ISO/IEC 27001

- It is a principal international standard focused on information security, published by the International Organization for Standardization (ISO),
- In partnership, with the International Electro technical Commission (IEC). Both are leading international organizations that develop international standards.
- ISO framework is a combination of policies and processes for organizations to use.
- ISO 27001 provides a framework to help an organization of any size or in any industry protect their information systematically and cost-effectively through the adoption of an Information Security Management System (ISMS).

The basic goal of ISO 27001 is to protect three aspects of information:

- **Confidentiality**: only the authorized persons have the right to access information.
- **Integrity**: only the authorized persons can change the information.
- **Availability**: the information must be accessible to authorized persons whenever it is needed.

Why ISO 27001 important?

Not only does the standard provide companies with the necessary know-how for protecting their most valuable information, but a company can also get certified against ISO 27001 and, in this way, prove to its customers and partners that it safeguards their data.

Individuals can also get ISO 27001-certified by attending a course and passing the exam

In this way, prove their skills to potential employers.

Because it is an international standard, ISO 27001 is easily recognized all around the world, increasing business opportunities for organizations and professionals.

Another relevant ISO Sections:

- ISO/IEC 27002:2013, Information technology Security Techniques — Code of practice for information security controls
- ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance.
- SO/IEC 27004, Information technology — Security techniques — Information security management — Measurement
- ISO/IEC 27005, Information technology — Security techniques — Information security risk management
- ISO 31000:2009, Risk management — Principles and guidelines

- ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012

What are the 14 domains of ISO 27001? (Sections A.5 to A.18)

There are 14 “domains” listed in Annex a of ISO 27001, organized in sections A.5 to A.18. The sections cover the following:

1. **A.5. Information security policies**: The controls in this section describe how to handle information security policies.
2. **A.6. Organization of information security**: The controls in this section provide the basic framework for the implementation and operation of information security by defining its internal organization (e.g., roles, responsibilities, etc.), and through the organizational aspects of information security, like project management, use of mobile devices, and teleworking.
3. **A.7. Human resource security**: The controls in this section ensure that people who are under the organization’s control are hired, trained, and managed in a secure way; also, the principles of disciplinary action and terminating the agreements are addressed.
4. **A.8. Asset management**: The controls in this section ensure that information security assets (e.g., information, processing devices, storage devices, etc.) are identified, that responsibilities for their security are designated, and that people know how to handle them according to predefined classification levels.
5. **A.9. Access control**: The controls in this section limit access to information and information assets according to real business needs. The controls are for both physical and logical access.
6. **A.10. Cryptography**: The controls in this section provide the basis for proper use of encryption solutions to protect the confidentiality, authenticity, and/or integrity of information.
7. **A.11. Physical and environmental security**: The controls in this section prevent unauthorized access to physical areas, and protect equipment and facilities from being compromised by human or natural intervention.
8. **A.12. Operations security**: The controls in this section ensure that the IT systems, including operating systems and software, are secure and protected against data loss. Additionally, controls in this section require the means to record events and generate evidence, periodic verification of vulnerabilities, and make precautions to prevent audit activities from affecting operations.
9. **A.13. Communications security**: The controls in this section protect the network infrastructure and services, as well as the information that travels through them.
10. **A.14. System acquisition, development and maintenance**: The controls in this section ensure that information security is taken into account when purchasing new information systems or upgrading the existing ones.
11. **A.15. Supplier relationships**: The controls in this section ensure that outsourced activities performed by suppliers and partners also use appropriate information security controls, and they describe how to monitor third-party security performance.

12. **A.16. Information security incident management**: The controls in this section provide a framework to ensure the proper communication and handling of security events and incidents, so that they can be resolved in a timely manner; they also define how to preserve evidence, as well as how to learn from incidents to prevent their recurrence.
13. **A.17. Information security aspects of business continuity management**: The controls in this section ensure the continuity of information security management during disruptions, and the availability of information systems.
14. **A.18. Compliance**: The controls in this section provide a framework to prevent legal, statutory, regulatory, and contractual breaches, and audit whether information security is implemented and is effective according to the defined policies, procedures, and requirements of the ISO 27001 standard.

HIPAPA

HIPAA (Health Insurance Portability and Accountability Act) is United States legislation that provides data privacy and security provisions for safeguarding medical information.

The law emerged in importance in recent years with the many health data breaches caused by cyberattacks and ransomware attacks on health insurers and providers.

