ISO/IEC 27001

Information Security Management

Securing your information assets

Product Guide

bsi.

...making excellence a habit.™

What is ISO/IEC 27001?

ISO/IEC 27001 is the international standard for information security management and details the requirements for a robust information security management system (ISMS).

Like to know more about ISO/IEC 27001? Book an introductory course with us now at **+6 03 9212 9638**.

Information security is concerned with safeguarding the confidentiality, integrity and availability of information, whether written, spoken or electronic. All organizations are collecting, storing and managing information of some kind, which makes information security imperative.

ISO/IEC 27001 takes a risk-based approach to the planning and implementation of your ISMS, resulting in an appropriate and affordable level of organizational security. In this way, it ensures that the right people, processes, procedures and technologies are in place to secure your organization's information assets.

ISO/IEC 27001 is suitable for organizations of all sizes, across all sectors. The standard is particularly useful in highly regulated industries such as banking, financial services, health, public and IT sectors. It is also highly effective for organizations which manage information on behalf of others as a way of demonstrating appropriate security controls are in place, and enabling customers to make an informed choice when managing their compliance with data protection requirements and other applicable legislation.

Why implement ISO/IEC 27001?

ISO/IEC 27001 provides a framework to help you implement a management system that protects both your information assets and your company, by reducing risks, litigation and downtime.

With company data becoming ever more accessible throughout organizations, it is important to minimize your vulnerability to security breaches. Regardless of the type of information, be it financial data, computer software code or customer/supplier lists, or how it is stored, robust security controls are necessary. With a clear security strategy you can assure stakeholders, especially customers, that their personal information is being protected. Adopting this international standard demonstrates that your organization is using a risk-based approach to selecting and implementing information security controls.

Initially, it may be perceived that implementing an ISMS can be a drain on resources, offering little in the way of financial return. In practice, it has been shown that costs will be outweighed by preventing and reducing the impact and frequency of security incidents. Since the upgrade from BS 7799 there has been a sharp increase in the global market for ISO/IEC 27001 certification across a variety of sectors. It has become a commonly used and cited standard for compliance, and is increasingly specified as part of contractual agreements.

By implementing ISO/IEC 27001 you are providing your organization with a structured approach to the planning, implementation and management of an ISMS that will help you reduce incidents and improve stakeholder confidence

85% of BSI information security clients built stakeholder confidence through the implementation of a system certified to ISO 27001*

*BSI Excellerator Research

The benefits of ISO/IEC 27001

ISO/IEC 27001 brings many benefits, especially when combined with independent certification from BSI. These include:

Demonstrating the independent assurance of your ISMS and security controls, and meeting corporate governance and business continuity requirements

+

Independently demonstrating that applicable laws and regulations are identified and that there are processes in place to ensure compliance

+

Providing a competitive edge by meeting contractual requirements and demonstrating to your customers that the security of their information is paramount

