

Sri Lanka Institute of Information Technology

**ISO 27001 Implementation for an Organization**

**IE3102-Enterprise Standards for Information Security**

Submitted by:

|  |  |
| --- | --- |
| Student Registration Number | Student Name |
| IT20620066 | Weththasinghe M N G |

Date of Submission

29/10/2022

**Table of Content**

Abstract……………………………………………………………………………………………..3

Introduction……………………………………………………………………………………….4

What is ISMS………………………………………………………………………………………5

How does ISMS work……………………………………………….…………………………5

What is ISO…………………………………………………………………………………………6

What is ISO 27001……………………………………………………………………..……...6

Evolution ISO through time………………………………………………………………..7

How to implement an ISMS with ISO 27001………………………..…..…………9

Cost……………………………………………………………………………………….…………14

Benefits of Certification……………………………………………………………………16

Benefits of ISMS……………………………………………………………………………….18

Conclusion……………………………………………………………………………………….20

References……………………………………………………………………………………….21

**Abstract**

The ISO/IEC 27001 security standard provides guidelines for organizations to define appropriate best practices in information security management, including standards that enable the proper selection and implementation of security measures. This standard enables organizations to secure their information assets and achieve adequate levels of security, allowing them to meet their business objectives. Currently, an increasing number of businesses desire to comply with ISO/IEC 27001:2013 criteria and acquire certification. This article presents the findings of a study conducted to identify the major hurdles and limits encountered by businesses when implementing the ISO/IEC 27001:2013 standard. Furthermore, this paper provides commentary on the results obtained to better understand the evolution and current state of this standard implementation. According to the report, organizations are becoming increasingly concerned about information security issues, particularly in light of recent cybersecurity incidents. Furthermore, certification is recognized as an important tool for instilling trust and demonstrating to all companies' consumers, suppliers, and stakeholders that information security components are validated and structured within the organization.

**Introduction**

International trade, telecommunications services, social media, and the myriad platforms and services that make up our digital world as well as national infrastructures are all impacted by the issue of information security. If information is to be protected against the threats that enterprises and society confront in this digital age, information security management must be efficient, adequate, and appropriate. Information may be lost or inaccessible due to a system failure, corrupted or modified either intentionally or unintentionally, and disclosed and exposed to unauthorized persons. An organization must evaluate its risks in terms of the likely occurrence of a security incident as well as the potential effects it could have on its operations. It needs to adopt a method to risk assessment that would be effective, suitable, and applicable to its business, and this technique is known as ISO implementation.

The ISO 27001 standard raises awareness of information security controls that can be used to evaluate how well a management system is working. Additionally, it offers the chance to pinpoint the ISMS's shortcomings and make improvements. Additionally, it assigns responsibility for information security and meeting customer and other stakeholder needs to the highest management.

**What is ISMS?**

An information security management system, or ISMS, is a set of guidelines and rules that regulate how a corporation handles sensitive data (ISMS). An ISMS seeks to reduce risk and guarantee business continuity by proactively minimizing the impact of a security compromise. Technology, data, processes, and employee behavior are frequently considered by an ISMS. It may be tailored to a specific sort of data, such as customer data, or it may be widely adopted to permeate the corporate culture.

**How does ISMS work?**

An ISMS is a systematic strategy to manage an organization's information security. Information security comprises a set of broad policies that control and manage security risk levels across a business.

The international standard ISO/IEC 27001 governs the development of an ISMS and information security. The standard, which was published jointly by the International Organization for Standardization and the International Electrotechnical Commission, suggests documentation, internal audits, continuous improvement, and corrective and preventive action but does not mandate any particular courses of action. To get ISO 27001 certified, a company needs an ISMS that lists its assets and conducts the following assessments:

**What is ISO?**

The non-governmental International Standards Organization (ISO) occupies a special position between the public and commercial sectors. Its members include national standards bodies that typically serve as a component of or are needed by national governments. The purpose of ISO is to streamline international cooperation and industrial standardization. To achieve these ends, ISO publishes technical standards. These standards aid in the creation, production, and distribution of goods and services that are more efficient, secure, and understandable. They make international trade more equitable. Additionally, they assist in the transfer of technology to underdeveloped nations and provide governments with a technical framework for legislation about health, security, and the environment. Additionally, customers and other users of goods and services are protected via ISO standards.

