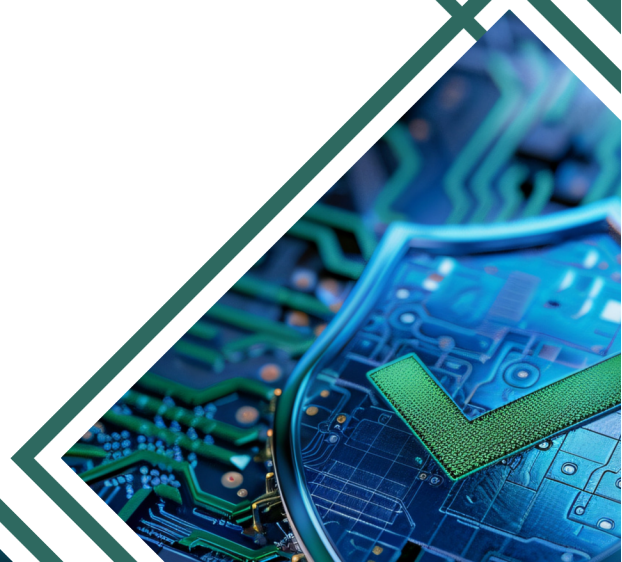# ISO 27001 ISMS

ISO27001- An Overview

ISO27001 Information Security Management System

ISO 27001 information security management system (ISMS) is an international standard or framework for organisations to use to manage and protect their information.

Why is it important?

The Australian Cyber Security Centre receives a report of a cyber-attack approximately every six minutes, with the rate and severity of reports increasing every year. The Australian Signals Directorate (ASD) also highlighted the average cost of cybercrime per report is up 14 per cent year on year putting a huge strain on operations for every organisation.

Unsurprisingly, an increasing number of business leaders feel their organisations are at greater risk from malicious cyber actors and are struggling to protect their sensitive information. This in turn disrupts business continuity, causes financial losses and reputation damage.

When you break it down, 95% of cybersecurity breaches are caused by human error of some sort. While you can never guarantee that your organisation won't fall victim to a cyberattack, having a robust system in place for the management of information will help significantly lower these risks.

Organisational Benefits of ISO27001

ISO 27001 is the only auditable international standard that defines the requirements of an information security management system. There are numerous organisational benefits to implementing this standard which act as a framework for managing information security risks, such as cyber attacks, hacks, data leaks or theft.

Secure Exchange of Information

Create a Culture of Security

Information is Safe from External Risks

Increased Client Retention & Satisfaction

Risk Management Capabilities

Protection of Assets, Data & Information

Inspires Trust & Consistency

Lowers Overall Risk

A Security Certification Framework

ISO 27001 certification is separated into 14 control areas. These are the business processes that will be part of the audit process as you work towards certification.

Information Security Policies	Organisation of Information Security
Human Resources Security	Asset Management
Access Control	Cryptography
Physical & Environmental Security	Operations Security
Communications Security	Systems Acquisition, Development & Management
Supplier Relationships	Information Security Incident Management
Business Continuity Management	Compliance

Key Certification Steps

1

REVIEW
Organisations should review and understand the ISO standards from the ISO Store.

2

DEVELOP
Follow the requirements of the standard in developing your organisations stanards.

3

DOCUMENT
Utilise the Plan-Do-Check-Act methodology to systematically document and manage your standards.

The right partner

At the heart of our business is a dedication to the client. Sustainable Certification understand for many business-owners, this could be their first attempt at certification and our goal is to make the process as simple and transparent as possible.

Our 'best in class' client portal provides clear insight of the certification status and audit process, giving you peace of mind at every stage.

Dedicated account managers give each client continual support for every step, making successful progression streamlined and hassle free.

The Certification Journey

Step 1 Application and Contract
Once the ISO 27001 system has been developed and implemented, an organisation should choose a certification body usually based on criteria making the process simple, hassle free and adds value.

Step 2 Pre assessment [optional]
If you are unsure if your ISMS meets the requirements, a gap analysis can be undertaken to evaluate against the system standard.

Step 3 Stage One Audit
A review of your management system(s) documentation against the standard is undertaken. This is the first step in the certification process.

Step 4 Certification Audit
The Certification Audit is conducted on site to verify that you have effectively implemented your own management system across your organisation.

Step 5 Years 2 & 3 Certification Maintenance
Conduct a Surveillance Audit at least once every 12 months to check the ongoing implementation of management systems across your organisation.

Step 6 Re-Certification
The cycle starts again with a stage 1 and stage 2 audits.

1	Application & Contract
2	Pre Assessment (Optional)
3	Stage One Audit
4	Certification Audit
5	Certification Maintenance
6	Stage One & Two Re-Certification

Client Experiences

"Sustainable Certification's approach really struck a chord with our ethos. The transparent and collaborative methodology aligned seamlessly with how Howatson+Co bridges their varied capabilities"
Hoàng Nguyễn - Chief Data & Technology Officer, Howatson+Co

"As a new client it was made easy to switch from a long-standing relationship to Sustainable Certification. A special call out to Maria Bouras & Renee Ladner who made the transition very easy. Very pleased so far".
Craig Hopwood, Supply Chain Manager, Faber Castell

"Throughout the years I have been working with Sustainable certification it has been a thorough enjoyment with a very clear and precise approach to each audit with professional guidance for my business to achieve and sustain our ISO certifications".
Stuart Norton-Baker – Group QHSE Manager, Optic Security Group

"The service provided flowed effortlessly with great communication from the auditor and Sustainable Certification. The auditors knowledge of the construction sector was a great benefit throughout the audit process."
Russell Sharp - HSEQ Manager, TVN On Country