+

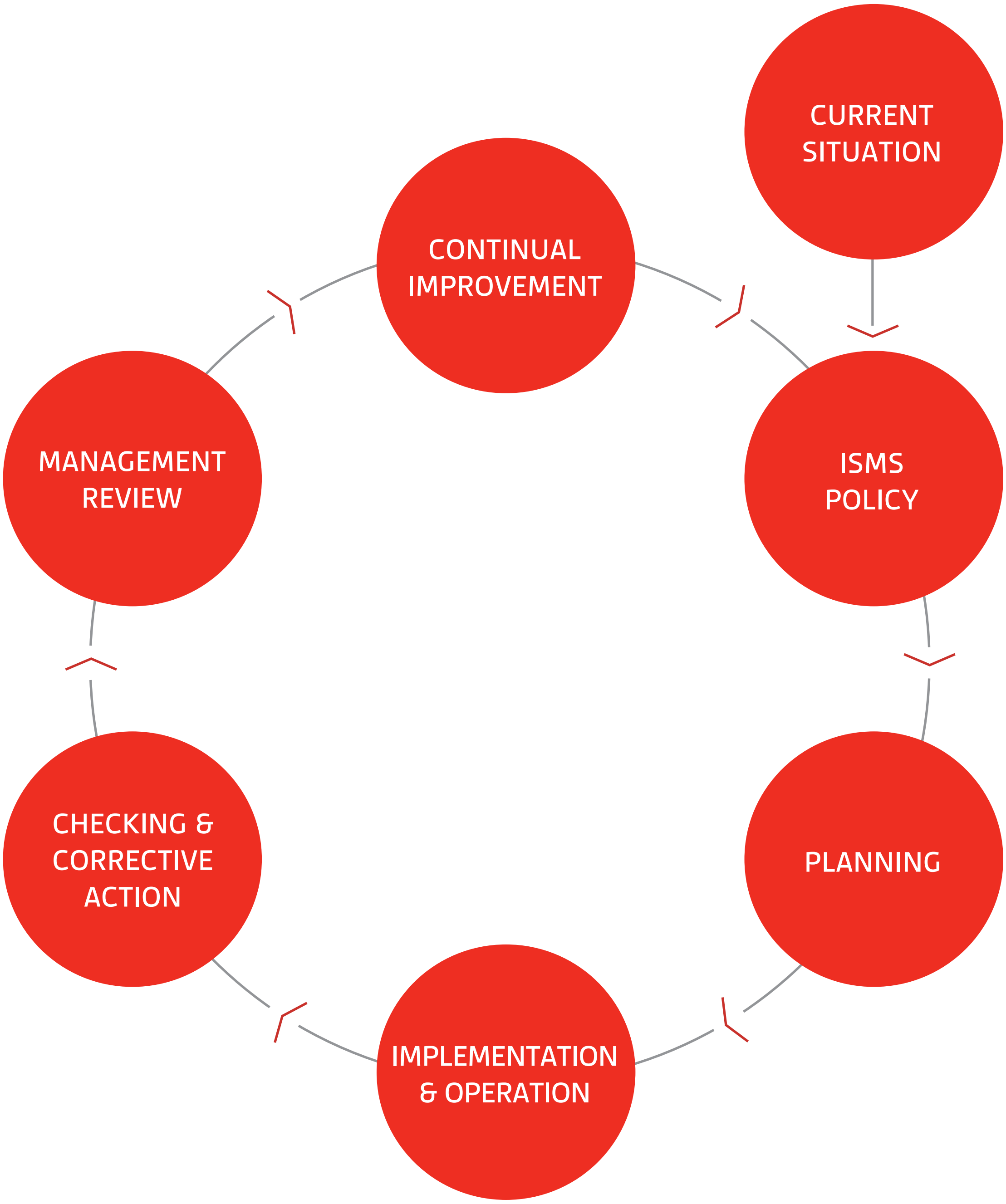
Independently verifying that your organizational risks are properly identified, assessed and managed, while formalizing information security processes, procedures and documentation

+

Proving your senior management's commitment to the security of its information

+

The regular assessment process helping you to continually monitor your performance and improve.



ISO/IEC 27001 Model

Before you can implement an Information Security Management System (ISMS), you must understand what information you currently have and how it is used by your business. Your current activities, products and services all impact on information security. Using ISO/IEC 27001 helps you to focus on and understand the information security issues up front and provides a clear framework for ISMS development.

Policy and Planning

ISO/IEC 27001 is made up of five main requirements sections and an appendix that contains security controls, each with specific aims and focus, organized into the following groups:

Security policy - To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Organization of information security - To manage information security within the organization and to maintain the security of the organization's information and processing facilities that are accessed, processed, communicated to, or managed by external parties.

Asset management - To achieve and maintain appropriate protection of organizational assets.

Human resources security - To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, are aware of information security threats, and exit an organization or change employment in an orderly manner.

Physical and environmental security - To prevent unauthorized physical access, damage and interference to the organization's premises and information. To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

Communications and operations management - To help ensure that information is processed correctly, backed up securely and handled appropriately.

Access control - To assist with controlling access to information, networks and applications, preventing unauthorised access, interference, damage and theft.

Information systems acquisition, development and maintenance To ensure that security is an integral part of the information system, helping with securing applications, files and reducing vulnerabilities.

Information security incident management - To ensure information security breaches and issues are communicated consistently, in a manner allowing timely corrective action to be taken.

Business continuity management - To ensure you counteract interruptions to business activities and protect critical business processes from the effects of major information systems failures or disasters.

Compliance - To avoid breaches of any law, statutory, regulatory or contractual obligation, and of any security requirements. To ensure compliance of systems with organizational security policies and standards.

Implementation and operation

Implementing an ISMS is a step by step process, with each step building on the previous to form a coherent and logical set of processes. Only at the end of the process is a BSI audit undertaken.

Scoping study

This initial step sets the scope of the project. The scope should reflect the clear objectives of the business and the project, including any specific requirements, locations and departments. This scope will guide you later in the process, keeping you focused on your task.

Risk assessment

A risk assessment is used to identify all your information assets and consider the associated risks, threats and vulnerabilities. This will enable you to draw up a list of information threats, which can be prioritised based on the level of risk they pose to your information assets.

Gap analysis

A gap analysis is a review of your progress so far and looks at how you have implemented the requirements of ISO/IEC 27001 and the applicable security controls. Some controls as set out in ISO/IEC 27001 may not apply to your organization and the information security risks to which it is exposed. If certain activities, such as performing electronic transactions, are not undertaken within your organization then the associated control can be formally excluded. A gap analysis can be carried out internally, or with the assistance of a BSI expert, and will give you a good indication of any requirements that still have to be met to ensure your ISMS is ISO/IEC 27001 compliant.

