Module 6

Standards for Information Security Management

Information Security Management Systems (ISMS) - ISO 27001 - Framing Security Policy of Organization- Committees- Security Forum, Core Committee, Custodian and Users, Business Continuity Process Team & Procedure- Information Security Auditing Process. IT Security Incidents

Information Security Management Systems (ISMS)

- An **Information Security Management System** describes and demonstrates the **organization's approach to information security and privacy.**
- It will help to **identify and address the threats** and **opportunities** around your valuable information and any related assets.
- That **protects the organization from security breaches** and shields it from disruption if and when they do happen.
- **An effective ISMS will also:**
  - **Help** you win **new business and enter new sectors**
  - **Strengthen your relationship** with your existing customers
  - **Build your organization's brand and reputation**
- **What does an ISMS do?**
- Safeguards your organisation’s information assets
- Makes it easy to show any interested party:
  - How secure those information assets are
  - How seriously your organization takes infosec
- Constantly evolves to keep up with:
  - New infosec risks and opportunities
  - Your organisation’s development and growth

- **What is needed to implement your ISMS?**
  - ISMS implementation resource
  - Systems and tools for implementation and ongoing management
  - Actionable policies and controls that will work in practice
  - Staff communications and engagement mechanisms
  - Systems and tools for supply chain management
  - Certification activity and working with external auditors
  - Ongoing ISMS operation and improvement resource
- **Safeguarding your customers**
  - No people system, policies or technology to support information or cyber security management
  - Minimum time spent on security related policies but not structured as a system or following any standards
  - Meeting the requirements for basic information security management e.g with Cyber Essentials
  - Investing in people, policies, processes & systems to show compliance with ISO 27001 & have an ISMS
  - Achieve & maintain an independently certified ISMS that follows ISO 27001, underpinned with a sustainable technology solution

What is an ISMS?

- An Information Security Management System (ISMS) is a set of rules that a company needs to establish in order to:

1. **identify stakeholders** and their expectations of the company in terms of information security

2. **identify which risks** exist for the information

3. **define controls** (safeguards) and other mitigation methods to meet the identified expectations and handle risks

4. **set clear objectives** on what needs to be achieved with information security

5. **implement all the controls** and other risk treatment methods

6. **continuously measure** if the implemented controls perform as expected

7. **make continuous improvement** to make the whole ISMS work better

- This set of rules can be written down in the form of policies, procedures, and other types of documents, or it can be in the form of established processes and technologies that are not documented.

- **ISO 27001** defines which documents are required, i.e., which must exist at a minimum.

- **Why do we need ISMS?**

- There are four essential business benefits that a company can achieve with the implementation of this information security standard:

- **Comply with legal requirements** – there is an ever-increasing number of laws, regulations, and contractual requirements related to information security, and the good news is that most of them can be resolved by implementing ISO 27001 – this standard gives you the perfect methodology to comply with them all.

- **Achieve competitive advantage** – if your company gets certified and your competitors do not, you may have an advantage over them in the eyes of those customers who are sensitive about keeping their information safe.

- **Lower costs** – the main philosophy of ISO 27001 is to prevent security incidents from happening – and every incident, large or small, costs money. Therefore, by preventing them, your company will save quite a lot of money. And the best thing of all – investment in ISO 27001 is far smaller than the cost savings you'll achieve.

