scope.

The ISO 27001 standard includes these main clauses:

- | | | |
|---------------------------------------|---------------------|----------------------------------|
| 4. Context of the Organization | 6. Planning | 9. Performance Evaluation |
| 5. Leadership | 8. Operation | 10. Improvement |



Who Should Get Certified?

ISO 27001 applies to any organization of any size in any industry in any region. Put simply, if your organization handles or stores information critical to internal and external partners, it has every reason to consider certification. However, most organizations get certified due to a contractual obligation from a client or prospective client or use it as a competitive advantage.

What Other Companies are Doing

We surveyed our current clients about their ISO certifications and discovered:

About **80%** of Schellman clients have undergone ISO 27001 certification due to a contractual obligation.

Nearly **20%** of Schellman clients have done so to gain competitive advantage or to match industry competitor's compliance efforts.



Benefits of ISO 27001 Certification

Beyond a competitive advantage and protecting your client's valuable information, getting ISO 27001 certified provides these additional benefits:

- Gives your company a functional, organization-wide plan to identify and mitigate information security risk
- Meeting the requirements of ISO 27001 means that you are required to perform specific activities at defined intervals (i.e. risk assessment, internal audit, etc.). The ISMS is an active compliance framework, allowing your company to continually mature its security posture while improving on current processes.



The Elements of the ISMS

While it may be tempting to look at each element of your company's ISMS individually, it is important to look at the big picture. The ISMS is intended to be a comprehensive, autonomous system that is continuous and interrelated with all of its different elements (clauses) and controls. Just as a house is not a house without a foundation, a roof, walls, ducts, even nails, an ISMS is not effective unless all clauses are met and interrelated.

After the first year of certification, many organizations begin to mature and maximize their ISMS, allowing it to act as a comprehensive system. But, for now, it is completely acceptable to achieve conformance with the requirements (a success in its own right) during the first year.

“I’ve seen organizations that have gone beyond the base requirements to construct a very complicated, elaborate and impressive management system,” explains Ryan Mackie, Schellman’s ISO practice director. “Unfortunately, after certification, the organization realized it was a tremendous effort to maintain and ended up with multiple nonconformities during the surveillance review.”

Focus on meeting the ISMS requirement, and then plan to work on continuous improvement as your company’s ISMS becomes more integrated across your organization, says Mackie.




ISMS Clauses

CLAUSE
4

Context of the Organization

Clause 4 is the main clause of the ISMS and requires your organization to determine the scope of the ISMS. Everything — risks, objectives, personnel, audit, oversight, controls — should be traced back to the scope.

Keep in mind: The scope also drives external audit time and audit cost. If a scope includes one location and is limited to few people supporting it with standard technology, that audit time may require less audit time, and cost, as compared to a scope that includes multiple locations with hundreds of employees supporting it, including many systems that cover different services.

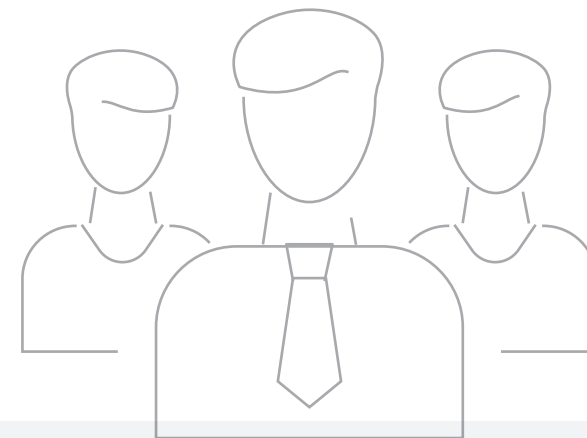


**Consider the end result
(i.e. the certificate)
when determining the
scope of your ISMS.**

The external deliverable for ISO 27001 is just the certification and it includes only the scope statement, locations within scope and the certificate dates. There is no supporting narrative or report that is issued as an external deliverable. Think of what that final certificate should look like, keeping in mind customer expectations, contractual requirements or even competitor certificates.

Leadership

Once the scope of your ISMS has been identified, company leadership must be committed to the design and implementation effort and allocate and assign resources as necessary to support the ISMS.



Tips for Getting Company Leadership On Board

If your company's leadership seems resistant to the initiative, or you're struggling with how to communicate the need for it, consider these tips.

Be frank

Data and security breaches are happening at alarming rates, and these rates will only continue to rise. An ISO 27001 certification won't prevent a breach, but it will identify and allow you to contain the breach much quicker than if you did not have an effective ISMS in place.

Highlight the growth opportunities and competitive advantages

If your company wants to expand globally or already operates in the international market, it will need an ISO 27001 certification to stay competitive. In fact, many European companies are requiring ISO 27001 certification for partners. Also look at what your competitors are doing.