**What is ISO 27001?**

The international standard ISO 27001 outlines requirements for an information security management system (ISMS). Through a systematic strategy that combines people, procedures, and technology, you can manage and safeguard all of the information within your firm. It is a collection of normative standards for creating, putting into practice, running, checking, and updating an information security management system (ISMS). Based on best practices in the industry, ISO 27001 is also used to choose security measures specific to each organization's requirements.

**Evolution of ISO through time**

**Steps and resources for developing standards**

A standards development track is first assigned to each ISO deliverable. This track sets the project's schedule as it moves through the various stages leading up to publication.

Whichever path is taken, the ISO standard development process is divided into stages. These steps, as well as the primary materials necessary at each level

## **Stages and resources for standards development**

**Proposal stage**

This is the initial step in figuring out whether a new International Standard is indeed needed in the concerned field. Form 4 is used to submit a new work item proposal (NP) to the committee for approval. (For more details, see the Global relevance policy.) The electronic voting system will be used to cast the ballot. The name of the candidate for project leader is listed on the form. At this early stage, any possible problems with copyright, patents, or compliance assessment should be disclosed.

For alterations and additions to already-published ISO standards, this stage can be skipped (as long as the scope does not change)

**Preparatory stage**

A working group (WG) will often be established by the parent committee to create the working draft (WD). The Convenor, along with specialists, make up the Working Group. Professionals are still keeping an eye on copyright, patent, and compliance assessment concerns throughout this phase. Until the experts are confident they have identified the greatest viable answer, further WDs may be distributed. The WG parent committee receives the paper after that and selects which step to move on to (Committee stage or Enquiry stage). The ISO/TC portal may be used to distribute papers at this stage of standards development and later levels as well.

**Committee stage**

The parent committee members are now given access to the working group's draft. The committee draft (CD), if the committee decides to use this step, is given to the committee members, who subsequently provide feedback via the Electronic Balloting Portal. Up till a consensus on the technical content is obtained, the following CDs can be issued. This step can be skipped completely. to learn when it may be skipped.

**Inquiry stage**

The Committee Manager delivers the Draft International Standard (DIS) to the ISO Central Secretariat. All ISO members are then given a copy, and they have 12 weeks to vote on it and comment on it. The DIS is approved if two-thirds of the TC/SC P-members vote in favor and no more than 25% of the total votes cast are against it (the draft should be presented through the submission site). If the DIS is approved and the draft doesn't undergo any technical modifications, the project will be released right away. However, the FDIS method must be performed if technical modifications are made.

**Approval stage**

Even though the DIS stage has been authorized, the FDIS stage is now required if technical modifications are made to the draft as a result of comments received there. The Committee Manager will submit the Final Draft International Standard (FDIS) to ISO/Central Secretariat (ISO/CS) if this stage is used. Following that, the FDIS is made available to all ISO members for an 8-week vote (the Submission Interface should be used to deliver the draft to ISO/CS). The standard is accepted if two-thirds of the P-members of the TC/SC vote in favor and no more than a quarter of the total votes cast are against.