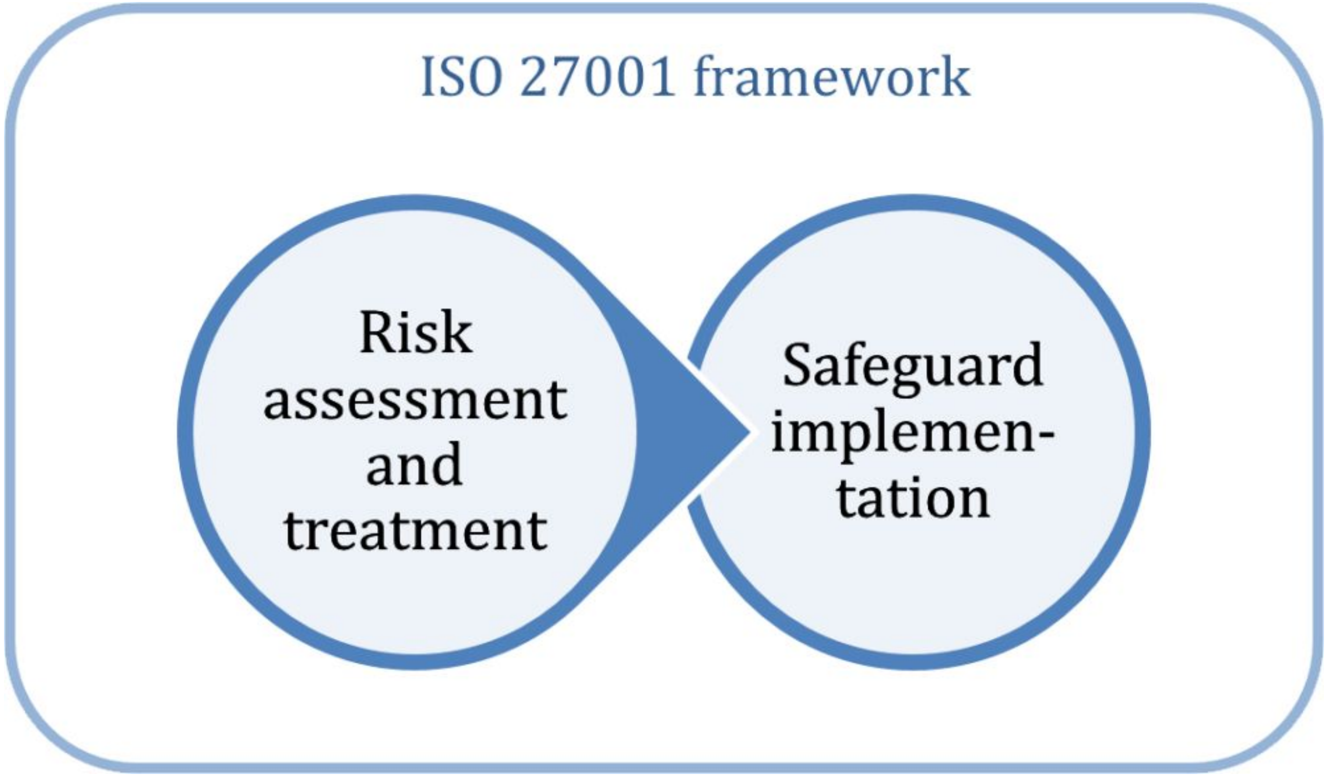
- **Better organization** – typically, fast-growing companies don't have the time to stop and define their processes and procedures – as a consequence, very often the employees do not know what needs to be done, when, and by whom. Implementation of ISO 27001 helps resolve such situations, because it encourages companies to write down their main processes (even those that are not security-related), enabling them to reduce lost time by their employees.

ISO 27001

- The full name of ISO 27001 is **"ISO/IEC 27001 – Information technology — Security techniques — Information security management systems — Requirements**."
- It is the leading international standard focused on information security, published by the **International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC).** Both are leading international organizations that develop international standards.
- ISO-27001 is part of a set of standards developed to handle **information security**: the ISO/IEC 27000 series.
- ISO 27001 provides a framework to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS).
- **What are the 3 ISMS security objectives?**
  - 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.
- ISO 27001 requires a company to list all controls that are to be implemented in a document called the Statement of Applicability.

How does ISO 27001 work?

- The focus of ISO 27001 is to protect the confidentiality, integrity, and availability of the information in a company. This is done by finding out what potential problems could happen to the information (i.e., risk assessment), and then defining what needs to be done to prevent such problems from happening (i.e., risk mitigation or risk treatment).
- Therefore, the main philosophy of ISO 27001 is based on a process for managing risks: find out where the risks are, and then systematically treat them, through the implementation of security controls (or safeguards).



- **Two parts of the standard**
- The standard is separated into two parts.

- The **first, main part** consists of **11 clauses (0 to 10).**

- **The second part, called Annex A**, provides a guideline for **114 control objectives and controls. Clauses 0 to 3 (Introduction, Scope, Normative references, Terms and definitions)** set the **introduction of the ISO 27001 standard**. The following **clauses 4 to 10**, which provide **ISO 27001 requirements** that are mandatory if the company wants to be compliant with the standard, are examined in more detail further in this article.

- **Annex A of the standard supports the clauses and their requirements** with a list of controls that are not mandatory, but that are selected **as part of the risk management process**.

Requirements for ISO 27001

- The requirements are summarized as follows:
- **Context of the organization** – One prerequisite of implementing an Information Security Management System successfully is understanding the context of the organization. External and internal issues, as well as interested parties, need to be identified and considered. Requirements may include regulatory issues, but they may also go far beyond.
- **Leadership** – The requirements of ISO 27001 for an adequate leadership are manifold. The commitment of the top management is mandatory for a management system. Objectives need to be established according to the strategic objectives of an organization. Providing resources needed for the ISMS, as well as supporting persons to contribute to the ISMS, are other examples of the obligations to meet.
- Furthermore, the top management needs to establish a policy according to the information security. This policy should be documented, as well as communicated within the organization and to interested parties.
  Roles and responsibilities need to be assigned, too, in order to meet the requirements of the ISO 27001 standard and to report on the performance of the ISMS.
- **Planning** – Planning in an ISMS environment should always take into account risks and opportunities. An information security risk assessment provides a sound foundation to rely on. Accordingly, information security objectives should be based on the risk assessment. These objectives need to be aligned to the company`s overall objectives. Moreover, the objectives need to be promoted within the company. They provide the security goals to work towards for everyone within and aligned with the company. From the risk assessment and the security objectives, a risk treatment plan is derived, based on controls as listed in Annex A.
- **Support** – Resources, competence of employees, awareness, and communication are key issues of supporting the cause. Another requirement is documenting information according to ISO 27001. Information needs to be documented, created, and updated, as well as being controlled. A suitable set of documentation needs to be maintained in order to support the success of the ISMS.

