



Integrated Quality Certification Private Limited

ISO 27001 – Information Security Management System Requirements

Management System

A Management System is the framework of processes and procedures used to ensure that an organisation can fulfil all tasks required to achieve its policies and objectives. Documented information ensures that everyone is not just "doing his or her thing", that there is a defined way to complete each of the business process organization has planned effectively and efficiently utilizing available resources. Management system ensures that all personnel are aware of their roles, responsibility and authorities for effective implementation of process including continual improvement.



Information Security



Information security, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge).

Information security's primary focus is the information assurance and balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while ensuring information is not compromised in any way when critical issues arise and maintaining a focus on efficient policy implementation, all without hampering organization productivity. These issues include but are not limited to natural disasters, computer/server malfunction, and physical theft.



Integrated Quality Certification Private Limited

ISO 27001 – Information Security Management System Requirements

Information security threats come in many different forms and the most common threats today are software attacks, theft of intellectual property, theft of identity, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. The theft of intellectual property has also been an extensive issue for many businesses in the information technology (IT) field. Sabotage usually consists of the destruction of an organization's website in an attempt to cause loss of confidence on the part of its customers.

INFORMATION SECURITY MANAGEMENT SYSTEM



An Information Security Management System outlines and demonstrates an organisation's approach to Information Security. It includes how an organisation identifies risks and opportunities that relate to its valuable information and associated assets and how it overcomes these

Information being valuable, poor information security can be costly. Whether it is computer security, physical security, broader cybersecurity, other privacy or just getting towards best practices, ISO 27001 is the recognised standard that others build from.

Planned Information Security Management System (ISMS) formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. ISMS preserves the confidentiality, integrity and availability of information by applying a risk management process, thus giving confidence to interested parties that risks are adequately managed.



Integrated Quality Certification Private Limited

ISO 27001 – Information Security Management System Requirements

Confidentiality – is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes

Integrity – maintaining and assuring the accuracy and completeness of data over its entire lifecycle i.e., data cannot be modified in an unauthorized or undetected manner

Availability – information must be available when it is needed i.e., the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

Broadly speaking, risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). Vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (man-made or act of nature) that has the potential to cause harm. The likelihood that a threat will use a vulnerability to cause harm creates a risk.

Concept of Risk-based thinking enables an organization to determine the factors that could cause its processes and its information security management system to deviate from the planned results, to put in place preventive controls to minimize negative effects and to make maximum use of opportunities as they arise. Risk being the effect of uncertainty, thus (any uncertainty) results in having positive or negative effects. A positive deviation arising from a risk can provide an opportunity, but not all positive effects of risks results in opportunities.

ISO 27001 requires that management:

- Define ISMS framework
- Systematically examines the organisation's information security risks / scenario's, taking account of the threats, vulnerabilities, and impacts.
- Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable.
- Providing proper awareness, training and education to others
- Adopts an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an on-going basis.

Controls are the practices to be implemented to reduce risks to acceptable levels. Controls can be technical, organizational, legal, physical and human.

Reasons to go for ISO 27001 Certification:

Primary reasons:

- Improve interested parties' trust by assuring compliance with their requirements
- Improve marketing edge (image and credibility) by attaining certification to ISO 27001
- Reduce expenses related to information security incidents
- Improve internal organization by better defining responsibilities and duties



Integrated Quality Certification Private Limited

ISO 27001 – Information Security Management System Requirements

Secondary reasons:

