SiGMA TECHNOLOGY

ISO 27001 Readiness Brief

SiGMA TECHNOLOGY

EXECUTIVE SUMMARY

Introduction to the ISO 27001 Certification

Most businesses hold or have access to valuable or sensitive information. Failure to provide appropriate protection to such information can have serious operational, financial and legal consequences. In some instances, these can lead to a total business failure.

The challenge that most businesses struggle with is how to provide appropriate protection. How do they ensure that they have identified all the risks they are exposed to and how can they manage them in a way that is proportionate, sustainable and cost effective.

ISO 27001 is the internationally recognized standard for Information Security Management Systems (ISMS). It provides a robust framework to protect information that can be adapted to all types and sizes of organization. Organizations that have significant exposure to information-security related risks are increasingly choosing to implement an ISMS that complies with ISO 27001.

The 27000 Family

The 27000 series of standards started life in 1995 as BS 7799 and was written by the UK's Department of Trade and Industry (DTI). The standards correctly go by the title "ISO/IEC" because they are developed and maintained by two international standards bodies: ISO (the International Organization for Standardization) and the IEC (the International Electrotechnical Commission). However, for simplicity, in everyday usage the "IEC" part is often dropped.

There is currently 45 published standards in the ISO 27000 series. Of these , ISO 27001 is the only standard intended for certification. The other standards all provide guidance on the best practice implementation. Some provide guidance on how to develop ISMS for particular industries; other's give guidance on how to implement key information security risk management processes and controls.

The CIA Triad

The information security risk types are commonly referred to as “CIA”. Risks in information security typically arise due to the presence of threats and vulnerabilities to assets that process, store, hold, protect or control access to information which gives rise to incidents. Assets in this context are typically people, equipment, systems or infrastructure.

Information is the data set(s) that an organization wants to protect such as employee records, customer records, financial records, design data, test data, etc. Incidents are unwanted events that result in a loss of confidentiality (e.g., a data breach), integrity (e.g., corruption of data), or availability (e.g., system failure).

THE TYPES OF RISKS THAT SENSITIVE AND VALUABLE INFORMATION ARE SUBJECT TO CAN GENERALLY BE GROUPED INTO THREE CATEGORIES

Confidentiality

Where one or more persons gain unauthorised access to information

Integriity

Where the content of the information is changed so that it is no longer accurate or complete

Avaiilability

Where access to the information in lost or hempered

KEY PRINCIPLES AND TERMINOLOGY

Threats In computer security, a threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.

Risks in information security typically arise due to the presence of threats and vulnerabilities to assets that process, store, hold, protect or control access to information which gives rise to incidents.

Assets in this context are typically people, equipment, systems or infrastructure. Information is the data set(s) that an organization wants to protect such as employee records, customer records, financial records, design data, test data etc.

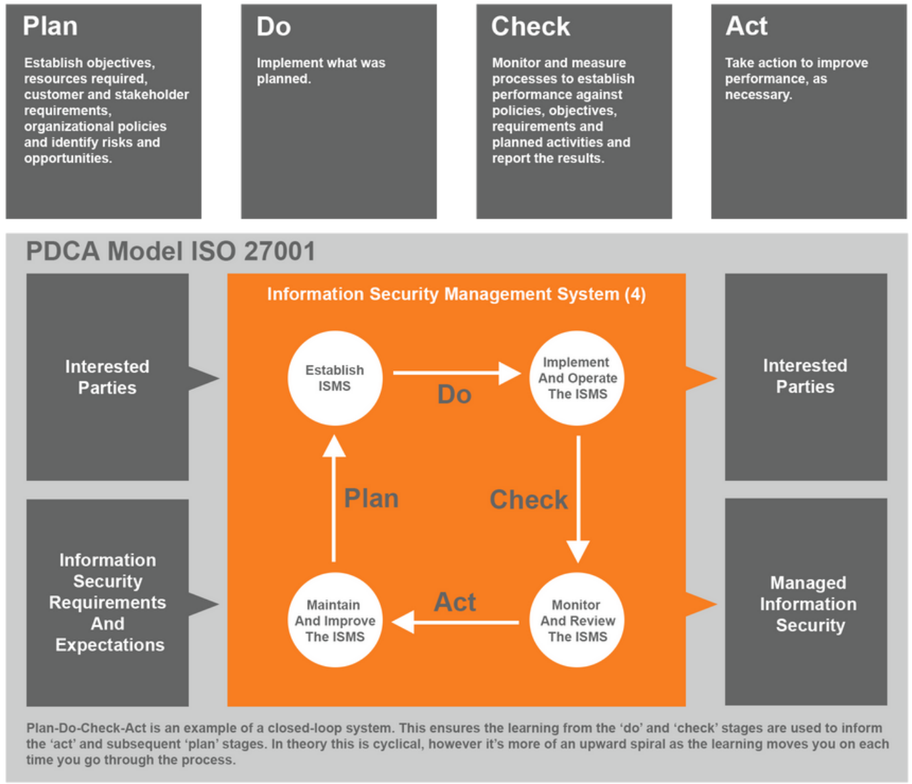
Incidents are unwanted events that result in a loss of confidentiality (e.g., a data breach), integrity (e.g. corruption of data) or availability (e.g., system failure). Threats are what cause incidents to occur and may be malicious (e.g., a burglar), accidental (e.g., a key stroke error) or an act of God (e.g. a flood).

Vulnerabilities such as open office windows, source code errors, or the location of buildings next to rivers, increase the likelihood that the presence of a threat will result in an unwanted and costly incident. In information security, risk is managed through the design, implementation and maintenance of controls such as locked windows, software testing or the siting of vulnerable equipment above ground floor levels.