- **Operation** – Processes are mandatory to implement information security. These processes need to be planned, implemented, and controlled. Risk assessment and treatment – which needs to be on top management`s mind, as we learned earlier – has to be put into action.
- **Performance evaluation** – The requirements of the ISO 27001 standard expect monitoring, measurement, analysis, and evaluation of the Information Security Management System. Not only should the department itself check on its work – in addition, internal audits need to be conducted. At set intervals, the top management needs to review the organization`s ISMS.
- **Improvement** – Improvement follows up on the evaluation. Nonconformities needs to be addressed by taking action and eliminating the causes when applicable. Moreover, a continual improvement process should be implemented, even though the PDCA (Plan-Do-Check-Act) cycle is no longer mandatory

The 14 domains of ISO 27001

- **Information security policies**: The controls in this section describe how to handle information security policies.
- **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.
- **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.
- **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.
- **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.
- **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.
- **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.

- **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.
- **Communications security**: The controls in this section protect the network infrastructure and services, as well as the information that travels through them.
- **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.
- **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.
- **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.
- **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.
- **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.

ISO 27001 controls

- The ISO 27001 controls (also known as safeguards) are the practices to be implemented to reduce risks to acceptable levels. Controls can be technical, organizational, legal, physical, human, etc.
- **How do you implement ISO 27001 controls?**
  - **Technical controls** are primarily implemented in information systems, using software, hardware, and firmware components added to the system. E.g. backup, antivirus software, etc.
  - **Organizational controls** are implemented by defining rules to be followed, and expected behavior from users, equipment, software, and systems. E.g. Access Control Policy, BYOD Policy, etc.
  - **Legal controls** are implemented by ensuring that rules and expected behaviors follow and enforce the laws, regulations, contracts, and other similar legal instruments that the organization must comply with. E.g. NDA (non-disclosure agreement), SLA (service level agreement), etc.
  - **Physical controls** are primarily implemented by using equipment or devices that have a physical interaction with people and objects. E.g. CCTV cameras, alarm systems, locks, etc.
  - **Human resource controls** are implemented by providing knowledge, education, skills, or experience to persons to enable them to perform their activities in a secure way. E.g. security awareness training, ISO 27001 internal auditor training, etc.

Documents associated with ISO27001

- ISO 27001 specifies a minimum set of policies, procedures, plans, records, and other documented information that are needed to become compliant.
- **ISO 27001 requires the following documents to be written**:
- Scope of the ISMS (clause 4.3)
- Information Security Policy and Objectives (clauses 5.2 and 6.2)
- Risk Assessment and Risk Treatment Methodology (clause 6.1.2)
- Statement of Applicability (clause 6.1.3 d)
- Risk Treatment Plan (clauses 6.1.3 e and 6.2)
- Risk Assessment Report (clause 8.2)
- Definition of security roles and responsibilities (controls A.7.1.2 and A.13.2.4)
- Inventory of Assets (control A.8.1.1)
- Acceptable Use of Assets (control A.8.1.3)
- Access Control Policy (control A.9.1.1)

- Operating Procedures for IT Management (control A.12.1.1)
- Secure System Engineering Principles (control A.14.2.5)
- Supplier Security Policy (control A.15.1.1)
- Incident Management Procedure (control A.16.1.5)
- Business Continuity Procedures (control A.17.1.2)
- Statutory, Regulatory, and Contractual Requirements (control A.18.1.1)
- And these are the mandatory records:
- Records of training, skills, experience and qualifications (clause 7.2)
- Monitoring and measurement results (clause 9.1)
- Internal Audit Program (clause 9.2)
- Results of internal audits (clause 9.2)
- Results of the management review (clause 9.3)
- Results of corrective actions (clause 10.1)
- Logs of user activities, exceptions, and security events (controls A.12.4.1 and A.12.4.3)

ISO 27001 certified

- A company can go for ISO 27001 certification by inviting an accredited certification body to perform the certification audit and, if the audit is successful, to issue the ISO 27001 certificate to the company. This certificate will mean that the company is fully compliant with the ISO 27001 standard.
- An individual can go for ISO 27001 certification by going through ISO 27001 training and passing the exam. This certificate will mean that this person has acquired the appropriate skills during the course.

