SIS CERT.™

We Do Not Sell, We Certify!

27001

INFORMATION SECURITY MANAGEMENT SYSTEM

support@siscertifications.com

+91 8860610495

www.siscertifications.com

ISO/IEC 27001 - AN INTERNATIONALLY ACCEPTED STANDARD FOR THE INFORMATION SECURITY MANAGEMENT SYSTEM

The 27000 series of standards was established in 1995 as BS 7799 and was drafted by the UK's Department of Trade and Industry (DTI). The standards go correctly by the title "ISO/IEC" since they are developed and maintained jointly by two international standards organizations: ISO (the International Organization for Standardization) and the IEC (the International Electro-technical Commission). However, in the interest of simplicity, the "IEC" section is often abandoned in daily use.

Currently, a total number of 45 standards are published in the ISO 27000 series. Among those, ISO/IEC 27001 is the only standard for certification. All other standards provide guidance on how best practices are implemented. Some render guidance on how to develop an ISMS for specific industries; others offer guidance on how to carry out key data security risk management operations and controls.

Most companies own or access valuable or sensitive information. Failure to provide adequate protection may have serious operational, financial and legal implications. Sometimes, this may lead to total business failure. Organizations need to build resilience in how they manage information security. Internationally recognized, ISO/IEC 27001 is an excellent framework that assists organizations in managing and protecting their resources to keep them safe.

ISO/IEC 27001 is an internationally recognized standard for information security management systems (ISMS). It offers a robust framework for safeguarding data that can be adapted to all types and sizes of organizations. The organizations that are highly exposed to information security and safety risks are increasingly choosing to execute an ISMS that abides by ISO/IEC 27001.

ISO/IEC 27001:2013 is the current edition of the standard for bodies to be certified

HOW ISO/IEC 27001 STANDARD WORKS AND WHAT IT OFFERS YOU AND YOUR COMPANY

security has been as important as ever. ISO/IEC 27001 not only helps protect your business but also sends a clear signal to customers, vendors, and to the marketplace in which your organisation can handle information security.

ISO/IEC 27001 is a robust framework to help you protect data, such as financial data, intellectual property or sensitive client information. It helps you determine risks and puts in place security measures that are appropriate to your company so that you can manage or reduce the risks associated with your personal data. It helps you continuously review and refine how you do it, not only for today, but for the future as well. As a result, ISO/IEC 27001 protects your company, your reputation and adds value.

The latest version of ISO/IEC 27001 was released in 2013 to help ensure its continued relevance to modern business challenges and ensure compliance with the risk management principles of ISO structure, which is a common framework for all revised and future standards of the ISO management system, including ISO 9001:2015 and ISO 14001:2015.

