CyberCX

Ten things you should know about ISO/IEC 27001

1. What is ISO/IEC 27001 and why is ISO 27001 important to me?

ISO/IEC 27001 (ISO 27001) is an international standard for information security, cyber security and privacy protection that defines the requirements for an Information Security Management System (ISMS).

Information is the lifeblood of most contemporary organisations. It provides intelligence, commercial advantage and future plans that drive success. These days, our valued information assets are stored and accessed electronically. Therefore, protection of these assets from either deliberate or accidental loss, exposure, compromise or destruction is increasingly important. ISO 27001 is a risk management framework designed to help organisations effectively identify and manage risks to their critical information assets required for the organisation to function.

2. Why are international standards like ISO 27001 important?

The global economy continues to become more integrated, with national boundaries now less important in terms of transacting business. In such an environment, the use of a common international standard provides a common and well-tested framework for managing risks related to information security, cyber security and privacy protection. Such shared language and focus, benefits local and global economies through consistent understanding and treatment of threats and risks.

In an increasingly connected world, information security continues to grow in importance.

What about in Australia and New Zealand?

Many Australian industry bodies and government entities reference ISO 27001 as the foundation for robust information security management practices. ISO 27001 underpins key strategies adopted by governments at all levels. The standard is particularly popular across state governments, which often mandate the implementation and operation of an ISO 27001-based ISMS across their agencies. ISO 27001 is also common in key service sectors such as ICT and data centre hosting.

3. What are the benefits

For consumers

Proof of conformity to international standards helps reassure current or potential business partners that products, systems and organisations are safe, secure, reliable and good for the environment.

For business

International standards can be a strategic tool to help businesses tackle challenges and compete on a global stage.

Adoption of international standards can open up new markets, improve competitiveness through greater customer satisfaction, reduce costs, streamline systems and processes and increase productivity.

For society

International standards improve security, safety, quality and environmental outcomes as well as encouraging international trade.

4. Why should you implement an ISO 27001-based ISMS?

Data and information need to be safe, secure and accessible. The security of information is important for personal privacy, confidentiality of financial and health information and the smooth functioning of systems and supply chains that we rely on in today's interconnected world.

ISO 27001 provides the framework for you to effectively identify risks and select appropriate security controls to assist you in managing these risks. It is a formal and structured process that allows you to achieve, maintain and demonstrate ongoing conformance with the recognised global standard in information security management.

Adoption of ISO 27001 provides real credibility to both internal and external parties that you understand security and take it seriously.

5. What are the core elements of ISO 27001?

ISO 27001 is made up of a number of short clauses and a much longer annex that lists multiple reference controls for consideration. Some of these key clauses relate to:

- The organisational context and needs of interested parties
- Commitment to information security by the organisation's leadership
- Understanding risks to the organisation and selecting appropriate risk treatments
- How to operate, monitor and improve an ISMS based on ISO 27001
- Addressing any identified areas of weakness

The reference controls for consideration include controls in for key areas:

- Organisational controls
- People controls
- Physical controls
- Technological controls

The standard does not mandate the use of these controls, and organisations often choose to incorporate other local and global control sets in their ISMS to manage their risks. These control sets could include controls related to credit card security (PCI-DSS), cloud security or controls from the Australian Government's Information Security Manual (ISM).

6. How does it work? What is a risk-based approach to Managing Information Security?

Unlike other security standards, for example, the Payment Card Industry – Data Security Standard (PCI-DSS) and Sarbanes-Oxley (SOX) which take a compliance approach and are highly prescriptive, ISO 27001 takes a risk-based approach to security management. In other words, there are no defined set of security controls that must be implemented regardless of the type of business operation, as is the case with PCI-DSS. Controls are selected based on their ability to mitigate risks to the organisation.

ISO 27001 is concerned with the process of continual improvement and a demonstrated commitment to managing information security based on risks to the organisation's information assets.

A risk-based approach to managing information security ensures that security risks are appropriately prioritised and efficiently managed, with controls specifically selected to manage identified risks to an organisation. It is a "use or explain" approach. Based on your organisation's risks, you can select controls to use to help manage risk, or simply explain why they aren't relevant and why you don't need them. There is no compliance for the sake of compliance with ISO 27001.