ISO 27000 standards

- Because it defines the requirements for an ISMS, ISO 27001 is the main standard in the ISO 27000 family of standards. But, because it mainly defines what is needed, but does not specify how to do it, several other information security standards have been developed to provide additional guidance. Currently, there are more than 40 standards in the ISO27k series, and the most commonly used ones are as follows:
- **ISO/IEC 27000** provides terms and definitions used in the ISO 27k series of standards.
- **ISO/IEC 27002** provides guidelines for the implementation of controls listed in ISO 27001 Annex A. It can be quite useful, because it provides details on how to implement these controls.
- **ISO/IEC 27004** provides guidelines for the measurement of information security – it fits well with ISO 27001, because it explains how to determine whether the ISMS has achieved its objectives.
- **ISO/IEC 27005** provides guidelines for information security risk management. It is a very good supplement to ISO 27001, because it gives details on how to perform risk assessment and risk treatment, probably the most difficult stage in the implementation.
- **ISO/IEC 27017** provides guidelines for information security in cloud environments.
- **ISO/IEC 27018** provides guidelines for the protection of privacy in cloud environments.
- **ISO/IEC 27031** provides guidelines on what to consider when developing business continuity for Information and Communication Technologies (ICT). This standard is a great link between information security and business continuity practices.

Current version of ISO 27001

- As of the publication date of this article, the current version of ISO 27001 is ISO/IEC 27001:2013.
- The first version of ISO 27001 was released in 2005 (ISO/IEC 27001:2005), the second version in 2013, and the standard was last reviewed in 2019, when the 2013 version was confirmed (i.e., no changes were needed).

Reference:

What is ISO 27001? A beginner’s guide. (advisera.com)

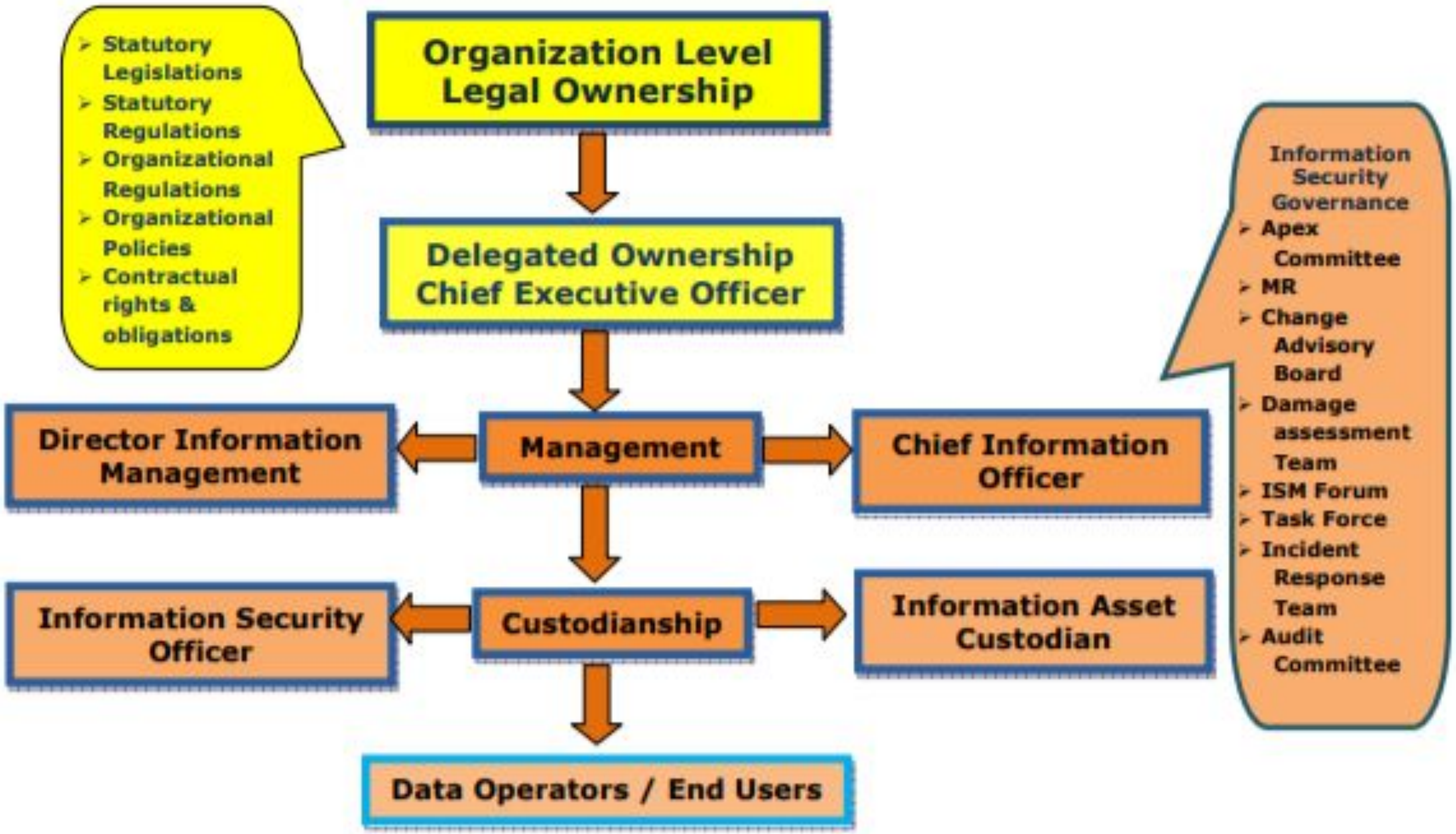
Standards for Information Security Management