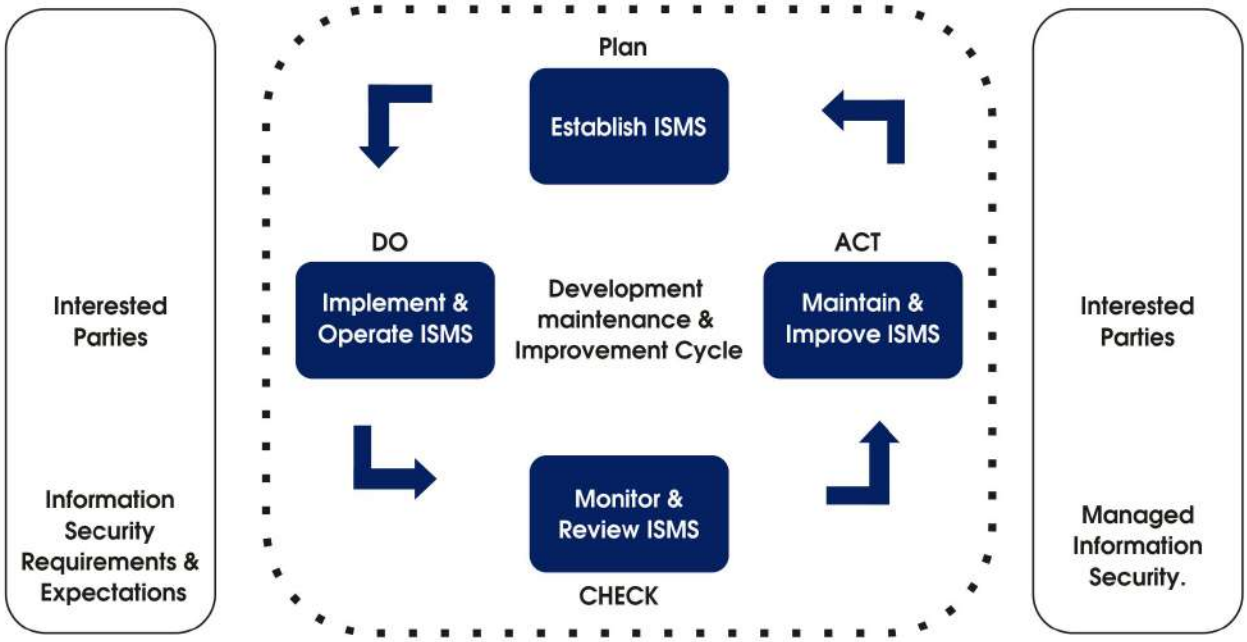
PDCA CYCLE

This certification is based on the Plan-Do-Check-Act (PDCA) cycle, also referred to as the Deming Wheel or the Shewhart cycle. The PDCA cycle can be applied not only to the overall management system but also to each individual component to emphasize continuous improvement.

In brief:

PLAN-DO-CHECK-ACT (PDCA)

MODELAPPLICABLE TO ISMS PROCESSES



Plan-Do-Check-Act is a typical closed-loop system. This ensures that the learnings from the "Do" and "Check" steps are used to inform subsequent "Act" and "Plan" steps. Theoretically, it's cyclic, but it's more of an ascending spiral as learning moves you through the process.

BENEFITS OF IMPLEMENTING ISO/IEC 27001 STANDARD EXPAND YOUR ACCESS TO MORE BUSINESS OPPORTUNITIES WORLDWIDE

Information security is becoming more and more important to organizations, and the acceptance of the ISO/IEC 27001 is therefore becoming increasingly frequent. Most organisations now recognize that it's not a matter of whether a security breach will affect them; it's an issue of when.

Implementing an ISMS and the achievement of ISO/IEC 27001 certification is an important undertaking for most organizations. But if they do it effectively, there are significant benefits to organizations that rely on the protection of valuable or sensitive details.

ISO/IEC 27001 certification helps your organization stand out as a responsible supplier, guaranteeing information security.

Enhances your corporate reputation:

It helps enhance the reputation of your organization and builds customer and other shareholder confidence through strategic communication.

Maximizes corporate profits:

You can maximize the benefits by ensuring the protection and security of data by implementing the standards.

Mitigates data security risks:

The implementation of the Information Security Management System allows for the control and management of the risks of incidents such as data loss, cybercrime, hacking, etc. which may occur within your organisation.

Strengthen your informational credibility:

It helps you prove that you have credibility in protecting corporate details among customers, customers, or other shareholders.

Reduced organizational expenses:

This certification helps monitor any data security violations. This saves tremendous costs associated with such a breach.

KEY CONCEPTS & TERMINOLOGY

The primary aim of an ISMS is to protect sensitive and useful data. Sensitive information usually includes employee, client and vendor details. Valuable information can include intellectual property, financial data, legal documents, business data.

THE TYPES OF RISKS ASSOCIATED WITH SENSITIVE AND VALUABLE INFORMATION CAN GENERALLY BE GROUPED INTO THREE CATEGORIES:

These kinds of information security risks are commonly known as "CIAs".

- **Information security risks** usually arise because of the presence of threats and vulnerabilities to the assets that process, store, and hold protect or control access to the data causing incidents.
- **Assets** are persons, equipment, systems or infrastructure.
- **Information** is the set of data that an organization wants to safeguard, such as employee records, client records, financial records, design data, test data, etc.
- **Incidents** are adverse events that lead to a loss of confidentiality (for example, a data breach), integrity (e.g. corruption of data) or availability (e.g. system failure).
- **Threats** cause incidents and can be harmful (e.g. a burglar), accidental (e.g. a keystroke blunder) or an act of God (e.g. A flood).
- **Vulnerabilities** such as open desktop windows, source code errors, or the location of buildings next to rivers, increase the likelihood that a threat will cause an unwanted and costly incident.

ISO/IEC 27001 CERTIFICATION REQUIREMENTS

The high-level structure of ISO/IEC 27001 is built around the principle of the Plan-Do-Check-Act. This Annex SL document comprises ten sections, the first three of which are of an introductory nature, whereas the seven others are auditable and provide the requirements for implementing ISO/IEC 27001. The structure includes some mandatory requirements for effectively implementing the Information Security Management System (ISMS) within an organization.

Let's go through the final seven sections for ISO/IEC 27001

- **SECTION 4-** Context of the organization: It focuses on ISMS within your organization and understanding of client needs. These factors can be external or internal and can affect intrigued parties, such as customers, contractors, stakeholders, etc.
- **SECTION 5-** Leadership: This highlights the importance of senior management when implementing an ISMS. This involves communicating the data security policy, assigning roles and responsibilities to the various levels of the workforce.
- **SECTION 6-** Planning: This includes planning the objectives of your current management system and analyzing the associated risks, in order to eliminate these risks.
- **SECTION 7-** Support: Here, the organisation is informed about the tools, technologies and resources needed to implement the ISMS.
- **SECTION 8-** Operation: It addresses the business requirements for the right ISMS.
- **SECTION 9-** Performance evaluation: This section includes monitoring and measuring the progress of an ISMS in terms of protection or security.
- **SECTION 10-** Improvement: This ensures that you have an effective ISMS. It ensures that your organization can respond to changing market demands through continuous improvement of the management system.