7. Where should I start?

Before starting out on the path to certification, it may be worthwhile understanding if certification is required or if conformance to the standard will suffice. For many organisations, certification is not a requirement.

For those industries where certification is a requirement, the path to achieving certification should not be treated as a one-off project. Organisations that successfully maintain certification over multiple years treat information security as a critical business process and invest time, resources and effort into ongoing compliance. Certification is the logical consequence of conformance and should be relatively easy if a robust risk management regime is established and maintained.

For most organisations, the logical place to start is to identify what the drivers are, who cares about security, and what critical information assets need to be protected. This is called the "scope" of the ISMS and drives all further activities.

After that, the organisation should undertake risk assessments against these critical information assets and identify the controls that help manage these risks.

The completion of these two activities provides the building blocks of the ISMS. CyberCX provides support for these activities through the ISMS Jump Start offering.

8. The audit process

External certification can only be conducted by an Accredited Certification Body (CB). In Australia, CyberCX recommends certification services from reputable CBs only, such as BSI and SAI Global. Certification lasts for three years.

The initial audit process is undertaken in two stages:

Stage 1:

Focuses on a desktop review of available ISMS documentation and processes. Sufficient evidence of a functioning ISMS is required to progress to the Stage 2 audit.

Stage 2:

Focuses on evaluating the implementation and effectiveness of the ISMS. The audit will assess evidence and will typically require the ISMS to have been running for a period of several months.

The certification cycle also requires regular external surveillance audits to be performed by the CB where they will seek evidence that the management system is being actively maintained. Surveillance audits for ISO 27001 are typically performed annually with a recertification audit undertaken every three years.

9. Who wrote ISO 27001?

ISO (International Organization for Standardization) is the world's largest developer of voluntary international standards. Many countries have their own national standards governing everything from railway gauges, electrical power point specifications, building materials, personal protective equipment and children's toys, to name just a few. When a standard reaches maturity and has widespread application in more than one jurisdiction, ISO forms a working group and works towards publishing an international standard.

The precursor of ISO 27001 was written by the UK Government and published by the British Standards Institute (BSI) as the BS 7799 standard in 1995. It provided the foundation for the first version of ISO 27001 released in 2005. The current version is the third edition published in 2022 and referred to as ISO/IEC 27001:2022. In Australia, this is the only version that organisations can be certified to.

10. Tips, trick and pitfall avoidance

Before certification:

1. Don't underestimate the number of stakeholders you will need to consult. In large organisations, stakeholder management can be a significant undertaking and key requirement for a successful implementation.
2. Partner with experienced information security providers who know the implication of advice, in particular with respect to the selection of information security controls. Many controls sound like a good idea, but the implementation can be much more challenging.
3. Start with an understanding of what information is important to you and what risks are relevant before becoming immersed in controls and technology. Like when we build a house, taking time to get the foundations of the ISMS right will mean a stronger structure in the long term.
4. Invest time up front to understand your risk posture; this will pay long-term benefits.

During certification:

Avoid anybody who guarantees certification within one month. They can't! CBs generally like to see several months' of evidence at the Stage 2 Audit to make a recommendation for certification to the Accreditation Body. For smaller scopes, this timeframe may be less, but it is best to plan on at least three months.

CBs are prevented under standards and Accreditation Body scheme rules from providing both certification and consulting or advisory services due to a conflict of interest. Some try to circumvent this restriction by offering extended pre-assessments or gap analysis . While these offerings may appear cheap, there are limits to their usefulness and the number of actionable recommendations that can be provided.

This is one of the services we're offering, so we need to be clearer here so as not to look hypocritical

No we offer a gap assessment but not certification. I think this is saying beware of organisations offering both services as this would be a conflict of interest.

After certification:

You will be entitled to display an ISO 27001 certification mark relevant to the CB that granted the certificate. This certification mark is tangible proof that you take care of information, are committed to protecting data entrusted to you, and are fulfilling your commercial, contractual and legal responsibilities with respect to information security. A common strategy is to promote this certification on your relevant marketing collateral and website as a source of differentiation from your competitors.

CyberCX

Contact us to find out how CyberCX can help improve your security posture with ISO 27001 certification and compliance services.

cybercx.com.au

1300 031 274