Framing Security Policy of Organization - Committees - Security Forum, Core Committee, Custodian and Users

Roles & Responsibilities in Information Asset Management

- All information assets shall be managed at organization level. The ownership of the information assets shall reside with the organization and individuals shall be assigned and made responsible and accountable for the information assets.
- Specific Individuals shall be assigned with the ownership / custodianship / operational usage and support rights of the information assets.

Information Asset Management Roles



- Statutory Legislations
- Statutory Regulations
- Organizational Regulations
- Organizational Policies
- Contractual rights & obligations

Organization Level Legal Ownership

Delegated Ownership Chief Executive Officer

Director Information Management

Management

Chief Information Officer

Information Security Officer

Custodianship

Information Asset Custodian

Data Operators / End Users

Information Security Governance

- Apex Committee
- MR
- Change Advisory Board
- Damage assessment Team
- ISM Forum
- Task Force
- Incident Response Team
- Audit Committee

Information Asset Management Responsibilities

1. **Legal Owner**

   The top management shall be legal owner of information asset. No individual can claim IP rights of an Information asset, unless and otherwise specifically agreed and approved by the management in contractual agreement.

2. **Delegated Ownership**

   The CEO shall have authority to represent the organization for the protection and security of the information asset as ownership of Information assets is delegated to this organizational role. CEO shall approve the Information Management / Security Policy. The CEO may delegate full / partial ownership along with the defined responsibilities to any officer / contractor / third party with operational rights and responsibility.

- The responsibilities of the Asset owner are as follows:

✔ Updating of information asset inventory register;

✔ Identifying the classification level of information asset;

✔ Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset;

✔ Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance;

✔ Authorizing access to those who have a business need for the information, and

✔ Ensuring access is removed from those who no longer have a business need for the information.

3. Director Information Management

- The Director, Information Management ensures that the information resources of organization are managed as a corporate asset and assists in establishing the strategic direction of information management for the organization. They provide support and leadership to officers and other directors responsible for managing information resources on a day-to-day basis.
- The Director, Information Management shall
  - ✔ provide specialist advice relating to information management practices
  - ✔ contribute to the strategic direction of information management within the organization
  - ✔ co-ordinate the development and implementation of information management practices including policies, standards, guidelines and procedures
  - ✔ assist business units to define and understand their responsibilities in relation to information management
  - ✔ assist business units to identify their information needs and requirements
  - ✔ work with the Chief Information Officer to plan and implement systems to effectively manage the agency's information assets.

4. Chief Information Officer

The CIO ensures that strategic planning processes are undertaken so that information requirements and supporting systems and infrastructure are aligned to legislative requirements and strategic goals. The CIO ensures that information security policies and governance practices are established to ensure the quality and integrity of the agency's information resources and supporting IT systems. They oversee the development of tools, systems and information technology infrastructure to maximise the access and use of an agency's information resources.

The Chief Information Officer is responsible for:

- ✔ interpreting the business and information needs and wants of the organization and translating them into ICT initiatives
- ✔ setting the strategic direction for information and communications technology and information management
- ✔ ensuring that ICT and information management investment is aligned to the strategic goals of the organization
- ✔ ensuring that projects and initiatives are aligned and coordinated to deliver the best value
- ✔ ensuring ICT planning is integrated into business planning
- ✔ identifying opportunities for information sharing and cross collaboration on projects and initiatives.

5. Information Security Officer

The information security officer is responsible for developing and implementing information security policy designed to protect information and any supporting information systems from any unauthorised access, use, disclosure, corruption or destruction.

