ISO 27001 Information Security Management Systems

Information Pack

Compliance Council

Contents

ISO 27001 At a Glance

Standard for information security management systems (ISMS)

Allows businesses to overcome the innumerable threats to their information that exist today

Relevant to any business with information assets that need to be protected

Over 30,000 businesses certified globally

Information security has emerged as one of the most pressing concerns for businesses all around the world. Whether it be customer records, intellectual property or employee details, just about all organisations today hold valuable information that needs to be protected.

The alternative? Without adequate protection, companies leave themselves vulnerable to significant financial, reputational and legal damage.

In this information pack, we cover the essentials of information security management and ISO 27001. We outline which businesses need an ISMS, explore the benefits of compliance with ISO 27001, and provide clear next-steps for your business to follow on your road to certification to the standard.

“

The alternative?

Without adequate protection, companies leave themselves vulnerable to significant financial, reputational and legal damage.

”

What is ISO 27001?

The ISO 27001 standard provides requirements for an information security management system (ISMS). Updated in 2013, and currently referred to as ISO/IEC 27001:2013, this Internationally recognised standard is considered the benchmark to maintaining customer and stakeholder confidentiality.

Like other ISO management system standards, businesses can attain certification to ISO 27001 following a third-party audit from a certifying body. While certification to the standard is not required, doing so engenders trust in customers, clients, employees, shareholders and any other internal and external stakeholders.

As of the end of 2015

30,000 businesses worldwide

had achieved certification to ISO 27001

Which was a..

20% Increase on the year prior

In an environment where information security concerns are well-publicised in the media, and where lapses in data security can result in a crippling business crisis, more and more organisations are seeking certification to safeguard their valuable information assets.

As of the end of 2015, almost 30,000 businesses worldwide had achieved certification to ISO 27001; a 20% increase on the year prior.

Which Companies Need an Information Security Management System?

According to ISO (the International Organisation for Standardisation), an information security management system is a;

> **"Systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. It can help small, medium and large businesses in any sector keep information assets secure"**

Any business that holds valuable, sensitive, personal or confidential information should consider implementing a compliant information security management system. Data loss does not discriminate, which is why Australian businesses of all sizes, in all industries, are taking a proactive approach to securing it.

Information Your Business May Need to Protect

- Employee records
- Configuration of technology assets
- Internal communications
- Customer information
- Location of assets
- Project tenders
- Product development information
- Internal assets
- Financial information

Need help managing risk in your office?
Download the ISO 27001 Risk Management Toolkit

Download

Examples of Information Security Vulnerabilities

There are several places where your company information may be vulnerable, many of which are easily overlooked. Here are 10 of the most prevalent;

1 Hard Copy Documents

A survey conducted by Shred-IT revealed that just 23% of Australian SMEs have a formal Clean Desk Policy, which is essential in protecting data from visitors, freelancers and cleaners.

2 IT Infrastructure

IT Infrastructure like cables, servers and modems, are critical points through which your company information flows. Unrestricted IT Infrastructure exposes your business to tampering.

3 Essential Services

Like your IT Infrastructure, your essential services like electricity, water and air conditioning must also be protected.

4 Removable Media

Removable media like USB sticks, external hard drives, digital cameras and Bluetooth devices, are vulnerable to unsolicited downloading, uploader and file transfer if unprotected.

23% of Australian SMEs have a formal Clean Desk Policy

5 Software

Software vulnerabilities have hurt businesses time and time again, and must be effectively controlled.

51% of employees say they've copied, scanned and printed confidential information in the office

6 Office Printer

A Xerox/McAfee study found that 51% of employees say they've copied, scanned and printed confidential information in the office.

*********123

47% of internet users are holding onto passwords that are at least 5 years old

7 Employee Passwords

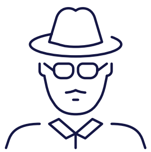
Shred-IT's survey also found that 47% of internet users are holding onto passwords that are at least 5 years old.

8 Undereducated Staff

An infamous Google study found that 48% of people will insert USB sticks they find in the parking lot into their work computers. Education of staff is vitally important to the security of your data.

48% of people will insert USB sticks they find in the parking lot into their work computers.

9 Unauthorised Employees



Authorisation controls are essential in most working environments. Employees should only have access to information they require for their position, and on the machines stipulated by the employer. Proper authorisation controls can mitigate the risk of unsolicited downloading and sharing of sensitive company information assets, like customer contact records and project documents.

