AWD

ISO 27001:2022

IMPLEMENTATION ROADMAP

Obtaining ISO 27001:2022 compliance can be a daunting task, especially for those organisations who are unfamiliar with the internationally recognised standard. However, our organisation specialises in providing practical and cost-effective solutions for achieving and maintaining ISO 27001 compliance for Australian businesses.

In this guide, we aim to educate you on the following essential elements of ISO 27001:

The fundamentals of the standard

The importance of complying with ISO 27001

The steps required to achieve implementation and certification

We understand the importance of starting off on the right foot, which is why our team of experts provide specialised support throughout the process to ensure a successful outcome. Our goal is to help you ace your audits with confidence.

AWD is dedicated to providing the necessary resources and support to ensure that your ISMS is not only compliant but also an asset to your organisation. We encourage you to take advantage of our expertise and experience to achieve ISO 27001 certification with ease.

What is ISO 27001?

ISO 27001 is an international standard that outlines the requirements for an Information Security Management System (ISMS).

The standard provides a framework for managing sensitive company information so that it remains secure. It helps organisations of all sizes and industries to protect their information assets, such as financial data, intellectual property, employee details and any other personal data. The standard is based on a risk management process and provides a systematic approach for establishing, implementing, maintaining, and continually improving information security. Organisations can be certified against ISO 27001 to demonstrate their commitment to information security and to provide assurance to customers, suppliers, and other stakeholders that their information is being handled appropriately.

Why it's important for your organisation to comply with ISO 27001?

Protects sensitive information: The standard helps organisations to protect sensitive information such as financial data, personal information, and intellectual property from potential security threats and breaches.

Demonstrates commitment to information security: Obtaining ISO 27001 certification demonstrates an organisation's commitment to information security and can help to build trust with customers, suppliers, and other stakeholders.

Enhances compliance with legal and regulatory requirements: ISO 27001 aligns with various legal and regulatory requirements such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) in the field of data protection and security.

Improves risk management: The standard provides a framework for managing information security risks and helps organisations to identify, assess, and prioritise potential security threats.

Increases overall efficiency and effectiveness: An ISMS based on ISO 27001 can help organisations to improve overall efficiency and effectiveness by streamlining security processes and reducing the potential for human error.

Helps in maintaining competitive advantage: Having certification for ISO 27001 can help organisations to gain a competitive advantage over their peers by providing a competitive edge in securing sensitive information and being compliant with legal and regulatory requirements.

ISO 27001:2022 Implementation Roadmap

1 Conduct a preliminary analysis to identify gaps in compliance

2 Define project scope and appoint manager to oversee implementation

3 Define Policy, Roles & Responsibilities

4 Conduct a risk assessment to identify potential threats

5 Provide training and awareness to employees

6 Documentation and document control

7 Implement and test controls to ensure functionality

8 Performance evaluation

9 Provide training and awareness to employees

10 Documentation and document control

Step 1:

Conduct a preliminary assessment of the current information security management system (ISMS) and identify any gaps in compliance with ISO 27001.

Conducting a preliminary assessment of the current ISMS and identifying any gaps in compliance with ISO 27001 is important for several reasons:

- Provides a baseline of the organisation's current information security management practices and helps to identify areas that need improvement.
- Helps to prioritise resources: By identifying gaps in compliance, the organisation can prioritise resources and efforts to address the most critical areas first.
- Saves time and money: By identifying gaps early on, the organisation can avoid unnecessary implementation costs and reduce the time required to achieve certification.
- Helps to understand the scope of the project and to determine the resources, time and budget required to achieve certification.
- The assessment can help to identify any existing controls or procedures that the organisation already has in place and can be leveraged, which can save time and resources.
- Helps in understanding the legal and regulatory requirements
- Helps in identifying risks and vulnerabilities and helps organisations to plan to address them, which can improve their overall security posture.

76,000+

cybercrime reports were made via ReportCyber.

13% increase

from the previous financial year.

– ACSC's annual cyber threat report

1. Review the ISO 27001:2022 standard and understand the requirements that your organisation needs to meet.

2. Define the scope of the assessment and determine which areas of the organisation will be covered.

3. Identify key stakeholders who will be involved in the assessment process, such as information security officers, IT staff, business managers, and compliance officers.

4. Collect and review documentation such as existing security policies, procedures, and guidelines.

5. Conduct interviews with key stakeholders to gather information about the organisation's current information security management practices.

