ISO27001: What Is It, and Do I Need It?

A Whitepaper for Australian SMEs

advance

Introduction

ISO27001 (full name, "ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements") is an international standard for information security management.

Because of this status as a standard, organisations can undergo a process to obtain an ISO27001 certification from an external auditor. The resulting certificate can be used to evidence to external parties that the business has implemented rigorous information security controls in line with an internationally recognised specification.

Such a certificate can lead not only to the opening of new markets and increased competitive advantage, but also to reduced costs and improved performance in information security.

However, ISO27001 can be a time- and resource-consuming certification to achieve, and some organisations have found better outcomes by targeting their budget more directly at implementing security controls, rather than achieving certifications.
In this paper, we look at what ISO27001 requires of organisations, and investigate if Australian SMEs should consider the certification process.

What is ISO27001?

The ISO27001 standard specifies requirements for establishing, maintaining and improving an information security management system (ISMS). The ISMS is a core concept of ISO27001 and is the main vehicle for identifying and treating information security risks. ISO27001 also specifies a number of mandatory and optional documents and records, as well as a number of several security controls that can be implemented depending on the risks an organisation identifies.

Two leading international standards organisations, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), collaborated to develop ISO27001 in 2005. The standard is made up of seven mandatory clauses, around 20 mandatory policies/records and 114 information security controls which are optional depending on identified risks.

A key concept in ISO27001 is that information security is not solely the purview of IT. In fact, less than half of the controls within ISO27001 are technical controls which IT would traditionally own. Other controls are categorised as organisational, legal, physical, and human resources.
A full list of ISO27001 mandatory documentation can be found in the appendix of this whitepaper.

What is an ISMS?

The information security management system, or ISMS, is a collection of documents, policies, rules and procedures for the organisation to follow. An ISMS is a core concept of ISO27001 and serves several purposes:

- Identify stakeholders of information security within the organisation
- Identify the information held by the organisation
- Identify risks to that information
- Define the controls to be put in place to manage those risks
- Oversee the implementation and measurement of controls
- Continuously improve the performance of information security

An ISMS is not a single document; rather, it is a collection of processes, people and technology which together achieve the information security goals of the organisation.

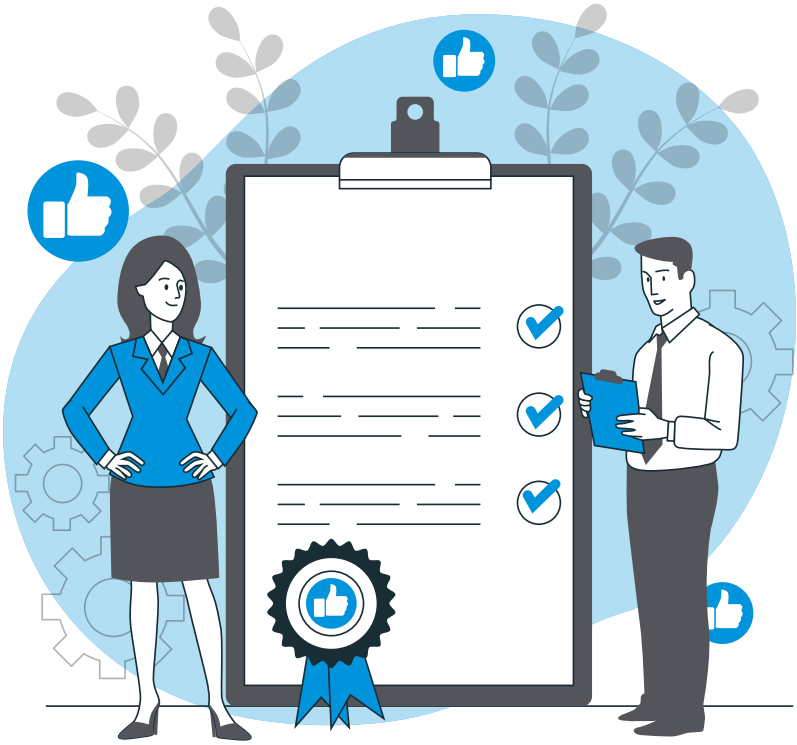
What is ISO27001 used for, and what are the benefits?

ISO27001 certification demonstrates to external parties that an organisation takes information security seriously and has implemented security controls to a high specification. It reassures customers, suppliers and regulators that information security risks have been identified and controls have been put in place to mitigate those risks.

In the case of many public-sector or large private-sector tenders, an ISO27001 certification may be mandatory; it demonstrates to the buyer that the supplier has adequate information security controls in place. This is particularly true where the ongoing relationship will involve the exchange of data, as the buying organisation seeks reassurance that all data transferred as part of the relationship will be kept secure. Even when an ISO27001 certification is not mandatory, many organisations feel that it provides an advantage in competitive tender processes.