Focus on your customers or potential customers

As noted in the first tip, data breaches are becoming common. An ISO 27001 certification demonstrates to your audience that you're doing everything you can to secure your customers' data.

Planning

Planning includes two components:

1. Information security risk assessment
2. Information security objectives

An information security risk assessment, when designed and executed properly, offers:

- Organizational transparency to its in-scope “information”
- The current exposure landscape
- The controls necessary to bring the risk to a pre-defined acceptable level
- The controls that are not in place but are necessary to bring the risk to a pre-defined acceptable level
- The control catalog supporting the ISMS (also known as the Statement of Applicability)

What a Risk Assessment Process Looks Like

An effective risk assessment process includes personnel from various departments — known as risk owners — who can collaborate on the risk to their area and what controls are in place (or should be in place) to reduce the risk to an acceptable level. **A risk assessment should not be performed by a random group of individuals but by those who directly own the risk.**

Once the risk assessment has been completed, you may find risks that require treatment.

The treatment of risks should be dynamic, allowing for:

- The risk owner to be directly involved in accepting the residual risk score and determining an effective treatment plan
- The treatment plan to be continuously monitored against planned milestones to ensure it remains active and
- An independent review of the treatments results performed to validate that the risk is mitigated to an acceptable level based on the treatment

Information Security Objectives

It's not uncommon for organizations to confuse information security objectives with the measurement and monitoring requirements in Clause 9.1, but they're not the same.

For information security objectives, you need to determine what the objectives are, who is responsible for them, what will be done, how they will be measured and when it will be completed.

These objectives should be pertinent, specific and relevant to the information security risk of your organization. They are typically one year forward planning (but could include shorter or longer duration plans), and if they can be associated with the results of the risk assessment, planning for information security objectives may be straightforward: Address a known vulnerability that has no mitigating controls or what your organization wants to accomplish to ensure effective information security.

Support

Support includes a number of key elements that are equally important to ensure an effective ISMS.

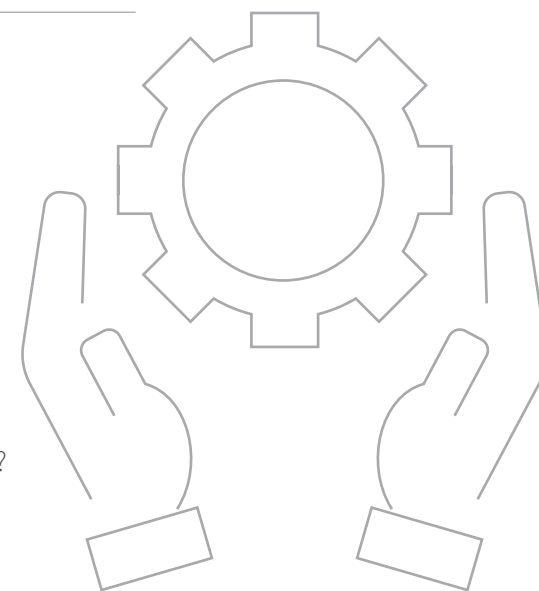
The ISMS needs:

Resources: Identify and define the resources necessary to support the ISMS

Competence: Once resources are identified, the organization must then determine their competence.

Consider: What is necessary for someone to be determined competent? How do we evaluate the resources against the competence criteria? What efforts are performed to ensure those people continue to be competent?

Awareness: An organization with the right and competent people to support its ISMS must ensure those people are aware of the elements of the ISMS that pertain to them.



Keep in mind: Support also pertains to a proper communication structure. This helps ensure any communication relevant to the ISMS is identified, performed by the right people, includes the proper message and is sent in the correct format to the required audience.

The ISMS could not operate effectively without proper document and record control. Those people who have a role within the ISMS must be able to understand their function through proper policies and procedures that are current, available and properly maintained and versioned.

CLAUSE
8

Operation

Operation focuses on the results of the risk assessment, implementing and executing against the risk treatment plan, and allowing for the processes and controls to be implemented and to function in order to mitigate information security risk relevant to the scope.

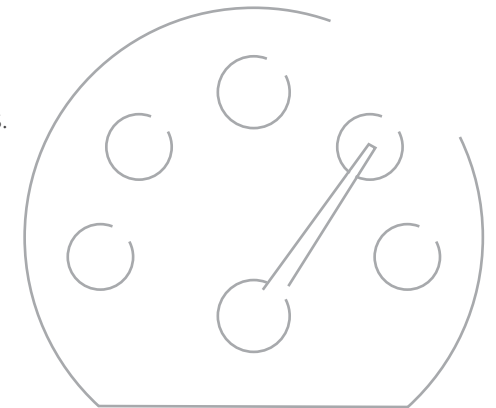
CLAUSE
9

Performance Evaluation

With the ISMS designed and operating, you need to determine if it is effective. This is broken down into three elements.

The first elements of Performance Evaluation are monitoring, measurement, analysis and evaluation.