Purpose of HIPAA

HIPAA has two purposes:

To provide continuous health insurance coverage for workers,

1. Who lose or change their job and eventually reduce the cost of healthcare by standardizing the electronic transmission of administrative and financial transactions.
2. Other goals include combating abuse, fraud, and waste in health insurance and healthcare delivery and improving access to long-term care services and health insurance.

The Seven Elements of an Effective Compliance Program are as follows:

1. Implementing written policies, procedures, and standards of conduct.
2. Designating a compliance officer and compliance committee.
3. Conducting effective training and education.
4. Developing effective lines of communication.
5. Conducting internal monitoring and auditing.
6. Enforcing standards through well-publicized disciplinary guidelines.
7. Responding promptly to detected offenses and undertaking corrective action.

HIPAA compliance checklist:

1. Determine which of the required annual audits and assessments are applicable to your organization.

2. Conduct the required audits and assessments, analyse the results, and document any deficiencies.
3. Document your remediation plans, put the plans into action, review annually, and update as necessary.
4. If the organization has not already done so, appoint a HIPAA Compliance, Privacy and/or Security Officer.
5. Ensure the designated HIPAA Compliance Officer conducts annual HIPAA training for all members of staff.
6. Ensure HIPAA training and staff member attestation of HIPAA policies and procedures is documented.
7. Perform due diligence on Business Associates to assess HIPAA compliance and annually review BAAs.
8. Review processes for staff members to report breaches and how breaches are notified to HHS OCR.

GDPR

What does GDPR stand for?

GDPR stands for General Data Protection Regulation. It's the core of Europe's digital privacy legislation.

Those paradigm-shifting components include:

- The Data Protection Officer (DPO) order
- A broader-than-ever-before view on individual rights
- An actually clear opt-in requirement
- A breach disclosure mandate

To support these new responsibilities, most enterprises will have to automate their privacy rights management processes.

Below are some of the most important ones that we refer to in this article:

Personal data — Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data.
Data processing — any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing… so basically anything.
Data subject — the person whose data is processed. These are your customers or site visitors.
Data controller — the person who decides why and how personal data will be processed. If you’re an owner or employee in your organization who handles data, this is you.

Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations.

6 Steps to GDPR compliance

To prepare for GDPR, organizations can use this six-step process:

1. Understand the law: Know your obligations under GDPR as it relates to collecting, processing, and storing data, including the legislation's many special categories.
2. Create a roadmap: Perform data discovery and document everything — research, findings, decisions, actions and the risks to data.
3. Know which data is regulated: First, determine if data falls under a GDPR special category. Then, classify who has access to different types of data, who shares the data, and what applications process that data.\
4. Begin with critical data and procedures: Assess the risks to all private data, and review policies and procedures. Apply security measures to production data containing core assets, and then extend those measures to back-ups and other repositories.
5. Assess and document other risks: Investigate any other risks to data not included in previous assessments.
6. Revise and repeat: Repeat steps four to six, and adjust findings where necessary.

Implementing your Security Control

Types of security controls:

There are several types of security controls that can be implemented to protect hardware, software, networks, and data from actions and events that could cause loss or damage. For example:

- **Physical security controls** include such things as data centre perimeter fencing, locks, guards, access control cards, biometric access control systems, surveillance cameras, and intrusion detection sensors.
- **Digital (operations) security controls** include such things as usernames and passwords, two-factor authentication, antivirus software, and firewalls.
- **Cybersecurity controls** include anything specifically designed to prevent attacks on data, including DDoS mitigation, and intrusion prevention systems.
- **Cloud security controls** include measures you take in cooperation with a cloud services provider to ensure the necessary protection for data and workloads. If your organization runs workloads on the cloud, you must meet their corporate or business policy security requirements and industry regulations.

A well-developed framework ensures that an organization does the following:

- Enforces IT security policies through security controls
- Educates employees and users about security guidelines
- Meets industry and compliance regulations
- Achieves operational efficiency across security controls
- Continually assesses risks and addresses them through security controls

A security solution is only as strong as its weakest link. You should, therefore, consider multiple layers of security controls (which is also known as a defence-in-depth strategy) to implement security controls across identity and access management, data, applications, network or server infrastructure, physical security, and security intelligence.

Additional Types of security controls:

Physical security controls include such things as **data centre perimeter fencing, locks, guards, access control cards, biometric access control systems, surveillance cameras, and intrusion detection sensors**.