AN INFORMATION SECURITY MANAGEMENT SYSTEM PROMOTES ALL 7 QUALITY PRINCIPLES

1. **Customer focus:** This ISO certification aims to improve for the best of the interested parties and the customer. This will help support the customer, grow the customer base, and ensure that their needs and expectations are communicated while monitoring the entire organization.
2. **Leadership Involvement–** To achieve quality objectives, leaders must establish a unity of purpose through alignment of strategy and policies, procedures and resources to better coordinate organizational processes and establish a culture of trust and integrity, provide people with the resources, training and authority to act on accountability.
3. **Employee engagement**–For efficiency reasons, people at all levels can accomplish this by communicating with employees, their organizational needs, sharing knowledge and experience, recognising contributions, learning and improving people.
4. **Process approach** –When activities are understoodand performed, the effectiveness of outputs delivered increases by understanding organizational capacity and identifying resource constraints before taking action.
5. **Improvement -** Improvement is important to an organization in order to maintain the existing level of performance and even continue to develop, this can be done by providing adequate training and understanding of how work proceeds with this follow-up, audit review and planning, implementation, recognition and recognition, which will translate into anticipation of internal and external risks and opportunities, and an improvement in process performance.
6. **Evidence-Based Decision-Making** - To learn from errors is simply that decisions should be based on an assessment of the details. This will allow for more effective solutions, by adding more.
7. **Relationship Management**–Managing relationships with relevant stakeholders, such as suppliers, can be achieved through maintaining a well-managed supply chain that ensures a stable flow of products and services, determining the relation of the interested party that needs to be managed.

ISO/IEC 27001:2013 CERTIFICATION JOURNEY

ISO27001 HISTORY

CODE OF PRACTICE BS7799 1990 → BS7799-1 1995 → BS7799-2 1998 → ISO17799 2000 → ISO27001 2005 → ISO27001 2013

The latest version of ISO/IEC 27001 is from the British Standard Institution BSI-7799, released in 1995. It was drafted by the UK government's Department of Trade and Industry (DTI) and composed of several parts. The ISO then made it an internationally recognized standard. ISO/IEC 27001 was issued in October 2005, replacing the previous BS7799-2 standard. This is a specification of an ISMS. ISO 27000 Series information security best practices to help organizations protect intellectual property and information resources.

ISO/IEC 27001:2013 is the most current version of the international standard and incorporates the 2017 amendments.

The information security management standard applies to fields such as:

IT Companies: cloud services, backup & disaster recovery, network security, managed print services, computer training. IT consulting, help desk support many more. **Financial Industries:** Retail Banks. Retail banks are the classic deposit-taking institutions that accept cash deposits from savers and pay interest on those savings: Investment Banks, Investment Managers, Government Institutions, exchanges and clearinghouses, Payment Processors, Insurance Providers. **Telecommunication Industry:** cable companies, internet service providers, satellite companies, and telephone companies.

GET THE BEST OUT OF YOUR BUSINESS MANAGEMENT SYSTEMS

DEMONSTRATE YOUR CAPACITY TO PROTECT YOUR CUSTOMERS' DATA WITH ISO/IEC 27001

Tips for successfully implementing an ISMS:

1. **To begin with,**
   "Why?" Ensure that the reasons for implementing an ISMS are clear and aligned with your strategic direction; otherwise, you may not receive critical support from senior management.

2. **Then think about "What for?"** Implementing and maintaining an ISMS requires meaningful involvement so make sure that your scope is sufficiently broad to cover the critical information that needs to be protected, but it's not so significant that we don't have the resources to implement and maintain it.

3. **Engage all your key players. Senior management in setting the context,** requirements, policies and objectives; managers and employees with invaluable knowledge of risk assessment, process design, and procedure writing.

4. **Keep in touch throughout the process with all your stakeholders.** Tell them what you're doing, why you're doing it, how you plan to do it, and how they're going to take part. Provide periodic updates on progress.

5. **Seek external help wherever you need it.** Do not fail due to lack of internal technical expertise or skills. Managing information security risks often requires expertise. However, be sure to verify third-party references before committing them.

6. **Streamline your processes and related documentation.** It may expand to become larger.