6. Observe and test controls to assess their effectiveness.

7. Identify gaps in compliance with ISO 27001:2022 and document any non-conformities.

8. Prioritise the identified gaps based on their potential impact on your organisation.

9. Create a report that summarises the findings of the assessment and provides recommendations for addressing identified gaps.

10. Review the report with key stakeholders and obtain their input and feedback.

How to:
conduct a preliminary assessment ?

Step 2:

Define the scope and appoint a project manager to oversee the implementation of the ISMS.

Scope definition ensures that all relevant aspects of an organisation's information security management system (ISMS) are covered. A project manager can coordinate and prioritise activities, allocate resources, and monitor progress to ensure the successful implementation of the ISO 27001:2022 standard. A project manager can also ensure that the implementation process adheres to the set timelines and budget, and effectively communicates with stakeholders. By having a dedicated project manager, organisations can minimise risks and ensure a smooth implementation process.

Defining the scope includes:

1. Identifying the objectives and requirements of the ISMS implementation project.
2. Determination of the boundaries of the ISMS by identifying the assets, locations, and processes that need to be included.
3. Evaluation of the current state of the organisation's information security and assess any gaps that need to be addressed.
4. Identifying the stakeholders and their respective roles and responsibilities in the implementation process.
5. Defining the scope and boundaries of the ISMS in terms of the assets, locations, and processes that are included, as well as any exclusions.
6. Ensuring that the defined scope is aligned with the organisation's overall information security strategy and business objectives.
7. Obtaining agreement from all relevant stakeholders on the defined scope and communicate it to all relevant parties.
8. Regularly reviewing and updating the scope to ensure it remains relevant and adequate for the organisation's evolving needs.

The financial losses due to BEC have increased to over

$98 million

with an average loss of $64,000 per report.

– ACSC's annual cyber threat report

Step 3:

Define Policy, Roles and Responsibilities.

In this step the organisation needs to develop the Information Security Policy (ISP) that outlines the organisation's approach to information security and defines the roles and responsibilities of all stakeholders. Depending on the size and scope of the organisation these roles may include: Data Protection Officer (DPO), Information Security Manager (ISM), Information Asset Owner (IAO) and Information Security Auditor (ISA). This process involves:

1. Defining and allocating responsibilities for managing and implementing information security controls, such as access control, incident management, and disaster recovery.
2. Developing an organisational chart and ISMS responsibility matrix.
3. Ensuring that all employees and relevant third parties are aware of their roles and responsibilities with regards to information security.
4. Establishing a communication plan to ensure that information security policy and wprocedures are communicated effectively to all stakeholders.
5. Ensuring that the policy, roles, and responsibilities are regularly reviewed and updated to reflect changes in the organisation's operations, technology, and risk environment.
6. Providing training and awareness programs to raise the level of understanding of information security among all stakeholders.

One cybercrime report is made approximately every

7 minutes.

– ACSC's annual cyber threat report

Step 4:

Conduct a risk assessment to identify and prioritise potential security threats.

Conducting a risk assessment to identify and prioritise potential security threats is a critical step in the implementation of ISO 27001:2022.

The following steps are typically involved:

1. Identify the assets that need to be protected, such as information, systems, and facilities.
2. Identify the potential threats and vulnerabilities that could negatively impact the assets.
3. Evaluate risks: Evaluate the likelihood and impact of each risk, taking into account the potential consequences if the risk were to materialise.
4. Prioritise the risks based on the results of the risk evaluation and allocate resources accordingly.
5. Develop a risk treatment plan: Develop a plan to mitigate or manage the risks, including implementing controls and establishing contingency plans.
6. Monitor and review: Continuously monitor the risk assessment and review it regularly to ensure that it remains relevant and up-to-date.
7. Document findings: Document the results of the risk assessment and the risk treatment plan, including the rationale behind the decisions made.
8. Obtain approval from relevant stakeholders on the risk assessment and risk treatment plan.

Medium-sized businesses had the highest average loss per cybercrime report where a financial loss occurred. The cost per cybercrime report on average increased to 14 percent:

$39,000 -small businesses
$88,000 -medium businesses
$62,000 -large businesses.

– ACSC's annual cyber threat report

Step 5:

Provide training and awareness programs for employees to ensure they understand their roles and responsibilities in maintaining information security.

The standard requires that adequate resources are provided for the ISMS to function effectively, which means that senior management will have to consider what existing resources the organisation have internally to fulfil the roles required to support the ISMS and whether it has resource gaps that will need to be filled.

