An Introduction to Security Management

Information security covers all aspects and practices designed to keep organisations data secure and protects their sensitive information, including policies and procedures to prevent unauthorised parties from accessing company information.

Constantly evolving daily, it covers a range of topics, covering the protection of information assets following the concepts of confidentiality, integrity, and availability.

Confidentiality: Ensuring that information can only be authorised persons.
Integrity: Ensuring that information is protected against tampering and corruption.
Availability: Ensuring information is always available and can be restored if problems occur.

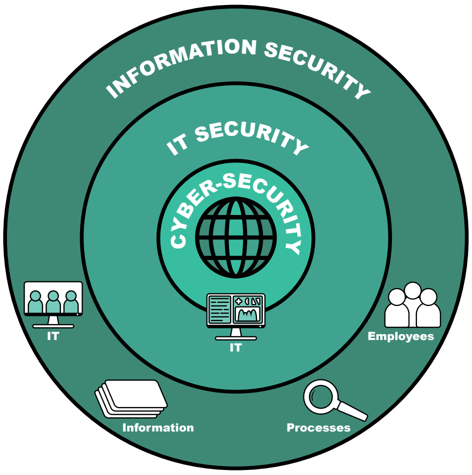
Information security focuses on protecting company assets, as businesses and the market grows it becomes more detrimental and challenging for businesses. Therefore, information security plays a vital role across all industries. With more emphasis on digital and software-driven companies.
Surprisingly, there is no legally binding framework for companies to adopt, there are however still many international standards and norms that define the requirements for security management.
Information assets include all data, information, and goods that represent added value to organisational operations of businesses, within that, it is vital to achieving business objectives.

- Devices, clouds, and other components of IT environments that process information.
- Applications, general support systems, staff, and equipment.
- Hardware, Software, data, databases, processes, and applications within an information system.

Information Security vs Cyber Security vs IT Security

IT Security is coined as the prevention and protection of data and systems from unauthorized parties. IT security refers to the IT infrastructure: everything from computers, servers, clouds, and even wiring and the like must be secure and protected from access by unauthorised persons.

An information technology system (IT system) is generally an information system, a communications system, or, more specifically speaking, a computer system — including all hardware, software, and peripheral equipment — operated by a limited group of IT users.



Cybersecurity should be understood as a branch of IT security. It’s core function is to protect the devices we all use (smartphones, laptops, tablets, and computers), and the services we access - both online, remotely, and at work - from theft or damage. It's also about preventing unauthorized access to the vast amounts of personal information we store on these devices, and online.

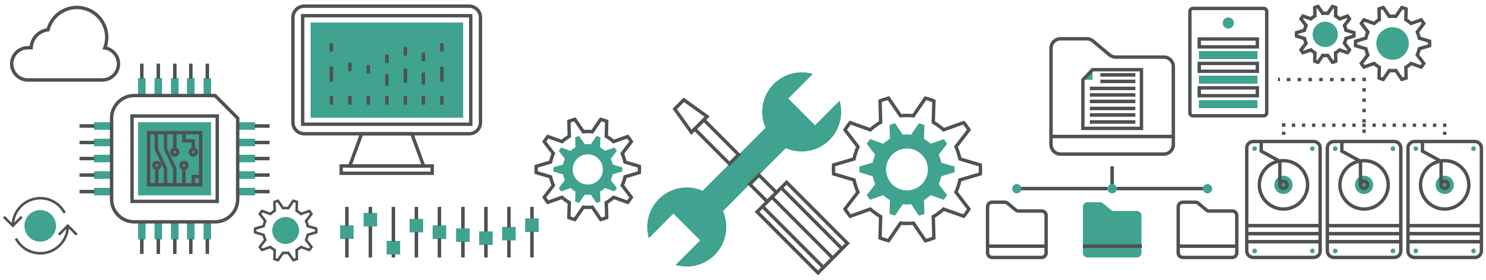
Information security has gained importance in recent years, numerous laws that directly deal with information security were implemented or updated.

Arguably to the evolution of digitisation and fast pace of technological progress. There is an abundance of risks associated as businesses follow suit in digitising organisations and processes.

More businesses adopting an online approach, an awareness growth for consumers, B2B, B2C, and stakeholders. Intensive due diligence processes taking place puts organisations information security under scrutiny and a microscope.

Certifications such as ISO 27001 are playing an increasingly crucial role in the competition for distributors and customers. With an emphasis on marketing and messages surrounding certification at the forefront.

It is vital that every company understands and considers information, IT, and Cyber security seriously, regardless of industry and size.



Objectives of Information Security

The three objectives of information security are:

- Confidentiality
- Integrity
- Availability

When a company implements protective measures for information security, it should always follow at least one of these objectives.

Confidentiality: is the practice of keeping information safe and private, if you don't want someone to know, it is important to keep it that way. Information must be protected from unauthorized access by third parties. It is important to highlight exactly who is authorised to prevent any valuable information from being accessed.

Measures that seek to protect the confidentiality of information include:

- Encryption of data
- User access control
- Physical and environmental security
- Operational security
- Communications security

Integrity: In terms of information security, integrity means that data/information is protected from being changed (either unintentionally or by unauthorised parties), thus being 'reliable'. Integrity primarily means protection against unintentional changes that may likely occur due to defective systems.

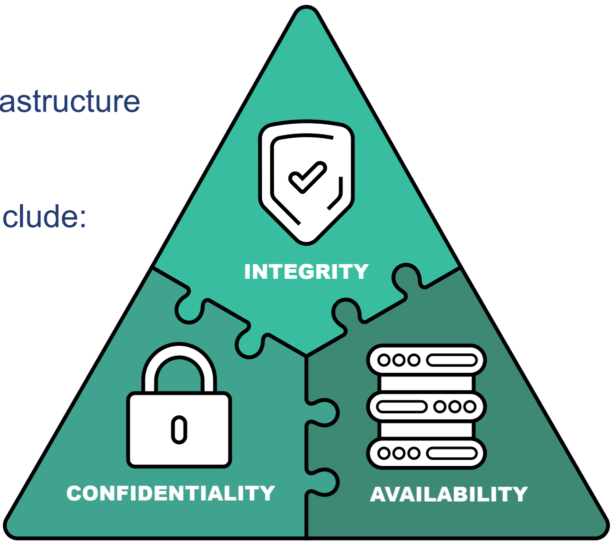
Measures that ascertain integrity include:

- Asset Management
- User control
- System acquisition, development, and maintenance

Availability: Availability means building the technological infrastructure that makes data and information available.

Measures that seek to protect the availability of information include:

- Risk analysis
- System acquisition, development, and maintenance
- Incident management
- Business continuity management


INTEGRITY
CONFIDENTIALITY
AVAILABILITY