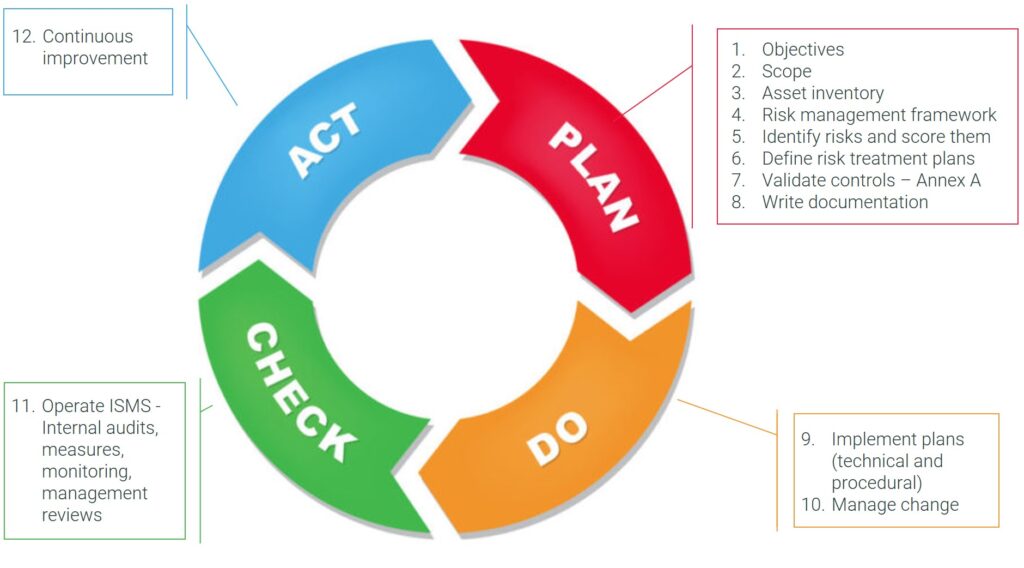
**Publication stage**

The secretary now submits the finished paper for publication using the Submission Interface. The manager may, however, provide the project leader's answer to member body comments on the FDIS if the standard is approved. The only changes made to the text before it is published are editorial ones. The ISO Central Secretariat publishes it as an international standard.

**How to implement an ISMS with ISO 27001**

This article describes the steps involved in putting ISO 27001's Information Security Management System (ISMS) into practice. Any ISMS or standard must have certain papers, such as policies, detailed job instructions, and protocols. Both ISO 27001 and this demand for formal documentation are present. The ISO 27001 system, is a risk management technique used to protect the confidentiality, integrity, and availability of information.

If the company's teams do not include professionals, they may begin by identifying the precise data they wish to protect and comprehending the risks associated with it. further decide how to manage those risks, implement any required technology fixes, and produce the necessary documentation. We created a set of 12 phases based on Deming's Plan-Do-Check-Act paradigm to install an ISMS with ISO 27001. The Information Security Management System (ISMS) implementation process is described in those 12 phases using ISO 27001.

****

#### 

#### **Step 1 – Define objectives**

An ISMS with ISO 27001 requires a lot of work to implement. Make sure everyone understands the goals for the implementation, and ensure there is a champion at the highest level who will support those goals.

#### **Step 2 - Define your scope**

What information specifically are you attempting to safeguard? What data would you prefer to keep private for your clients, shareholders, trustees, or other interested parties? When deciding the scope, it's helpful to start by taking into account all of your business operations.

High-level process maps will show where the data you want to keep secure is kept, where it is located in systems and networks, who is in charge of it, and who has access to it.

**Step 3 – Make an inventory of assets**

It's helpful to achieve this using a process map for the business activities in scope. This is an inventory of the information you wish to protect and the various assets linked with it (such as hardware, software, databases, and physical locations).

**Step 4 - Define your risk management framework**

This standard focuses on controlling the threats to the information's availability, confidentiality, and integrity. Therefore, this is an important component of your implementation. Although the framework isn't specified specifically, you must set up one that incorporates a risk assessment procedure that yields consistent results regardless of who does the evaluation. The framework must also provide choices for risk management that take the findings of the risk assessment into account.

**Step 5 - Identify the risks and score them**

The ISO 27000 series is a "family" of standards, of which ISO 27001 is a member. The section of ISO 27005 offers recommendations for information security risk management. It suggests two methods for determining and rating risks:

1. Scenario-based methodology: risks are identified by considering potential events and evaluated by assessing their impact. In other words, you make an effort to consider every scenario that may go wrong (events) and determine what impact (consequences) this would have on the privacy, accuracy, and accessibility of the information under your purview.
2. Asset-threat-vulnerability approach: risks are found by beginning with an inventory of assets. For each category of the asset (such as laptops, servers, and networks), the threats (theft, human error, malware, etc.), their vulnerabilities (such as a lack of adequate employee security training), and their value to the organization (whether monetary or otherwise) are taken into account and scored accordingly.

