GUIDE TO GETTING CERTIFIED TO ISO 27001

COMPLIANCECOUNCIL.COM.AU

Compliance Council

TABLE OF CONTENTS

WHAT IS AN INFORMATION SECURITY MANAGEMENT SYSTEM

Data and information are valuable assets in every organisation and deserve to be protected from potential risks or threats. To secure your intellectual property, financial data and third party or employee information, you have to implement an Information Security Management System (ISMS).

An ISMS is a combination of processes and policies that help you identify, manage, and protect vulnerable corporate data and information against various risks. Specifically the ISMS's key objective is to ensure the confidentiality, integrity and availability of data and information in maintained.

ISO 27001

ISO 27001 is an internationally recognised standard that sets requirements for ISMS. The requirements provide you with instructions on how to build, manage, and improve your ISMS. The standard updated in 2013, and currently referred to as ISO/IEC 27001:2013, is considered the benchmark to maintaining customer and stakeholder confidentiality.

As of the end of 2017, almost 40,000 businesses worldwide had achieved certification to ISO 27001; a 19% increase on the year prior.

BENEFITS OF ISO 27001

If you are a business owner who is thinking about implementing an ISMS in his/her organisation or a manager in a company who wants to get Senior Management on board with an ISMS, you need to know more about what value ISO 27001 can add to your business. Here we explain some of the major benefits that you can expect to achieve:

ALLOWS FOR THE SECURE EXCHANGE OF INFORMATION

This standard helps you identify the threats toward your information security and create plans to address them. For any specific risk, you will have someone who is responsible capable enough to control the situation in case something goes wrong. This kind of process can manage and minimise risk exposure and automatically lead to a safer information exchange.

MAKES INFORMATION SECURITY EVERYBODY'S RESPONSIBILITY

When you implement ISO 27001 in your company, you create awareness among employees and provide information security training to allow them to become accountable for information security, regardless of their role in the orgnaisation.

Eventually, data protection finds its way into the organisation's culture, and somehow simplifies the information security process in a way that everyone understands it and works to achieve it.

BRINGS A COMPETITIVE ADVANTAGE AND BUILDS REPUTATION

It is safe to say that all of your clients or partners, who share their valuable data with you, are perfectly aware of the importance of information security and expect you to grant them that. Having certification to an information security standard such as ISO 27001 is a strong way of demonstrating that you care about your partners and clients' assets as well. This builds trust, creates a positive reputation for you, and distinguishes you from your competitors who are not certified to the ISO 27001.

MEETS LEGAL OR THIRD PARTY OBLIGATIONS

It is probably the case that sometimes you are asked by a client, third party or by law to show your organisation capability in information security. In situations like this, ISO 27001 could be an excellent choice. This standard is recognised and used by many organisations worldwide, and by applying its clear and practical instructions, you can prove your trustworthiness concerning information and data security.

ACHIEVE A RETURN ON INVESTMENT

By implementing this standard, you can achieve a return on investment in at least two ways. One way is through the marketing value that it adds to your organisation since the certification can attract potential clients and also assist with pre-sales due diligence conducted by your potential clients.

Second, ISO 27001 helps you avoid, eliminate or reduce the undesired effect of risks which otherwise can severely impact your organisation's reputation leading to financial penalties and related legal issues.

FOUR FACTS ABOUT 27001 STANDARD YOU NEED TO KNOW

What it is that comes into your mind when you think about safety standards in general or ISO 27001 in particular? From what we have seen and heard, there are some general assumptions and beliefs that are not so helpful. Let us shed some light on that area and reveal some interesting facts about ISO 27001.

THIS STANDARD IS NOT ABOUT DOCUMENTATION

ISO 27001, like other recently updated standards, uses the term documented information, which means any organisation can retain the necessary information in the way that best suits it and to the extent that is needed. In other words, you are in charge of the format and amount of documented information that is kept for your records. After all, this documented information is supposed to help you keep track of what you have done and what needs to be done in the future.

IT IS NOT COMPLICATED

The name of information security could be overwhelming for some of us and create this delusion in our mind that everything related to it is too complicated for a non-technical person. ISO 27001 is here to make the process of implementing ISMS smooth and simple enough that everyone can be a part of it. It provides all the guidance and outlines you need along the way to your information.