The standard requires the organization to put specific criteria in place to ensure that it is evaluating its information security performance and the effectiveness of its ISMS on a continuous basis. You need to define the who, what, when, how, etc., in relation to measuring operation, process and control performance.



Keep in mind: Measurement and monitoring are intended to be continuous and reproducible. To determine if your ISMS is performing at an effective level, a mature ISMS will have its measurement and monitoring applied throughout the organization, in a variety of processes and controls. This will help ensure that any issue is identified quickly and that it is presented to the proper audience.

The second element is internal audit. This is a necessary step to help ensure that the ISMS continues its conformance to the requirements in Clauses 4-10 and that the controls necessary to support the ISMS are in place and operating effectively. Additionally, the internal audit is a good way to identify opportunities for continual improvement. The requirements of competent and independent auditors help this function provide results that management can rely on, without any bias or subjectivity.

The third element is the management review process. Your ISMS has been designed and implemented to meet the requirements, it has been free to run its operations as planned, and teams have performed their process and control performance measurement and internal audit processes against the ISMS.

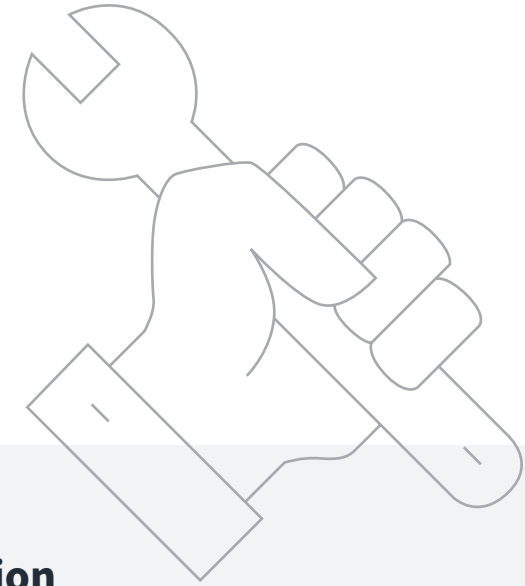
Now, those results (as well as other data relevant to the effectiveness of the ISMS) go back to parties in top management who supported the ISMS (in Clause 5) so they can:

- Determine if the whole of the ISMS is meeting its objectives and operating effectively
- Determine if any changes are required (in processes, systems or staff) to ensure it corrects known issues or continues its successful path down maturity lane

Improvement

There are two ways an organization can improve:

1. Fix the things that are broken.
2. Improve the things that are currently working as intended.



This is known as nonconformity and corrective action (for the fixing) and continual improvement (for the improving).

Most organizations perform both of these processes equally well but are better at demonstrating the break-fix process. It may be difficult to properly track and demonstrate continual improvement but those organizations that are in years two, three or four of certification — and can devote more time to improvement as the foundation of their ISMS is now solid — will be able to find ways to incorporate continual improvement into their project or program management function (control domain A6), management review process (Clause 9), information security goals and objectives (Clause 6), hiring plans and documentation (Clause 7), etc.

Once an organization better knows what it looks like (in relation to the ISMS), it can become easy to capture and demonstrate.

The Importance of Controls

Though most controls may already be in place within an organization, it is extremely important to perform a healthy assessment of those controls.

When performing the risk assessment:

1. Ensure the current control is the right control to mitigate the associated risk.
2. Determine if the control, in its current state, meets the requirement of the control activity in Annex A.
3. Determine if the control is effectively operating and maintainable.

An effective management system will create a control baseline — one that can mitigate the risk to an acceptable level and meet the requirements — and then work to improve that control baseline to demonstrate maturity and continual improvement within the organization.



ISO 27001 is Making an Impact

Did you know?

32%

There was a **32%** increase in ISO 27001 certifications globally from 2020 to 2021, based on the most recent ISO Survey.

64%

During that same period, there was a **64%** increase in ISO 27001 certifications in the United States.

Why Schellman for ISO 27001?

We at Schellman believe our clients deserve the best. That's why we never use contractors and our audit staff is continually monitored to ensure that they are competent and provide effective assessments. This helps us provide for continuity of the audit team from year to year, allowing for the team members to know your company inside and out.

Unlike other firms, we:

- Have over 90 lead auditors for ISO 27001
- Provide you with a dedicated management team, which gives you an easily accessible point of contact without having to call a service line
- Have weekly status check-ins on the lead-up to audit, giving you time to ask questions or check on status updates
- Stick to our project timelines, which gives you your certificate in weeks rather than months
- Have cross-trained teams of auditors who can conduct multiple audits at once, saving you time and money



CLICK FOR MORE INFO

www.schellman.com

4010 W Boy Scout Blvd, Suite 600 / Tampa, FL 33607 / 1.866.254.0000
Outside of the United States, please dial: +1.813.288.8833