Although the scenario-based approach appears easier and more alluring in theory, I've observed that it quickly runs out of steam unless the people conducting the risk assessment are well knowledgeable about information security. I tend to favor the Asset-Threat-Vulnerability model since you frequently "don't know what you don't know!"

#### **Step 6 - Risk treatment plan(s)**

You must choose a course of action for each risk that has been identified. Seven options are provided in the note to the definition of risk treatment in BS EN ISO/IEC 27000:2017:

1. opting not to begin or continue the action that poses the danger to prevent it;
2. assuming or escalating risk to seize an opportunity;
3. taking away the risk source;
4. changing the likelihood;
5. altering the results;
6. spreading the risk (via agreements and risk finance) with another party or parties; and
7. retaining the risk by educated choices.

Except for selections 2 and 7, all the other choices suggest that you should alter the possibility of danger occurring or the seriousness of the repercussions if it does. This is accomplished in both situations using a "control." For instance, you may elect to prevent critical client information from ever being stored on a laptop in the first place to reduce the possibility of losing it. There has to be a mechanism that stops individuals from loading the information or recognizes when it has been transmitted so it can be deleted to prevent people from storing client data on their laptops The controls are those. Generally speaking, the Treatment Plan is comprised of all the controls. However, you might have several treatment plans. Since it serves as the foundation for the activities you choose to take, I like to refer to this as the risk action plan.

#### **Step 7 – Verify the risk treatment plan against the Annex A controls**

To assist make sure that no important controls are omitted in your ISMS, ISO 27001 provides a list of 114 controls, each of which must be reviewed, and their inclusion/exclusion justified. The Statement of Applicability is a list of the items you include or exclude, together with your reasoning.

Where ISO 27001 is both extremely helpful and perhaps detrimental to your project in this set of controls. Without first evaluating their risks and utilizing the findings of this assessment to prioritize their action plan, I have seen organizations begin with this set of controls. As they work their way down the list, they choose the best tools and techniques to put each control in place. They inevitably end up with endless internal arguments, spending far more time and money than they anticipated, and have no clear sense of priorities. Don't start with Annex A if you take anything from this article!

#### **Step 8 - Write documentation**

You will now have a good understanding of your risks and what you must do to manage them. Writing the documentation—that is, the rules and procedures outlining how you will run your ISMS—will be at its most effective at this time.

It should be noted that formal documentation of every operation is not necessary. However, it's desirable to record a procedure if it’s not carried out regularly or if it's complicated and involves numerous phases to reduce human error.

**Step 9 – (at the same time as step 8) – Implement technical risk mitigating solutions**

There's a good chance you'll need to use technical solutions. Technology-based changes are underway, including tightening security groups on your on-premise Active Directory, implementing a Directory-As-A-Service solution, updating the anti-malware software already installed, and adding information classification and data retention capabilities to your document management system.

**Step 10 - Manage the change**

All competent business analysts and change managers will tell you that altering how people work needs to begin from the very beginning of a project, even if this is step 10 in the process. Don't forget that new processes and/or systems will likely require training for the staff. People are impacted by ISO 27001 since it is a business transformation initiative rather than an IT one.

**Step 11 – Operate your ISMS – internal audits, measures, monitoring, and management reviews**

You are now in the "Check" and "Act" sections of the PDCA diagram. By carrying out routine internal audits, measuring (such key performance indicators), and monitoring, you can verify that employees are adhering to risk management policies and procedures and that technology solutions are efficient.

The appropriate individual(s) or group(s) in your governance structure will assess the findings of audits, measurements, and monitoring and decide whether to maintain the current controls or make changes.

**Step 12 - Continuous improvement**

An ISMS is created when Steps 1 through 11 become a cycle of "business as usual"!