PDCA CYCLE

ISO 27001 is based on the Plan-Do-Check-Act (PDCA) cycle, also known as the Deming wheel or Shewhart cycle. The PDCA cycle can be applied not only to the management system as a whole, but also to each individual element to provide an ongoing focus on continuous improvement.

ISO audits are a systematic, evidence-based, process approach to evaluation of your Information Security Management System. They are undertaken internally and externally to verify the effectiveness of the ISMS. Audits are a brilliant example of how risk-based thinking is adopted within Information Security Management.



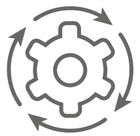
Benefits OF ISO 27001 CERTIFICATION

Information security is becoming increasingly important to organizations, and the adoption of ISO 27001 is therefore more and more common. Most organizations now recognize that it is not a question of if they will be affected by a security breach; it is a question of when.

Implementing an ISMS and achieving certification to ISO 27001 is a significant undertaking for most organizations. However, if done effectively, there are significant benefits for those organizations that are reliant on the protection of valuable or sensitive information. These benefits typically fall into three areas:

Commercial: The most obvious reason to certify to ISO 27001 is that it will help you avoid security threats. This includes both cyber criminals breaking into your organization and data breaches caused by internal actors making mistakes. Having independent third-party endorsement of an ISMS can also provide an organization with a competitive advantage or enable it to 'catch up' with its competitors. Companies can demonstrate to potential clients that you take security seriously and stand out from the competition.

Peace of Mind: Many organizations have information that is mission-critical to their operations, vital to sustaining their competitive advantage or an inherent part of their financial value. Having a robust and effective ISMS in place enables business owners and managers with responsibility for managing risks to sleep easier at night knowing that they are not exposed to a risk of heavy fines, major business disruption or a significant hit to their reputation.



Operational: The holistic approach of ISO 27001 supports the development of an internal culture that is alert to information security risks and has a consistent approach to dealing with them. This consistency of approach leads to controls that are more robust in dealing with threats. The cost of implementing and maintaining them is also minimized, and in the event of them failing the consequences will be minimized and more effectively mitigated.

NEXT STEPS - PRELIMINARY WORK AND GAP ANALYSIS

Determining the scope is the most decisive step in the process of setting up and operating an ISMS, therefore this phase will be carried out with extra diligence.

As a part of ISO 27001 Readiness assessment, Sigma Technology will prepare pre-assessment activities/pre-audit gap analysis to ensure a successful certification endeavor. Purpose of this pre-assessment or audit readiness is to ensure that the required Policies and Procedures, Governance Framework, organization of the Information Security and other required documents and control objectives are in place.

Develop scope of the management system which will describe:

- The boundaries of the physical site or sites included (or not included)
- The boundaries of the physical and logical networks included
- The internal and external employees group included (or not included)
- The internal and external processes, activities or services included
- Key interfaces at the boundaries of the scope

Develop a realistic schedule for the ISO 27001 certification considering the compliance per Domain (ISO Annex A), and internal review of the controls for the expedited certification process.

ISO 27001 Annex A

What are the control changes in ISO 27001:2022 Annex A?

Some Annex A controls have been merged or removed, and some have been added. ISO 27001:2022 lists 93 controls rather than ISO 27001:2013's 114.

These controls are grouped into 4 'themes' rather than 14 clauses. They are:

- People (8 controls)
- Organizational (37 controls)
- Technological (34 controls)
- Physical (14 controls)

The completely new controls are:

- Threat intelligence
- Information security for use of cloud services
- ICT readiness for business continuity
- Physical security monitoring
- Configuration management
- Information deletion
- Data masking
- Data leakage prevention
- Monitoring activities
- Web filtering
- Secure coding

The controls now also have five types of 'attributes' to make them easier to categorize:

- Control type (preventive, detective, corrective)
- Information security properties (confidentiality, integrity, availability)
- Cybersecurity concepts (identify, protect, detect, respond, recover)
- Operational capabilities (governance, asset management, etc.)
- Security domains (governance and ecosystem, protection, defense, resilience)

ISMS Implentation Phase

Activities for ISMS implementation leading to ISO certification

Step 1: Business Case preparation & ISMS setup

1.1 Initial Planning of ISMS Implementation consisting of defining the:

- Business Context
- Needs & expectations of interested parties
- Roles, Responsibilities and authorities
- Governance structure
- Stakeholder Buy-In, commitment, business case & ownership for ISMS
- Resource requirements and competencies needed for ISMS

Step 3: Establish the ISMS Framework

- 2.1 Assist with defining ISMS scope & boundaries
- 2.2 Assistance in defining the ISMS Policy
- 2.3 Support in defining the Risk Management Methodology & performing assessments
- 2.4 Support in risk treatment
- 2.5 Assistance in developing a security awareness program & communication plan

Step 3: implement the ISMS Framework

- 3.1 Provide support with Operational Plan and Risk Assessment
- 3.2 Assistance with implementing the selected controls

Step 4: Maintain & Review ISMS Framework

- 4.1 Assistance with monitoring the selected controls
- 4.2 ISMS Internal Audit roll out
- 4.3 Supporting in conducting Management Review
- 4.4 Providing recommendations for improvements

Step 5: improve the ISMS Framework

- 5.1 Verification of security improvement plans
- 5.2 Corrective and Preventive Actions
- 5.3 Support for updating ISMS framework (if required)

Step 6: ISMS Certification

- 6.1 Support in selection of suitable Certification Body
- 6.2 Support clients during the ISO certification audit

SiGMA TECHNOLOGY

(800)748-6602

info@sigmatechllc.com
https://www.sigmatechllc.com

Sigma Technology Partners LLC
2300 Wilson Blvd, #700 Arlington, VA 22201