10 Travelling Staff

Travelling employees are two to four times more likely to suffer information theft than non-travelling employees. An effective information security management system must cater to these in-transit data threats.

According to data recovery firm Kroll Ontrack, human error accounts for a staggering 26% of data loss incidents. Thus an information security management system doesn't only address the technical controls of data protection, but also outlines the policies and procedures necessary to deal with internal and accidental threats.

Travelling employees are **2-4x** more likely to suffer information theft than non-travelling employees

Benefits of ISO 27001 Certification

A compliant information security management system has several benefits, including;

- Allows for the secure exchange of information
- Manages and minimises risk exposure
- Ensure your business meets its legal obligations

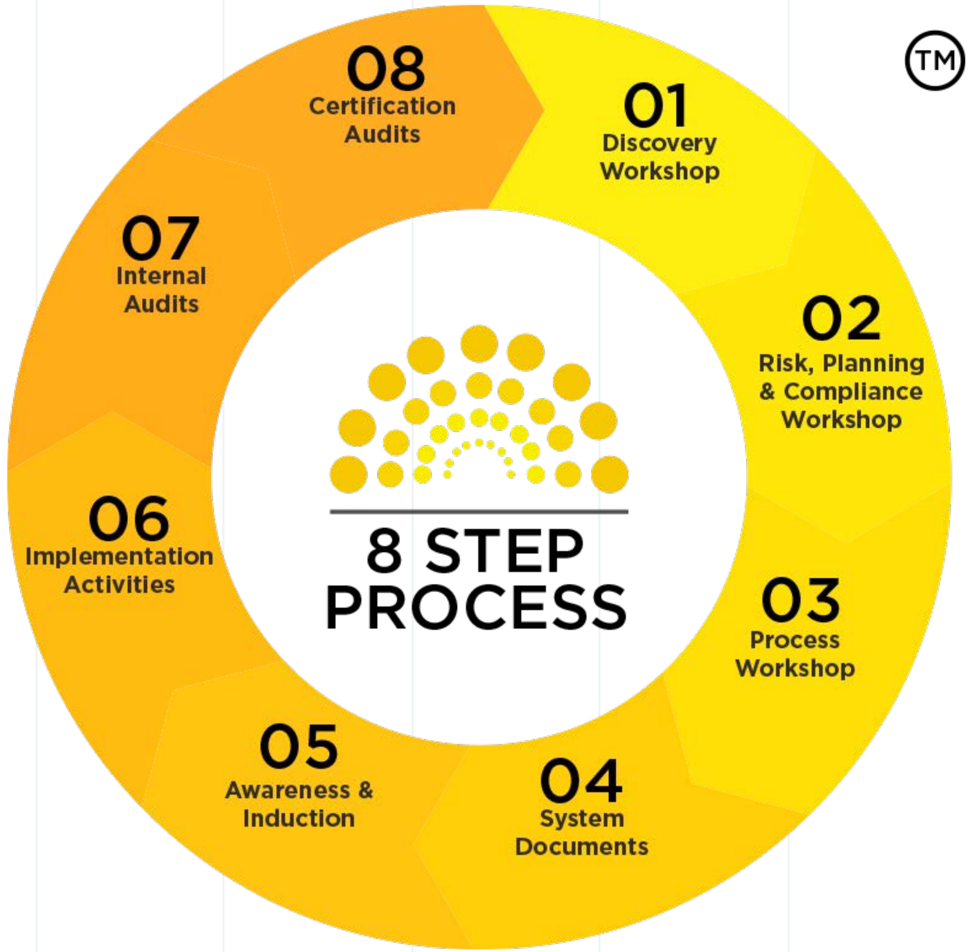
Achieving certification to ISO 27001 isn't mandatory, but has a number of additional benefits, including;

- Establish trust among internal and external stakeholders
- Gain a competitive advantage over competitors without certification
- Tender for projects where ISO 27001 certification is a prerequisite

How to Become Certified to ISO 27001

Businesses become certified to ISO 27001 following an audit from a third-party certifying body. Before attaining certification, their information security management system must be deemed compliant with the criteria outlined in ISO 27001.