The following steps can be taken:

1. Determine training needs: Identify the training needs of employees based on their roles and responsibilities and the information security risks faced by the organisation.
2. Develop training materials: Develop training materials that are relevant and appropriate for each group of employees.
3. Provide regular training: Provide regular training sessions to all employees to ensure they are aware of the information security policies and procedures.
4. Make training accessible: Make the training materials and sessions accessible to all employees, regardless of location or role.
5. Use different delivery methods such as in-person sessions, online courses, or webinars, to cater to different learning styles.
6. Evaluate the effectiveness of the training programs and make necessary improvements.
7. Incorporate information security into ongoing training programs, such as onboarding, induction, and annual reviews.
8. Provide ongoing awareness programs and communications to reinforce the importance of information security.
9. Encourage participation: Encourage employees to participate in information security awareness activities and provide feedback on the training programs.

The number of publicly reported software vulnerabilities (Common Vulnerabilities and Exposures – CVEs) worldwide has increased by up to:

25%

– ACSC's annual cyber threat report

Step 6:

Documentation and document control.

Ensuring proper documentation and document control is important to demonstrate compliance with the standard, provide evidence of due diligence, and maintain the effectiveness of the information security management system.

Documentation hierarchy:

- Information security policy: A high-level statement that defines the organization's approach to information security.
- Procedures: Detailed instructions on how to implement and maintain the information security controls.
- Records: Records of security incidents, risk assessments, and audits.

Document control includes:

- Creation and maintenance of accurate and up-to-date documentation.
- Control of document distribution and access.
- Version control to ensure that only the latest version of a document is in use.
- Regular review and update of documentation to reflect changes in the organization's information security management system.

150,000 to 200,000

Small Office/Home Office routers in Australian homes and small businesses are vulnerable to compromise including state actors.

– ACSC's annual cyber threat report

Step 7:

Implement and test controls to ensure they are functioning as intended.

The implementation and testing of controls are crucial steps in the ISO 27001 implementation roadmap.

The following steps outline the general process:

1. Identify controls: Determine the controls required to address identified risks to the organisation's information assets.
2. Plan and design controls: Determine the design and implementation approach for each control, including any necessary resources, procedures, and schedules.
3. Implement controls: Put the controls in place, ensuring they are properly configured and integrated into the organisation's operations.
4. Test controls: Verify the effectiveness and reliability of the controls by conducting testing, such as vulnerability scans, penetration tests, or internal audits.
5. Monitor and risk assessment review: Continuously monitor and review the controls to ensure they remain effective and aligned with the organisation's changing needs and threat environment.

It is important to implement and test controls in a systematic and thorough manner to ensure that the organisation's information security management system is effective and provides the intended level of protection.

> *Excluding government sectors, the* ***health care and social assistance sectors*** *reported the highest number of cyber security incidents during the 2021–22 financial year.*
>
> ***– ACSC's annual cyber threat report***

Step 8:

Performance evaluation.

Internal audits and management review are key components of the ISO 27001:2022 implementation process and are conducted to evaluate the effectiveness of the information security management system (ISMS). Internal audits provide valuable information to the organisation to help it continuously improve its information security posture and ensure that its ISMS remains effective in protecting its information assets.

Following is an overview of the process:

1. Plan the audit and the management review: Develop a plan for conducting the internal audit, including the scope, objectives, procedures, and schedule.
2. Conduct the audit: Conduct the internal audit, which typically involves reviewing documentation, observing controls in action, and interviewing personnel.
3. Evaluate findings: Analyse the findings from the audit to determine the extent to which the ISMS is compliant with the standard and the effectiveness of the controls.
4. Report results: Prepare a report that summarises the results of the internal audit, including any non-conformities and areas for improvement.
5. Conduct a management review meeting where all the key stakeholders and top management attend and contribute to the review.
6. Follow up: Address any non-conformities and implement improvements identified during the internal audit.
7. Repeat the cycle: Schedule and conduct regular internal audits to ensure the ongoing effectiveness of the ISMS.

The ACSC received more than

25,000 calls

in the 2021–22 financial year, an average of

69 calls per day

a 15 % increase on the 2020–21 financial year.

– ACSC's annual cyber threat report

Your organisation can conduct internal audits through suitably trained auditors and engaging a professional third-party auditor.

An internal pre-certification audit by a professional ISO 27001:2022 auditor can help ensure that your organisation is fully prepared for the certification process and that any compliance gaps are identified and addressed before the formal audit.