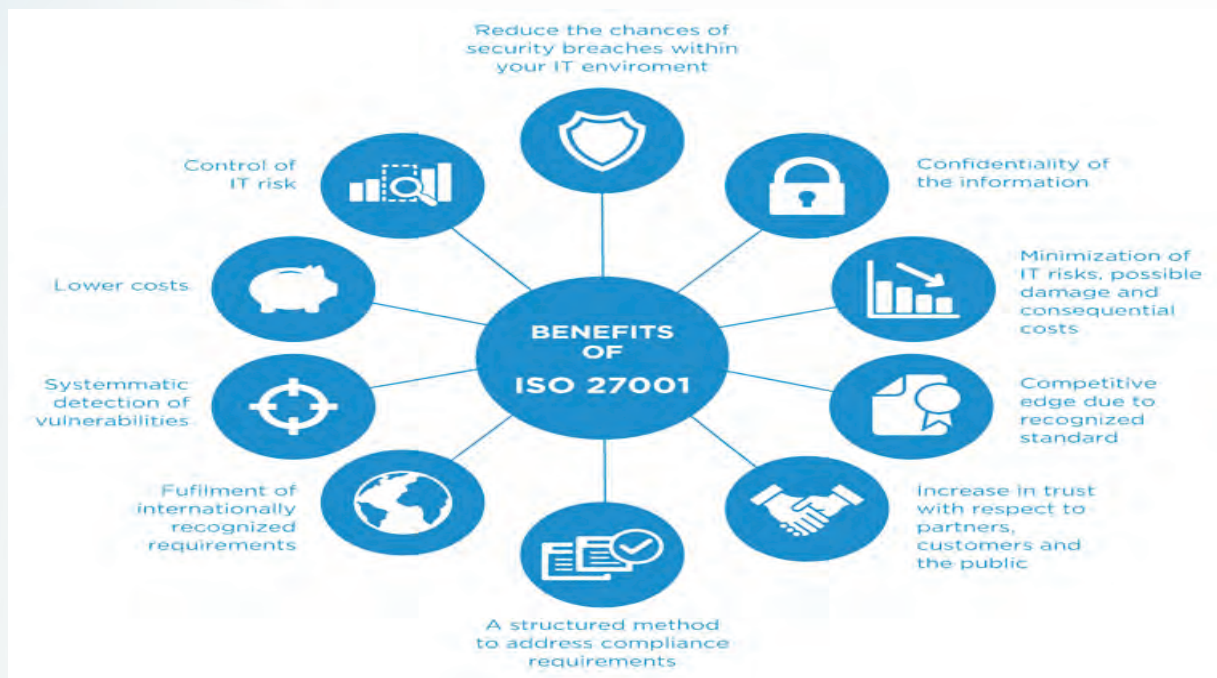
- Integrate information security to business process for better alignment
- Improve decisions by basing them on data from the information security management system
- Create a culture of continual improvement of the information security
- Improve employee, and other interested parties', engagement in information security improvement

Organisations that claim to have adopted ISO 27001 can therefore be formally audited and certified compliant with the standard.



Prepared by Technical Committee ISO/IEC JTC-1, ISO 27001 – information security management system standard has earned a global recognition as the basis for providing a framework which helps organizations, establish, implement, operate, monitor, review, maintain and continually improve ISMS.

Benefits of ISO 27001 Certification:






Integrated Quality Certification Private Limited

ISO 27001 – Information Security Management System Requirements

- Improves company reputation in the market
- business' security risks are managed cost-effectively
- Improved communication process as people work together across functions and levels
- sends a valuable and important message to customers and business partners that this business does things the correct way
- It demonstrates a clear commitment to Information Security Management to third parties and stakeholders
- It can provide a framework to ensure the fulfilment of commercial, contractual and legal responsibilities
- It provides a significant competitive advantage, and can effectively be a license to trade with companies in certain regulated sectors
- It provides for inter-operability between organisations or groups within an organisation
- It can provide compliance with, or certification against, a recognised external standard which can often be used by management to demonstrate due diligence.

Any organization seeking to improve organizational information security systems, seek marketplace recognition, build trust and improve stake-holders confidence, ISO 27001 is a valuable tool.

IQC's global network of auditors allows organisations to work with experienced audit resources; to add value and mitigate the ISMS risks and have an authenticated and credible IAF recognized Information Security Management System certification.

IQC  has the edge and thus provides advantage of using the wide-pool of resources and contacts for delivering cost effective and competent certification services through IQC which is an independent entity for providing accredited, value added, independent and impartial management system certification services.

IQC's group companies include the following,

- IQC Global Engineering LLC (IQC GE), registered in Abu Dhabi and accredited under EIAC for 17020, for offering Third party independent inspection, expedition and project services to oil & gas, power, engineering and industrial projects.
- IQC Global Engineering Private Ltd, registered in Bengaluru, Karnataka – INDIA, for Third party independent inspection, expedition and project QA-QC services to oil & gas, power, engineering and industrial projects.
- Neutrality for Inspection and Testing FAHHS with registered office in Amman, Jordan for offering Inspection, expediting and auditing services.