The information security officer shall:

- ✔ Develop policies, procedures and standards to ensure the security, confidentiality and privacy of information that is consistent with organizational Information security policy
- ✔ Monitor and report on any information intrusion incidents and activate strategies to prevent further incidents.
- ✔ Work with information custodians to ensure that information assets have been assigned appropriate security classifications.
- ✔ Maintenance and upkeep of the asset as defined by the asset owner
- ✔ System Restart and recovery
- ✔ Implementing any changes as per the change management procedure
- ✔ Backup of the information
- ✔ Updating of information asset inventory register;
- ✔ Identifying the classification level of information asset;
- ✔ Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset;
- ✔ Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance;
- ✔ Authorizing access to those who have a business need for the information, and
- ✔ Ensuring access is removed from those who no longer have a business need for the information.

6. Data Operators / End Users

- Employees, Third Parties, Contractors authorized by the Owner / custodian to access information and use the safeguards established by the Owner / custodian.
- Being granted access to information does not imply or confer authority to grant other users access to that information. The users are bound by the acceptable usage policy of the organization.

Business Continuity Process Team and Procedure

Contents

- What Is Business Continuity Planning (BCP)?
- Key features
- Understanding Business Continuity Planning (BCP)
- Developing a Business Continuity Plan
- Business Continuity Impact Analysis
- Top Threats to Business Continuity
- 4 Characteristics Guiding Continuity Planning
- Benefits of Business Continuity Planning

What Is Business Continuity Planning (BCP)?

- Business continuity planning (BCP) is the **process involved in creating a system of prevention and recovery from potential threats to a company**.
- The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster.

Key Features

- Business continuity planning (BCP) is the process a company undergoes to create a prevention and recovery system from potential threats such as natural disasters or cyber-attacks.
- BCP is designed to protect personnel and assets and make sure they can function quickly when disaster strikes.
- BCPs should be tested to ensure there are no weaknesses, which can be identified and corrected.

Understanding Business Continuity Planning (BCP)

- BCP involves defining any and all risks that can affect the company's operations, making it an important part of the organization's risk management strategy. Risks may include natural disasters—fire, flood, or weather-related events—and cyber-attacks. Once **the risks are identified, the plan should also include:**
  - Determining how those risks will affect operations
  - Implementing safeguards and procedures to mitigate the risks
  - Testing procedures to ensure they work
  - Reviewing the process to make sure that it is up to date

Developing a Business Continuity Plan

There are several steps many companies must follow to develop a solid BCP. They include:

- **Business Impact Analysis**: Here, the business will identify functions and related resources that are time-sensitive. (More on this below.)
- **Recovery**: In this portion, the business must identify and implement steps to recover critical business functions.
- **Organization**: A continuity team must be created. This team will devise a plan to manage the disruption.
- **Training**: The continuity team must be trained and tested. Members of the team should also complete exercises that go over the plan and strategies.

Business Continuity Impact Analysis

- An important part of developing a BCP is a business continuity impact analysis. It identifies the effects of disruption of business functions and processes. It also uses the information to make decisions about recovery priorities and strategies.
  - The impacts—both financial and operational—that stem from the loss of individual business functions and process
  - Identifying when the loss of a function or process would result in the identified business impacts

Top Threats to Business Continuity

- Depending on your particular business and level of risk, every brand will have different primary threats to business as usual. That’s why risk assessments prior to assembling a business continuity plan can be so helpful.
- While you’ll need to have a plan in place for every possible outcome, the following threats are the most common business disruptors to watch.
    1. Global pandemics.
    2. Natural disasters
    3. Utility outages
    4. Cybersecurity

1. Global pandemics

- Pandemics can throw a wrench in your business plans from all angles and directions. With citizens forced to stay home and do as much work from there as possible, to increased demand for certain items, and decreased supply due to manufacturer shut-downs or disruptions across the supply chain.
- One of the most important plans to put in place if you fear a global pandemic is how your people will communicate with each other and conduct necessary business offsite. It's also important to have options when it comes to supply in case your supply chain is disrupted.

2. Natural disasters

- A natural disaster refers to anything weather related — tornados, hurricanes, tsunamis, etc. — or other natural phenomena like earthquakes, wildfires, and volcanic eruptions.
- Some of these types of disasters are difficult to predict and can onset in seconds. They could cause grave damage to physical structures and anything inside, as well as disrupt supply chains through affected areas.

3. Utility outages

- A loss of power generation, communication lines, or water shutoffs can cause severe disruption to day-to-day operations, potentially damaging physical assets, and losing productivity and service.

4. Cybersecurity

- A cyberattack is any computer-based attack on a technical asset. Examples of cyberattacks include ransomware attacks, data theftA cyberattack is any computer-based attack on a technical asset. Examples of cyberattacks include ransomware attacks, data theft, SQL injections, and distributed denial of service (DDoS) attacks.
- At best, your technical infrastructure will be at limited functionality until the issue is resolved. At worst, if you don’t have a data backup, you could potentially lose access to all your business data.