IT IS NOT THE IT DEPARTMENTS RESPONSIBILITY

The truth is, just because it is about information security, it does not mean it shouldn't concern other departments. In fact, every single person in the organisation will have responsibilities for the ISMS as information isn't just the concern of the information technology team.

ISO 27001 expects people who are involved in the process, to have enough competency and awareness about ISMS so they are able to participate and be accountable for what they need to do.

IT IS NOT PRESCRIPTIVE

ISO 27001 is a standard that sets the outcomes that are expected to be achieved but how you actually do that is up to the organisation. For example, A.7.2.2 information security awareness, education and training states that:

All employees of the organisation and, where relevant, contractors shall receive appropriate awareness, education and training and regular updates in the organisational policies and procedures, as relevant to their job function.

This requirement doesn't state how often, what type of activity or which topics should be address through awareness, education and training. From an auditor's perspective, they may have certain thoughts about what is appropriate or not based on their experience but they can't mandate that you take a certain approach if you can demonstrate that you have achieved the outcome in a way that aligns with the context of your organisation. Context can include applicable legislation, contractual requirements, expectations from the Board, information security risks or any other item that is specific to your organisation.

ISMS REQUIREMENTS

ISO 27001 provides organisations with 10 clauses that serve as information security management system requirements and a section titled Annex A that outlines 114 controls that should be considered by the organisation. Since organisations of any size and type collect, process, and communicate information in various ways, they can benefit from the implementation of an ISMS that aligns with ISO 27001.

Clause 1 to 3 provide introductory information about terms and definitions and normative reference of ISO 27001. The main content starts from clause 4 so we start from there as well.

4 CONTEXT OF ORGANISATION

Context of organisation is a core concept that you build your ISMS on top of it. It is about identifying and analysing your business and your environment. To do so, you have to determine all the factors that can affect the success of your ISMS and achieving its goals, including:

- All the internal and external issues related to the ISMS
- All the internal and external interested parties and their expectations
- The scope of ISMS

The importance of defining the context of the organisation comes from the fact that it is the base for some important processes that you will build later on, such as risk management, and continual improvement.

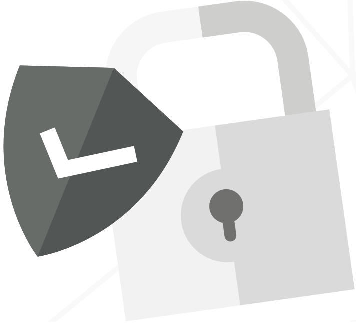
What you need to achieve at this point is identifying what are the assets you want to protect with an ISMS and why.

Your context and the scope of your ISMS are what that differentiates you from all the other organisations and gives you the opportunity to discover your uniqueness and enjoy the benefits of ISO 27001.

5 LEADERSHIP

When top manager involves in an organisation process, the chance of getting desired outcomes is much higher than the time he/ she is passive and not involved. ISMS success relies on top management commitment and the standard emphasises on this fact by designating this clause to the leadership role and responsibility. Here is what senior management should do to show support and engagement:

- Establishing the ISMS policy and objectives or an objective framework
- Aligning the ISMS policy and objectives with the overall business strategy
- Integrating the ISMS requirements and controls into other organisation processes
- Allocating all the necessary resources
- Communicating with and supporting people who have a role to play in ISMS implementation



6 PLANNING

When planning for ISMS, ISO 27001 is strongly concerned with identifying and treating risks and opportunities. It requires organisations to have a risk management process in place that defines, determines and addresses the risks; the standard also emphasises that this should be an ongoing process to ensure the continual improvement in the company. What you have found in terms of internal and external issues and interested parties requirement as result of clause 4 provides the risk management basis.

The other part of the planning relates to setting information security goals and planning to achieve them. These goals should be aligned with the ISMS policy and risk management results. At the same time, goals should be measurable and communicated through the organisation.

7 SUPPORT

An adequate level of support is necessary to successfully implement and maintain ISMS in an organisation. This clause suggests that you can provide support when there are enough resources, competencies, communications and documented information related to the ISMS.