Obviously, an ISO27001 certification ensures information security within an organisation. However, many organisations do not seek business for which the certification is mandatory, and do not feel it gives them a significant competitive advantage, often opting to implement other information security frameworks rather than ISO27001.

This is because other frameworks, such as the Essential Eight and the NIST Cybersecurity Framework, can be less prescriptive and ultimately less costly to implement. This is particularly true for smaller organisations, who often find that their budget is better spent on directly implementing security controls rather than creating mandatory documentation which can be of limited benefit to them.



How does ISO27001 compare to other information security standards and frameworks?

ISO27001 is generally considered one of the most comprehensive mainstream information security frameworks. This is due to its breadth, including many departments across an organisation, and the extent of its mandatory requirements and optional controls.

Unfortunately, this is also a reason many view it as overly administration-heavy.

SOC2, developed by the American Institute of CPAs (AICPA), is another common security standard similar to ISO27001. Similarly to ISO27001, organisations can obtain an SOC2 certification that can evidence a high standard of information security to external parties.

For most organisations, the decision between obtaining SOC2 and ISO27001 certification is a regional one. SOC2 is more widely used and recognised in North America, while ISO27001 enjoys wider recognition in Europe. The location of the organisation's suppliers, customers and operations will usually determine the best certification to obtain. There are many crossovers between ISO27001 and SOC2, meaning organisations can achieve both, although they do have many different requirements.

The NIST Cybersecurity Framework (CSF) is another common methodology. Developed by the American National Institute of Standards and Technology as a voluntary framework for American critical infrastructure organisations, the NIST CSF has a more technical focus, whereas ISO27001 takes a risk-based management focus.

As this is a voluntary framework, there is no certifying body or NIST auditors, and it is not possible to obtain a NIST CSF certification. This means the NIST CSF lacks the external evidence benefits and competitive advantage benefits of ISO27001 but is less administration and documentation focused.
The Essentially Eight is a well-known cybersecurity framework in Australia, as it was published by the Australian Government. Like the NIST CSF, the Essential Eight is a technical-focused framework; however, it is less comprehensive than the NIST framework and much less comprehensive than ISO27001. It is not possible to obtain a certification in the Essential Eight. As a more basic, entry-level framework, the Essential Eight is favoured by organisations at the start of their cybersecurity journey.

Conclusion

ISO27001 is a fantastic certification for organisations that need to evidence their information security maturity to external parties. It can open up new markets for which ISO27001 certification is mandatory, and provide a competitive advantage in markets where it is not.

Unfortunately, it does involve a significant amount of policy and administrative work, and many SMEs have not found that the documentation it requires gives them good return on investment.

For larger organisations, it is not unheard of to obtain an ISO27001 certification for their European market, obtain an SOC2 certification for their North American market, and use the NIST framework internally for its technical focus. While this is not common practice, it demonstrates that organisations can implement multiple standards and frameworks if they feel there is business benefit in doing so.

Australian SMEs at the beginning of their cybersecurity journey may find more value in first using the Essential Eight, which will provide quicker and better results for smaller organisations with low maturity. As maturity increases, SMEs need to determine if they will gain significant benefit from the cross-organisational involvement and external certification elements of ISO27001.

If so, then ISO27001 certification may be appropriate, but this is a large step up from the Essential Eight. If they do not expect significant competitive benefits from ISO27001, then they may find value in next moving to the NIST framework, benefitting from its comprehensive technical nature whilst maintaining a low admin overhead.

Appendix:
Mandatory Documents for ISO27001

1. Scope of the ISMS
2. Information Security Policy and Objectives
3. Risk Assessment and Risk Treatment Methodology
4. Statement of Applicability
5. Risk Treatment Plan
6. Risk Assessment Report
7. Definition of Security Roles and Responsibilities
8. Inventory of Assets
9. Acceptable Use of Assets
10. Access Control Policy
11. Operating Procedures for IT Management
12. Secure System Engineering Principles
13. Supplier Security Policy
14. Incident Management Procedure
15. Business Continuity Procedures
16. Statutory, Regulatory, and Contractual Requirements
17. Records of Training, Skills, Experience and Qualifications
18. Monitoring and Measurement Results
19. Internal Audit Program
20. Results of Internal Audits
21. Results of the Management Review
22. Results of Corrective Actions
23. Logs of User Activities, Exceptions, and Security Events

Contact Info

+61 8 8238 6500

sales@advance.net.au

www.advance.net.au