Statement of applicability

The statement of applicability should list all the controls and references to how and why they apply to your scope.

Security improvement programme

By this stage you will have a good understanding of your information security situation. Revised policies and procedures now need to be developed to protect the information assets against the risks you have identified, such as staffing issues, technical resources and improvements. Some may require immediate action, while others will simply require updated rules or instructions – perhaps as simple as locking filing cabinets after use.

Testing, review and internal audit

As you take actions intended to improve information security, each action or change in process must be tested to ensure it delivers the required improvements. This could include an external BSI assessment, penetration testing or peer review. Internal audits of the ISMS must also be undertaken.

Implementation

Once your policies, procedures and controls have been developed, you will need to deploy them. As every organization is different, working practices also differ. Implementing policies can be aided by training, discussion and promotion. The positive involvement of senior management is also required to make these changes.

Document finalizatio

The statement of applicability (SOA) should be clear, concise and easily understood. Because ISO/IEC 27001 requires ongoing improvement, your documentation should be regularly reviewed and amended to reflect changes in business practices, processes and the results of your ongoing security improvement programme.

Management review

Management shall review the organization's ISMS regularly to ensure its continued suitability, adequacy and effectiveness. Information security should be pivotal to the daily operations of an organization and adjustments made as appropriate to improve the overall performance of the system.

Continual improvement and corrective action

As with all management system standards there is a need to look back at what has been achieved. Internal audits and management reviews continue to be key methods of assessing the performance of the ISMS and tools for its continual improvement. Nonconformities of the ISMS have to be dealt with together with corrective actions to ensure they don't happen again. As with all management system standards, continual improvement is a core requirement of the standard.

Learn how to implement ISO/IEC 27001 with one of our training courses.
Visit **bsigroup.com.my/isoiec27001-training**

With BSI our commitment does not stop with a certificate

BSI offers independent third-party certification to ISO/IEC 27001. With BSI the certification process is simple. After you apply we appoint a client manager who will guide you and your business through the certification process. Once you've achieved the certificate our support doesn't stop there. We'll continue to visit your organization for three years, delivering the expertise you need to remain compliant. So not only will you be able to demonstrate to stakeholders and customers that you comply with information security best practice, you will also benefit from regular audits and opportunities for improvement.

Find out how much ISO/IEC 27001 with BSI will cost your organization. Contact us **+6 03 9212 9638** or visit **bsigroup.com.my/certification**

Route to certification

1. Buy the Standard.
   Visit **bsigroup.co.uk/buy27**

2. Make contact. Call us on
   +6 03 9212 9638

3. Complete the BSI application form

4. Plan your BSI training

5. Consider an optional BSI gap analysis (pre-certification audit)

6. Your BSI assessment team is appointed

7. Formal BSI assessment – stage 1

8. Formal BSI assessment – stage 2

9. BSI certificate awarded

10. BSI certification and beyond

Need help implementing your system?

At BSI we are dedicated to helping you every step of the way. We created the Associate Consultant Programme (ACP) as an impartial service to help you find the consultancy support you need. We aim to make the process of certification as simple as possible and, as an independent certification body, choose not to offer or recommend specialist consultancy services. That's why we set up the ACP with more than 100 members across the UK, all with demonstrated experience of working with certified management systems. To find out more visit bsigroup.com/27acp

BSI information security solutions

Whether you want to implement ISO/IEC 27001 to protect your information assets and develop best practice, or require full certification to meet contractual requirements and reassure customers, BSI can assist you along your journey. We offer a range of information security products including:

- Standards and publications
- Information guidance and advice
- Training – courses, in-house and elearning
- Gap analysis
- Management system certificatio
- Entropy Software™ – management system software for improving security controls

Why BSI?

BSI is recognized by the UK Government as the National Standards Body (NSB) for the UK. We develop, publish and market standards and related products. Our business enables organizations to perform better and make excellence a habit. For more than a century our experts have been challenging mediocrity and complacency to help embed excellence into the way people and products work... to perform better, reduce risk and achieve sustainable growth. Our clients range from globally recognized brands to small, local companies in 150 countries worldwide. We are a Royal Charter company that develops and delivers products and services in a truly inclusive way, we are committed to continual improvement and work with the highest level of integrity. Regardless of your location, organization size or sector, nothing says confidence like the BSI mark.

To find out more about our assessment and certification solutions

Visit our website **bsigroup.com.my/certification**

T: +6 03 9212 9638 (Kuala Lumpur)
+6 07 276 3506 (Johor Bahru)
+6 04 227 9651 (Penang)
+6 082 232 003 (Kuching)
E: info.malaysia@bsigroup.com
W: bsigroup.com.my