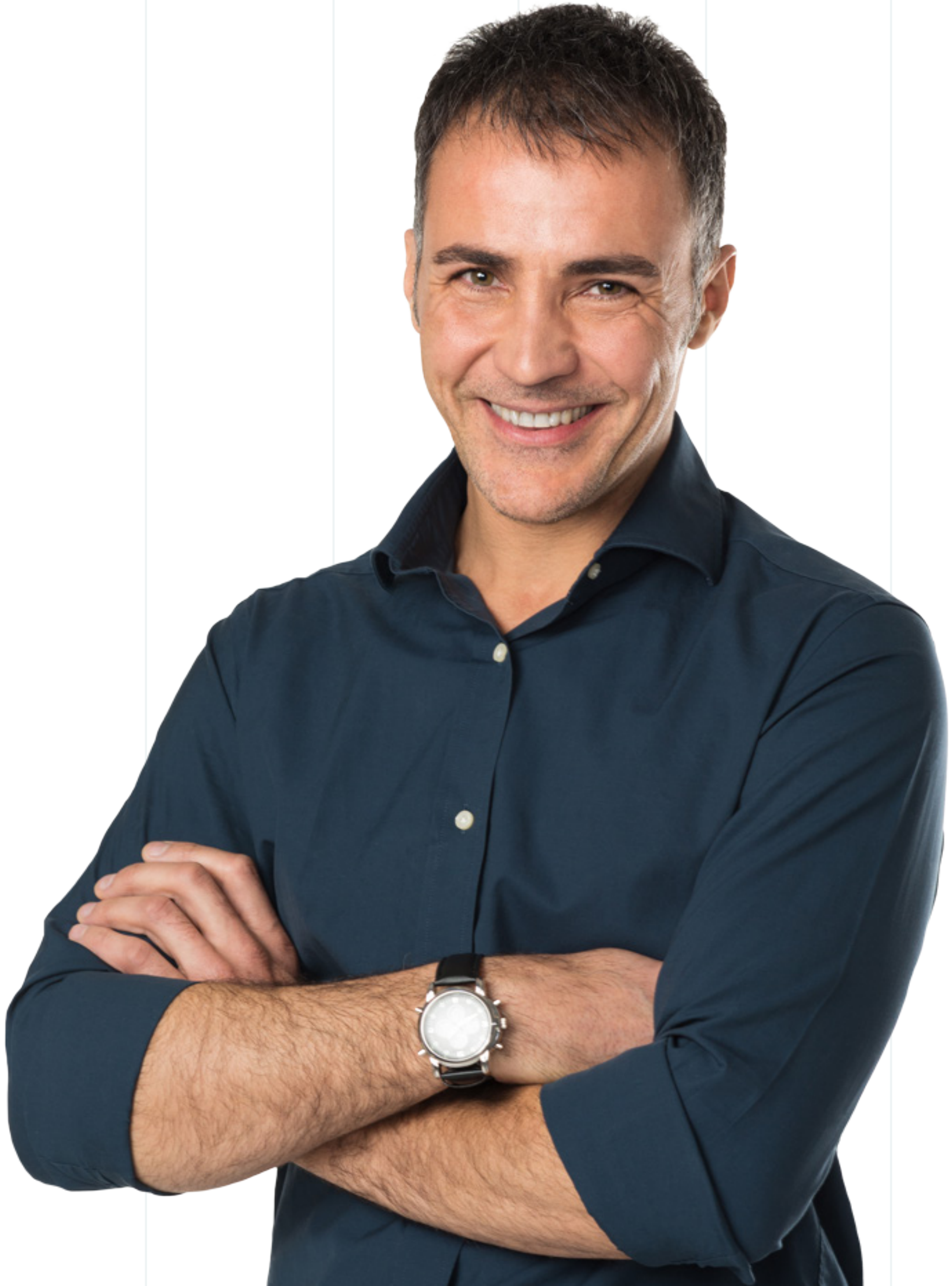
The certification process is different for every business, depending on its size, industry and the current state of its management systems. At Compliance Council, our experienced compliance consultants have designed an efficient framework to assist your business gain ISO 27001 certification between 4-6 months. We call this our 8 Step Process.



Working with Compliance Council

"I would like to thank you for all your hard work in helping us implement our Integrated Management System and achieving Certification from Best Practice in such a short period of time. Compliance Council have made a huge difference to all of our companies and our companies future and we couldn't have done it without the help of your team. I would strongly recommend Compliance Council to other organisations."

- **Manager**



Contact Us

To discuss how our experienced information security management consultants can assist your business attain certification to ISO 27001, get in touch with us today.

Contact Us

1800 771 275

info@compliancecouncil.com.au

Compliance Council