Keep in mind that implementing an ISMS is a major corporate project that will undoubtedly change how workers behave. It may evolve into a program with several auxiliary projects. As a result, the typical project success criteria are applicable: senior team support is required, a budget must be agreed upon, resources must be assigned, a senior executive must be identified as the accountable lead, a project manager must be identified, etc. Despite not being an IT project, many of its components are, therefore you might find our essay on IT Project Processes helpful. responsible leader, appointing a project manager, etc. Despite not being an IT project, many of its components rely on IT, therefore you might find our article on IT Project Processes beneficial.

**Cost**

While determining the exact cost of any compliance certification can be difficult, ISO 27001 is particularly varied. To reduce the costs associated with postponing ISO 27001, our experts recommend starting your compliance journey as soon as feasible.

* How many employees work with you?
* Where are companies and employees geographically located?
* What information does the Application collect?
* Is your platform distributed across multiple cloud platforms?

We've created a cost analysis in the post below to help you make budgetary decisions as you work to become ISO 27001 certified.

## **ISO 27001 Design and Implementation Cost**

ISO 27001 implementation can be time-consuming and costly. Workflow automation and coaching from an ISO 27001 specialist are the most important variables. You must scope your ISMS, do a gap analysis to determine the control areas that must be established, then walk through the implementation of those controls.

ISO 27001 will affect the majority of your organization's workers. It will need a few months of committed time from key players. The cost will be determined by the amount of time sunk by salaried staff or the hiring of a compliance team to handle design and execution.

* The following are the average cost ranges for design and implementation:
* Annual salary for a Compliance Manager in the United States is USD 115,000.
* Annual cost of compliance software and tools: $20,000 to $150,000
* Time Frame: 2-3 months

## **Cost of Assessing Risk and Internal Audit**

Before evaluating preparation for an external audit, a company that is becoming ISO 27001 compliant for the first time, such as through a surveillance audit (see below), must undertake an independent internal audit.

The key word here is "independent." Larger organizations may be able to delegate internal auditing to employees who were not involved in implementation. However, you may need to hire a third party to complete this stage. It is important to note that these auditors are not needed to be ISO 27001 certified. The fee will almost certainly be per hour and will be determined by the size and breadth of your ISMS.

**The average ranges for risk assessments and internal audits:**

The formal ISO 27001 audit is typically completed in person, and the duration is determined by the size of your company. A small corporation with five employees and one location may only require a few days of auditing, whereas a larger, multi-site organization may require up to a month.

**The following are the average audit and certification ranges:**

* ISO 27001 Auditor Cost: $5,500 – $18,000
* Time Needed: 3 – 10 days

## **Surveillance Audits Cost**

ISO 27001 cost varies by audit firm (the United States has only 21 audit firms!). Surveillance audits are required in years 2 and 3 following the original formal certification. Surveillance audits can determine whether or not the company is still operating as indicated in the initial certification year. You must keep your ISMS and associated controls up to date to comply. This will necessitate the time of a compliance consultant or salaried employee, in addition to the cost of auditors.

**The following are the average ranges for surveillance audits:**

* Compliance Specialist Salary: $75,000 – $90,000 annually
* Cost of ISO 27001 Audit: $5,500 – $12,000
* Time Needed: 1 – 4 days

We cannot stress this enough: these price ranges are only estimates. The cost of ISO 27001 certification is governed by several factors, including team buy-in, the readiness of your product and engineering teams, the size of your company, and many others.

**Benefits of Certification**

**Quality assurance**

Working with a recognized organization ensures a high level of Information Security excellence. The accreditation adheres to a strict structure and is subject to ongoing quality assessments. These two aspects assist assure an unequaled degree of excellence.

**Avoidance and mitigation of damages**

The reduced risk of security breaches is one of the most important advantages of ISO 27001 certification. Potential losses are mitigated, security breaches are less likely, and potential breakthroughs are tracked down and removed in the early stages with ISO 27001 certification.