4 Characteristics Guiding Continuity Planning

- You may be able to avoid some major disruptions, but there’s always room for the unexpected. That’s why you need a solid plan to restore your business after disaster strikes.
    1. Comprehensive
    2. Realistic
    3. Efficient
    4. Adaptable

1. Comprehensive.

- You may never be able to plan for every single possible disruption — or the combinations thereof — but it is worth trying. Don't assume your first plan is going to work.
- You'll need to make sure you have backup plans, and backup plans for your backup plans. Consider every single factor that could play a role, and assume that everything will go wrong at some point.

2. Realistic.

- You don't want to get into a disaster situation and find that your best laid plans actually cannot be carried out as planned.
- Be realistic about the plan you've laid out and make sure that it has as many contingency plans built in as possible.

3. Efficient.

- Business is complex, so we won’t sit here and say your business continuity plan needs to be simple. But it needs to be able to be executed efficiently and with the resources you have at hand. T
- he extra stress and expectations in a time of disaster or disruption can make even regular tasks more difficult to accomplish. Make sure this is accounted for in your plan.

4. Adaptable.

- Nothing on paper could ever compare to the curveballs that nature or other unexpected forces may throw at us. Leave lots of room in your plan to adapt to the moment, as circumstances change — sometimes minute to minute.
- The plan should account for constant monitoring of the situation and provide a good foundation from which to pivot to addressing the issue at hand.

Benefits of Business Continuity Planning

- Lacking a plan for initiating emergency response can lead to financial loss, loss of consumer (and team member) confidence, and impact your brand reputation. Here are some of the primary benefits of having a continuity plan in place.

  1. Maintain business operations.
  2. Build customer confidence.
  3. Preserve your brand and reputation.
  4. Protect your supply chain.
  5. Gain a competitive edge.
  6. Mitigate financial risk.

1. Maintain business operations.

- If you can keep your business operations running through a crisis, you can mitigate financial loss and send a message of stability to your team members and your customers. Having a strong partnership with your human resources function will be important here.

2. Build customer confidence.

- Your customers want to know that you can respond to anything, so they can keep expecting the service from your brand that they’re accustomed to. In disaster situations, consumers often look to their favorite brands to see how they’re reacting on the public stage and how they’re able to weather the internal storm.

3. Preserve your brand and reputation.

- Large-scale disasters and disruptions are likely going to be media fodder, so it’s unlikely you’ll get a chance to follow your plan quietly. The world will be watching.
- Brands that seem prepared and able to rise to the occasion with strength, consistency, and grace will prove their resiliency to their consumers.

4. Protect your supply chain.

- Supply chain is a great example of the maxim, “Don’t put all your eggs in one basket.” Supply chain disruptions are common because there are so many ways they could happen.
- A pandemic could shutter manufacturing facilities, for example. Or a natural disaster could cripple transportation in an important geographic area. A good plan will set out already-vetted options for circumventing supply chain issues.

5. Gain a competitive edge.

- In cases where many businesses are affected by a disruption, your ability to get business moving again will go a long way in showing consumers that your brand is among the best.
- In disaster times, too, consumers watch brands closely to see how they'll react. Quick but poised action will build trust in your brand, giving you an edge on your competitors.

6. Mitigate financial risk.

- Knowing what to do quickly in case of a business disruption is an important piece of risk management. The longer the downtime, the more potential for financial loss.
- But with the right plans to pick up quickly and restore functionality where you need it most, you can keep your loss as minimal as possible.

Information Security Auditing Process

Contents

- **What is Information Security Audit?**
- **Why do a security audit?**
- **When is a security audit needed?**
- **Types of security audits**
- **Phases of Information Security Audit and Strategies**
- **What systems does an audit cover?**
- **Steps involved in a security audit**

What is Information Security Audit?

- An IT security audit evaluates the security structure of an organization’s information system. It helps businesses to protect against data threats and breaches. These involve technical reviews reporting on configurations, technologies, infrastructure, and more.

Why do a security audit?

There are several reasons to do a security audit. They include these six goals:

- Identify security problems and gaps, as well as system weaknesses.
- Establish a security baseline that future audits can be compared with.
- Comply with internal organization security policies.
- Comply with external regulatory requirements.
- Determine if security training is adequate.
- Identify unnecessary resources.