Resources include people, time, budget, information and infrastructure that might be required in the process of complying to ISO 27001. Competencies relate to the people and their capabilities to perform their part in ISMS. On the other hand, a communication process should be available to facilitate access to the information for people who need it. The range of communications should include all the internal and external interested parties to the extent that is necessary. Smooth and adequate communication is a key to ISMS.

8 OPERATION

At this point, you have already defined the context of organisation, risks and opportunities and planned the necessary processes to achieve ISMS goals and address the risks. Now it is time to execute the plans.

When you implement the processes and controls, you have to make sure the ISMS requirements are met as planned and you are capable of taking proper actions when there is a change to your scope.

The result of the operation phase should be monitored and reviewed in case an adjustment is required; for example, when interested parties have new expectations or an unexpected change to the ISMS occurs.

9 PERFORMANCE EVALUATION

When the required processes are implemented, it is time to evaluate and see if the company has reached the predefined outcomes. In the evaluation phase, you want to find answers to these questions:

- How is the information security performance?
- How effective is the ISMS?

To answer these questions, you need to determine exactly how to measure the ISMS processes. ISO 27001 expects organisations to have an internal audit program, which is responsible to see if all the ISMS requirements are met.

Once again top management should carry out the task of reviewing the whole process and ensuring that everything is still align with the overall goals and strategic direction of the organisation.

10 IMPROVEMENT

There is always room for improvement. This could happen through removing minor or major nonconformities or through acting on new opportunities that can be revealed during different steps of the ISMS process.

Since the overall context and scope of any organisation is a subject to constant changes, making improvement to the ISMS must be an ongoing process and a critical part of an effective ISMS.

ANNEX A

Annex A outlines 114 security controls that an organisation should consider, these controls are divided across 14 security domains which are:

SECURITY DOMAIN	SECURITY CATEGORIES AND CONTROL OBJECTIVES
A.5 Information security policies	**A.5.1 Management direction for information security** *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
A.6 Organisation of information security	**A.6.1 Internal organisation** *Objective:* To establish a management framework to initiate and control the implementation of operation of information security within the organisation. **A.6.2 Mobile devices and teleworking** *Objective:* To ensure security of teleworking and use of mobile devices.
A.7 Human resource security	**A.7.1 Prior to employment** *Objective:* To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. **A.7.2 During employment** *Objective:* To ensure that employees and contractors are aware of fulfil their information security responsibilities. **A.7.3 Termination and change of employment** *Objective:* To protect the organisations interests as part of the process of changing or terminating employment.
A.8 Asset management	**A.8.1 Responsibility for assets** *Objective:* To identify organisational assets and define appropriate protection responsibilities.

A.8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.

A.8.3 Media handling

Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.

A.9 Access control

A.9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

A.9.2 User access management

Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

A.9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

A.9.4 System and application access control

Objective: To prevent unauthorised access to systems and applications.

A.10 Cryptography

A.10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A.11 Physical and environment security

A.11.1 Secure areas

Objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

A.11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.

A.12 Operations Security

A.12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities

A.12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

A.12.3 Backup

Objective: To protect against loss of data

A.12.4 Logging and monitoring

Objective: To record events and generate evidence

A.12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

A.12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities

A.12.7 Information systems audit considerations

Objective: To minimise the impact of audit activities on operational systems.

A.13 Communications security

A.13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A.13.2 Information transfer

Objective: To maintain the security of information transferred within an organisation and with any external entity.

A.14 System acquisition, development and maintenance

A.14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provides services over public networks.

A.14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

A.14.3 Test data

Objective: To ensure the protection of data used for testing.

A.15 Supplier relationships

A.15.1 Information security in supplier relationships

Objective: To ensure protection of the organisations assets that is accessible by suppliers.

A.15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity

Objective: Information security continuity shall be embedded in the organisations business continuity management systems.

A.17.2 Redundancies

Objective: To ensure availability of information processing facilities

A.18 Compliance

A.18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A.18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

RISK MANAGEMENT AND SECURITY CONTROLS

ISO 27001 considers information security risk management to be the foundation of ISMS and demands organisations to have a process for risk identification and risk treatment. It is through this process that businesses can fully leverage the ISMS benefits.