**Higher levels of trust**

When it comes to personal data, trust is everything. An ISO 27001 accreditation also serves as a guarantee of confidence. It not only demonstrates that your data is treated with integrity, but it also demonstrates that security procedures and policies are constantly developed and evaluated to further improve data protection.

**The easy way to identify data security**

ISO 27001 accreditation is a method of evaluating a supplier and recognizing those that have high-quality and dependable data security practices. Instead of wasting time looking through bids from possible suppliers just to discover that their data security policy and technical information aren't ISO 27001 certified, you may safely pre-qualify providers. You can bring up ISO 27001 early in the negotiation process, knowing that your time will be well spent on a provider who has earned the ISO 27001 seal of approval.

**Improves security awareness**

Most firms base their relationships on trust and the assumption that individuals have your best interests at heart and will naturally protect your data. The ISO 27001 certification validates that trust by demonstrating that an organization's procedures prioritize security awareness and that data and information security practices are regularly updated.

**Prevents downtime**

When running a business, efficiency is critical, and a proactive data security policy will assist reduce downtime in times of crisis. Any supplier you engage with should have robust Business Continuity (BC) and Disaster Recovery (DR) plans as part of their ISO 27001 certification and ISMS. These plans help to ensure that service delivery continues during a crisis, reducing disturbance and downtime for both personnel and consumers.

**Reduces loopholes in security**

The minimization of potential security gaps is one of the most important ISO 27001 benefits for enterprises. These gaps can be especially difficult to control if your data is shared with multiple third-party providers. Thorough risk assessment and risk management procedures, as well as continuous improvement of data security standards, help to avoid data problems from forming.

**Attracts new business and employees**

### It is vital to demonstrate a commitment to information security to both customers and employees of your company. ISO 27001 certification communicates to customers the importance you place on their data and establishes your firm as respected and trustworthy.

**Reduce human errors**

The Information Commissioner's Office (ICO) of the United Kingdom provides data security incident trends and routinely identifies breaches caused by human error. Working with an ISO 27001 certified data processing vendor means that all of their staff receive regular Information Security Awareness training, limiting the possibility of human mistakes and malicious activity.

**Benefits of ISMS**

**Protects sensitive data**

An ISMS safeguards all forms of proprietary data assets, whether they are paper-based, digitally maintained, or in the cloud. Personal data, intellectual property, financial data, consumer data, and data given to corporations by third parties are examples of these assets.

**Meets regulatory compliance.**

ISMS assists firms in meeting all regulatory compliance and contractual standards, as well as providing a greater understanding of the legalities surrounding information technology. Because breaking the law can result in significant fines, having an ISMS can be especially advantageous for highly regulated businesses with important infrastructures, such as finance or healthcare.

**Provides business continuity.**

When a company invests in an ISMS, it automatically increases its level of defense against attacks. This minimizes the number of security incidents, such as cyber assaults, resulting in fewer disruptions and downtime, both of which are critical considerations in ensuring business continuity.

**Reduces costs.**

An ISMS provides a comprehensive risk assessment of all assets. This enables businesses to prioritize the most vulnerable assets to avoid indiscriminate expenditure on unnecessary defenses and to provide a focused approach to defending them. This systematic strategy, combined with decreased downtime as a result of fewer security incidents, dramatically reduces an organization's overall spending.

**Enhances company culture.**

An ISMS offers a comprehensive approach to security and asset management across the enterprise that is not restricted to IT security. This encourages all employees to be aware of the dangers associated with information assets and to incorporate security best practices into their regular routines.

**Adapts to emerging threats.**

Security risks are always changing. An ISMS assists companies in preparing for and adapting to newer threats and the ever-changing security landscape.

**Conclusion**

For enterprises that want to be taken seriously when it comes to information security management, staying silent is no longer an option. The ISO 27001 standard raises awareness of information security controls that may be used to gauge how well a management system is working. Additionally, it offers the chance to pinpoint the ISMS's shortcomings and make improvements. Additionally, it assigns responsibility for information security and meeting customer and other stakeholder needs to the top management.