7. **Design and apply guidelines you can follow in practice.** Don't make the mistake of documenting an overly complicated rule that no one can follow. It is preferable to accept a risk and keep looking for ways to manage it.

8. **Don't forget your suppliers**. Some providers will assist you in improving your ISMS, others will increase your risk. Make sure that all the high-risk providers have controls in place that are at least as good as yours. If they don't find another way.

9. **Train, train and train once more.** Information security is probably a new concept for many of your employees, or many of them. People may need to change habits rooted through the years. One awareness information session is unlikely to be enough.

10. **Keep in mind to allocate enough resources to regularly test your controls.** The threats your organization faces will constantly change and you need to test whether you can respond to those threats

WHAT TO DO NEXT ONCE IMPLEMENTED

AWARENESS TRAINING: Your organization should become more aware of the various standards covered by ISMS. Separate training meetings should be held for executives, middle managers and junior managers, which will help create a motivating, implementation - ready environment.

INTERNALAUDIT: A strong internal audit system is crucial for the organization. Internal auditor training is recommended and the AQN can offer internal auditor training for the standards you are implementing. It is important to implement corrective actions to improve each of the documents audited to close the gaps and ensure the efficiency of the ISMS.

POLICY AND OBJECTIVES: Your organization should develop an integrated quality policy, environmental policy, health and safety policy, information security policy and relevant objectives in order to meet the requirements. Working with high- level management, your business should hold workshops with all levels of management staff to define integrated goals.

CONDUCT A MANAGEMENT "SYSTEM" REVIEW MEETING:
Senior management should review the various formal operational aspects of the organization that apply to existing standards. Review policy, objectives, internal audit findings, process performance results the results of the complaints, feedback and legal compliance, the results of the risk and incident assessment, and the development of a post-meeting action plan, which must be recorded in minutes.

INTERNAL GAPANALYSIS: Your organization should determine and compare the level of conformity of existing systems with the standards requirements of your new ISMS. The staff involved must understand the operations of the organisation and develop a process diagram for the activities within the company.

DETAILED REVIEW OF GAPS IN IMPLEMENTED SYSTEMS:
A formal pre - certification gap analysis should be conducted to evaluate the effectiveness and compliance of implementing the system within the organization. This final gap analysis will prepare your organisation for the final assurance verification.

DOCUMENTATION / PROCESS DESIGN: The organization should create process documentation that meets the relevant standards. Draft and implement a manual, functional procedures booklet, work instructions and system procedures and provide corresponding terms.

CORRECTIVE ACTIONS: The organization should be prepared for the final certification verification, provided that the deviation analysis verification performed at the last stage and all non-conformances (NCs) have been remediated. Verify that all significant Ncs are closed and that the organisation is prepared for the final certification audit.

DOCUMENTATION / PROCESS IMPLEMENTATION: The processes and documents developed in Phase 4 should be rolled out across the organization, covering all services and activities. The organization should organize an implementation workshop according to the ISO standard.

FINAL CERTIFICATION AUDIT:
After completion, your organization should be recommended to include in the required standard. CONGRATULATIONS

SIS CERTIFICATIONS

OUR MISSION IS TO CREATE THE WORLD'S BEST MANAGEMENT SYSTEMS AND MAKE THEM GLOBALLY ACCESSIBLE AND USEFUL.

SIS CERT.™

We Do Not Sell, We Certify!

At SIS, we build excellence by promoting our customers' success through ISO 9001 standards. We help organizations strengthen their resilience, helping them to d evelop sustainably, adapt to change, and prosper over the long term. Excellence is our habit. For over 25 years, our experts have challenged mediocrity and complacency to help incorporate excellence into the workings of people and products. With over 15,000 customers in more than 30 countries, SIS is an organization whose standards inspire excellence throughout the world.

OUR PRODUCTS & SERVICES

We offer a unique mingle of complementary products and services, administered by our threeoperational components: Knowledge, Assurance and Compliance

KNOWLEDGE

The heart of our business is focused on the knowledge we create and transmit to our clients. When it comes to frameworks, we continue to build our reputation as an expert body, bringing together industry experts to shape standards at the local, regional and international levels. In fact, SIS originally developed eight of the world's ten most stringent management systems.

ASSURANCE

Independent assessment of whether a process or product complies with a specific standard ensures that our customers achieve a high level of excellence. We educate our customers on world - class implementation and auditing techniques. Optimize the benefits of our standards.

COMPLIANCE

In order to receive real long-term benefits, our customers need to ensure continued compliance with regulations, a market need or a booth so that it becomes a habit. We offer an array of differentiated services and management tools that facilitate this process

TM

SIS CERT.

We Do Not Sell, We Certify!

More information call us
+91 8860610495

VISIT OUR WEBSITE
www.siscertifications.com

support@siscertifications.com