For the sake of simplicity, you can think of risks as everything that could go wrong in the scope of your ISMS, such as a damaged server or a hacked bank account. Although it might not be clear how to create the risk management process when you first start off with ISO 27001. That being said, this section can help you make a better sense of the risk management process through couple of steps, which are simplified to give you just the general idea of what needs to be done.

FIRST STEP:

RISK IDENTIFICATION

This step includes finding all the risks in the scope of your ISMS that could compromise the confidentiality, integrity and availability of information. You should develop some specific criteria for accepting the risk and those criteria come from the internal and external issue as well as interested party requirements (clause 4 of the standard).

SECOND STEP:

RISK OWNER IDENTIFICATION

You need to determine exactly who is responsible for each specific risk. This person should also have enough authority to act when it is necessary, for example, who is accountable when a USB flash containing client information is lost.

THIRD STEP:

RISK PRIORITISING

Think about the consequences of every single risk if it really happens and the likelihood of that risk happening one day. Doing so, you will be capable of prioritising all the risks based on the possibility of their occurrence and the severity of the results.

FOURTH STEP:

CONTROLS AND STATEMENT OF APPLICABILITY (SOA)

After identifying all the ISMS risks in the step 1, now you have to associate each risk with one or more appropriate control from ISO/IEC 27001:2013, Annex A.

There are 114 controls in Annex A which include policies, processes, procedures, organisational structures and hardware and software functions that you can implement to address risks to your ISMS.

Then you can create your SoA, which contains all the selected controls along with some explanations. In the explanations, you should mention the reason for including that specific control and its status, meaning whether it has been implemented or not, you also need to elaborate on the controls you haven't used.

FIFTH STEP:

RISK TREATMENT PLAN

In the final step of your risk management, you have to create the risk treatment plan based on what you have done in previous steps. There is no specific framework that you need to use but the plan could include the controls that need to be implemented, their status and the risk owners who are responsible for implementing controls and measuring the results for future improvements. The result of this step should be retain as documented information.

CERTIFICATION TO ISO 27001

What does an ISO certification body do: Stage 1 and Stage 2 with audit certification body

Third Party Certification is the process of having your Management System audited by an independent third party. This type of auditing is typically used by Conformity Assessment Bodies (CABs) who are regulated by a government organization known as JAS-ANZ. These CABs can issue registered certificates of compliance to various standards such as ISO 9001, AS 4801, and ISO 14001.

STAGE 1 AND STAGE 2

The formal assessment process includes two stages. In stage 1, the auditing body will confirm whether you have met the requirements of your proposed scope and the objectives you have set for yourself. If the auditing body finds any areas of concern, which is normal at this point, you will have some extra effort to put in which results in a better ISMS.

The auditing body will give you some time to address the areas of concern, before beginning stage 2 of the audit. In stage 2, your system will be assessed again to make sure that all areas of concern are corrected and identify any non-conformances indicating lapse in the implemented of ISMS processes.

At this point, if there are no major nonconformities, your certification can be issued; otherwise, you will be given time to correct existing nonconformities before the next visit of the audit and only after removing all the major nonconformities you will be eligible for ISO 27001 certification.

SURVEILLANCE AUDITS

Typically, the certification body will conduct an annual surveillance of your management system for the first three years after your certification is issued. This way, you will be sure that everything is working the way that you expected and your ISMS still meets the ISO 27001 requirements.