**References**

* ISO/IEC Directives Part 1 and Consolidated ISO Supplement, [section 2.3](https://www.iso.org/sites/directives/current/consolidated/index.xhtml#_idTextAnchor141)
* [Form 4 - New work item proposal](https://isotc.iso.org/livelink/livelink/4229242/Form_04_New_work_item_proposal.doc?func=doc.Fetch&nodeid=4229242)
* [Electronic balloting portal](https://isotc.iso.org/livelink/eb3/)
* [Patent policy](https://www.iso.org/iso-standards-and-patents.html)
* [Conformity assessment for standards writers - Do's and don'ts](https://www.iso.org/publication/PUB100303.html)
* [Global relevance policy](https://www.iso.org/governance-of-technical-work.html)
* [ISO TC platform](https://isotc.iso.org/livelink/livelink)
* ISO/IEC Directives Part 1 and Consolidated ISO Supplement, [section 2.4](https://www.iso.org/sites/directives/current/consolidated/index.xhtml#_idTextAnchor150)
* [Patent policy](https://www.iso.org/iso-standards-and-patents.html)
* [Conformity assessment for standards writers - Do's and don'ts](https://www.iso.org/publication/PUB100303.html)
* [How to Write Standards](https://www.iso.org/stages-and-resources-for-standards-development.html)
* [Electronic balloting portal](https://isotc.iso.org/livelink/eb3/)
* [Form – Limit date extension requests](https://isotc.iso.org/livelink/livelink/6637198/Form_-_Limit_date_extension.doc?func=doc.Fetch&nodeid=6637198)
* ISO/IEC Directives Part 1 and Consolidated ISO Supplement, [section 2.5](https://www.iso.org/sites/directives/current/consolidated/index.xhtml#_idTextAnchor160)
* [Submission Interface](https://isotc.iso.org/livelink/si/)
* [Electronic balloting portal](https://isotc.iso.org/livelink/eb3/)
* [Comment collation tool](https://isotc.iso.org/livelink/livelink?func=ll&objId=5156909&objAction=browse&sort=name)
* [Form - Limit date extension](https://isotc.iso.org/livelink/livelink/6637198/Form_-_Limit_date_extension.doc?func=doc.Fetch&nodeid=6637198)
* ISO/IEC Directives Part 1 and Consolidated ISO Supplement, [section 2.6](https://www.iso.org/sites/directives/current/consolidated/index.xhtml#_idTextAnchor172)
* [Submission Interface](https://isotc.iso.org/livelink/si/)
* [Form 13 - Report of voting on ISO/DIS](https://isotc.iso.org/livelink/livelink/4229250/Form_13_Report_of_voting_on_draft_International_Standard.doc?func=doc.Fetch&nodeid=4229250)
* [Electronic balloting portal](https://isotc.iso.org/livelink/eb3/)
* ISO/IEC Directives Part 1 and Consolidated ISO Supplement, [section 2.7](http://www.iso.org/sites/directives/current/consolidated/index.xhtml#_idTextAnchor184)
* ISO/IEC Directives Part 1 and Consolidated ISO Supplement, [section 2.8](https://www.iso.org/sites/directives/current/consolidated/index.xhtml#_idTextAnchor195), [section 2.9](https://www.iso.org/sites/directives/current/consolidated/index.xhtml#_idTextAnchor198) and [section 2.10](https://www.iso.org/sites/directives/current/consolidated/index.xhtml#_idTextAnchor208)
* <https://www.techtarget.com/whatis/definition/information-security-management-system-ISMS>
* <https://heylaika.com/blog/compliance-101/how-much-does-iso-27001-certification-cost/>
* <https://www.isaca.org/resources/isaca-journal/past-issues/2011/2011-planning-for-and-implementing-iso-27001>
* <https://www.infosectrain.com/blog/a-basic-introduction-to-iso-27001/#:~:text=ISO%2027001%20is%20the%20international,organization's%20information%20through%20risk%20management>.
* <https://digitaloctopii.com/blog/what-is-isms/how-to-implement-isms-iso-27001/>
* <https://ieeexplore.ieee.org/document/8710558>