Step 9:

Gap assessment.

A gap assessment in the ISO 27001 implementation process is an evaluation of the existing information security management system (ISMS) to determine any areas that need improvement to meet the requirements of the ISO 27001 standard. This assessment involves a review of policies, procedures, and processes, as well as an evaluation of the organisation's technology and infrastructure, to identify any gaps in compliance with the standard.
The objective of a gap assessment is to identify any weak points in the ISMS and provide recommendations for improvement so that the organisation can achieve full compliance with ISO 27001.

This is a very crucial phase in the ISO 27001:2022 implementation process where your organisation might need to consider engaging a third party auditor to do a comprehensive gap assessment of your ISO 27001 compliance and the potential risks and vulnerabilities in your information security management system (ISMS). In this phase you want to ensure that your ISMS is in line with the international standard ISO 27001.

Our team of professional internal ISO 27001 auditors can provide you with a thorough gap assessment of your ISMS, identifying areas for improvement and providing recommendations for achieving full compliance with the ISO 27001:2022 standard.

Contact us today to schedule your gap assessment and take the first step towards enhancing the security of your organisation's critical information assets.

All sectors of the Australian economy were directly impacted by ransomware in 2021–22. The ACSC received

447 ransomware

cybercrime reports via ReportCyber.

– ACSC's annual cyber threat report

Step 10:

Plan your certification audit.

The final step in the ISO 27001 implementation roadmap is planning your certification audit.

1. Choose a Registered Certification Body: Get in touch with an accredited RCB for the certification audit. Select them early and get to know their availability and fees to avoid surprises later.
2. Budget for costs: Consider factors such as number of sites and employees, and industry for initial certification costs. Also factor in maintenance costs.
3. Prepare for assessment: Select RCB and schedule assessment dates.
4. Conduct internal audits: Perform internal audits of ISMS against ISO27001:2022 standard before RCB certification assessment.
5. Ready for audit: Prepare for the two-stage certification visit. Stage One is a document review, and if successful, set a date for Stage Two. Upon successful completion, certification is achieved.
6. ISO 27001 certification audits are always challenging. Our experts in AWD will participate in the ISO 27001 Certification audit along with your staff members. We will make sure that the audit is performed in a logical and reasonable manner and ensure that all external auditor concerns are addressed.

In the 2021–22 financial year, using the new definitions, ***95 cyber incidents*** *(approximately 8% of all cyber incidents the ACSC responded to)* ***affected critical infrastructure.***

– *ACSC's annual cyber threat report*

Every business has its own unique set of vulnerabilities and it's important to protect your organisation from threats. At AWD, we understand the need for comprehensive protection - that's why our range of Cybersecurity Services offers 24/7 threat detection and compliance tailored to all budgets. Whether you're looking for ISO 27001 or Essential 8 compliance consultation, VAPT solutions or Forensic Investigations, you can rely on AWD as a trusted MSSP provider for reliable cyber security measures.

Don't wait any longer to protect your sensitive information! Trust our team of experts to guide you through the ISO 27001 implementation process and achieve compliance with the international standard for information security management.

Our proven methodology, combined with our knowledge and experience, will ensure that your business is secure and protected.

CONTACT US TODAY!

BOOK A FREE CONSULTATION AND TAKE THE FIRST STEP IN SECURING YOUR ORGANISATION.

☎ 1300 855 651

Suite 210, 134/136 Cambridge Street,
Collingwood VIC 3066 Australia

www.awd.com.au

AWD - IT, Cybersecurity & Web Solutions

Why choose AWD?

What do our clients say?

"We needed a security-focused and ISO 27001 compliant setup for our internal IT systems and reached out to a number of providers. Others told us that what we were asking for was too complex - and a handful of them provided us with quotes. AWD's quote was very competitive, and I was impressed by their deep understanding of cybersecurity solutions and compliance knowledge and expertise. They provided a compliance consultant that made our ISO 27001 implementation a hassle free and smooth journey. Our ongoing support interactions have been great as well - no matter what we ask for, the AWD team just gets it done and it's all included as part of their support. Would definitely recommend these guys!"

David Weber
Co-Founder and COO / CFO - Fortiro

WATCH CLIENT'S TESTIMONIAL

1300 855 651

Suite 210, 134/136 Cambridge Street,
Collingwood VIC 3066 Australia

www.awd.com.au

AWD - IT, Cybersecurity & Web Solutions