ISO 27001 START TO FINISH

Now that we have covered different aspects of this information security standard, to summarise, we can put everything together and see how you should go through your ISO 27001 journey, generally speaking you need to:

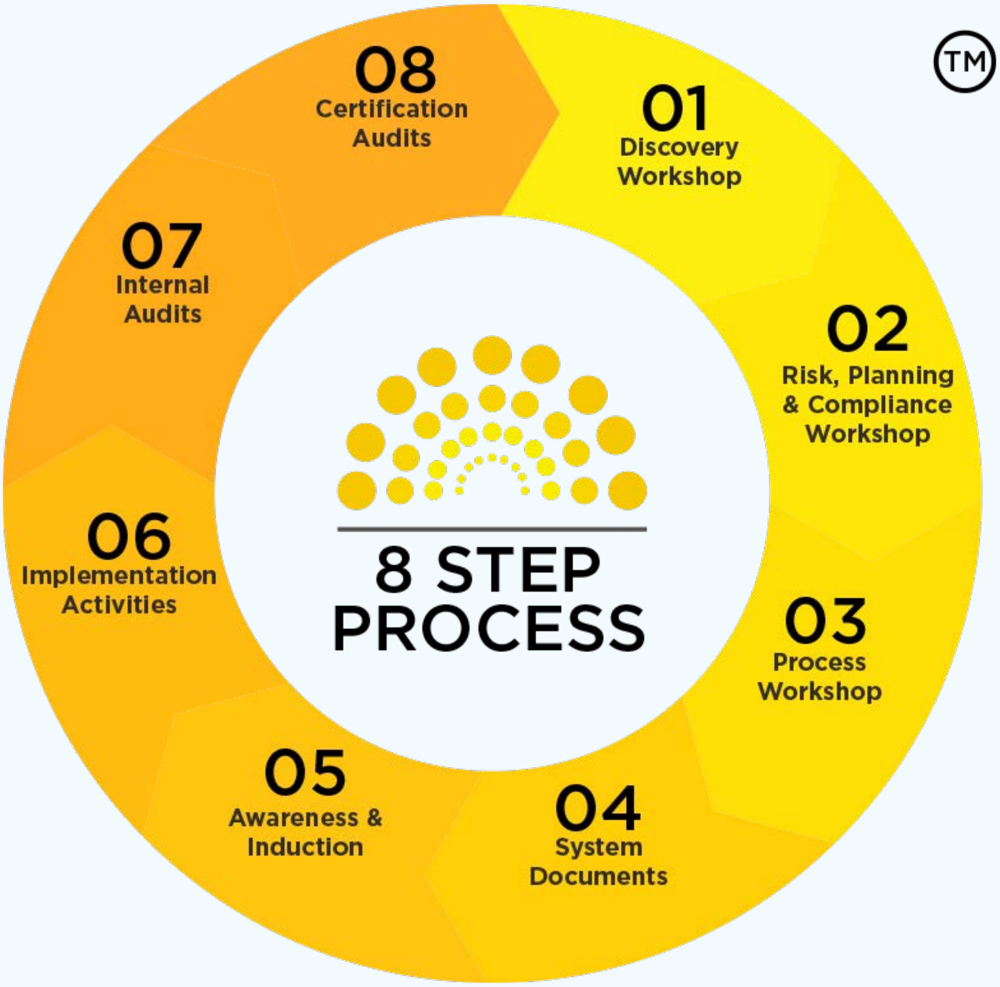
1. Read the standard requirements and understand how it can apply to your business
2. Establish the scope of your ISMS
3. Perform a gap analysis to see where you are standing with regard to your information security and where the standard requires you to be
4. Gather all the information or support you need for implementing your ISMS
5. Arrange for a third party certification audit

At the end, you should build an ISMS that improves your overall business condition by increasing your ROI and helping you stand out in the crowd, so you need to implement it perfectly. Although the whole process could be easier and faster if you decide to work with a consultant. Here at Compliance Council we have helped many companies and developed an 8 step process to assist you with developing and implementing an ISMS which put your business on the path to becoming certified.

WHY COMPLIANCE COUNCIL?

Compliance Council removes the burden and stress of meeting industry standards from time-poor industries. Based in Sydney, Australia, our team of compliance professionals consists of experts from various sectors, having gained significant experience working with companies of all sizes ranging from new start-ups to large Australian blue chip organisations.

Here at Compliance Council we have helped many companies and developed an 8 step process to assist you with developing and implementing an ISMS which put your business on the path to becoming certified.



To discuss how Compliance Council can assist you with complying with ISO 27001, contact us using the below details.

Compliance Council

www compliancecouncil.com.au

☎ 1800 771 275

✉ info@compliancecouncil.com.au