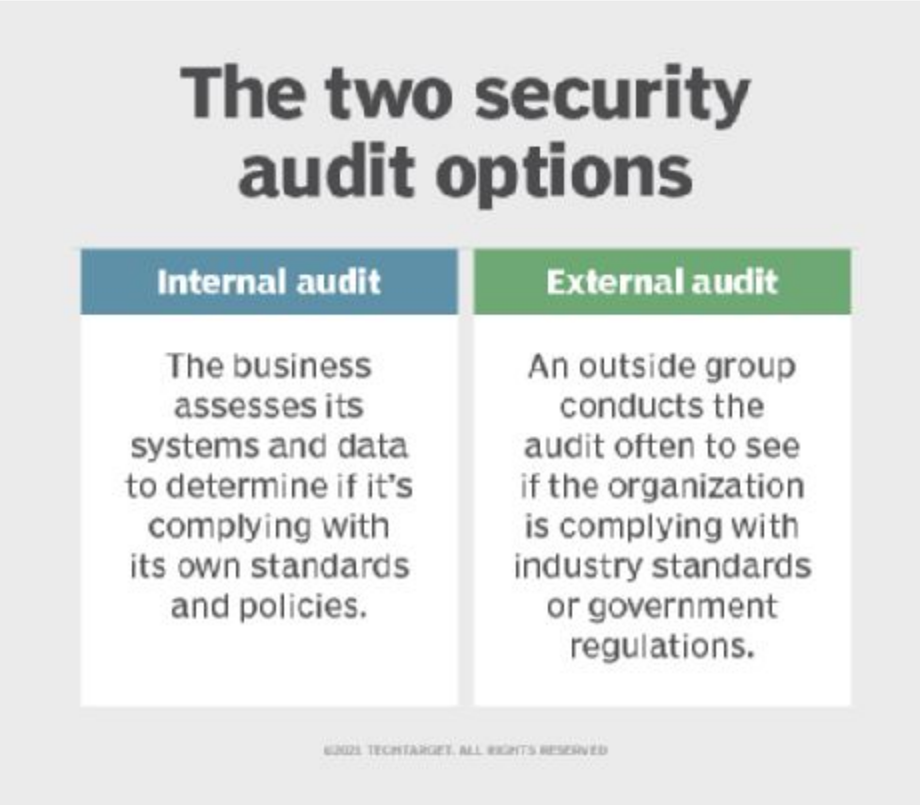
When is a security audit needed?

- How often an organization does its security audits depends on the industry it is in, the demands of its business and corporate structure, and the number of systems and applications that must be audited. Organizations that handle a lot of sensitive data -- such as financial services and heathcare providers -- are likely to do audits more frequently. Ones that use only one or two applications will find it easier to conduct security audits and may do them more frequently. External factors, such as regulatory requirements, affect audit frequency, as well.

- Many companies will do a security audit at least once or twice a year. But they can also be done monthly or quarterly. Different departments may have different audit schedules, depending on the systems, applications and data they use. Routine audits -- whether done annually or monthly -- can help identify anomalies or patterns in a system.

Types of security audits

- Security audits come in two forms, internal and external audits, that involve the following procedures:
  - Internal audits.
  - External audits.



The two security audit options

Internal audit	External audit
The business assesses its systems and data to determine if it's complying with its own standards and policies.	An outside group conducts the audit often to see if the organization is complying with industry standards or government regulations.

- **Internal audits:** In these audits, a business uses its own resources and internal audit department. Internal audits are used when an organization wants to validate business systems for policy and procedure compliance.
- **External audits:** With these audits, an outside organization is brought in to conduct an audit. External audits are also conducted when an organization needs to confirm it is conforming to industry standards or government regulations. There are two subcategories of external audits
  - second-party audits
  - third-party audits.
- **Second-party audits** are conducted by a supplier of the organization being audited.
- **Third-party audits** are done by an independent, unbiased group, and the auditors involved have no association with the organization under audit.

Phases of Information Security Audit and Strategies

- **Pre-audit agreement stage**

- Agree scope and objective of the audit. Agree on the level of support that will be provided. Agree locations, duration and other parameters of the audit. Agree financial and other considerations. Confidentiality agreements and contracting have to be completed at this stage.
- Developing/creating a formal agreement to state the audit objectives, scope, and audit protocol.
- (e.g., statement of work, audit memorandum, or engagement memo)

- **Initiation and Planning stage**

- Conducting a preliminary review of the client's environment, mission, operations, polices, and practices. Performing risk assessments of client environment, data and technology resources; completing research of regulations, industry standards, practices, and issues.
- Reviewing current policies, controls, operations, and practices; Holding an Entrance Meeting to review the engagement memo, to request items from the client, schedule client resources, and to answer client questions. This will also include laying out the time line and specific methods to be used for the various activities.

- **Data collection and fieldwork (Test phase)**

- This stage is to accumulate and verify sufficient, competent, relevant, and useful evidence to reach a conclusion related to the audit objectives and to support audit findings and recommendations. During this phase, the auditor will conduct interviews; observe procedures and practices, perform automated and manual tests, and other tasks.

- Fieldwork activities may be performed at the client's worksite(s) or at remote locations, depending on the nature of the audit.

- **Analysis**

- Analyses are performed after documentation of all evidence and data, to arrive at the audit findings and recommendations. Any inconsistencies or open issues are addressed at this time. The auditor may remain on-site during this phase to enable prompt resolution of questions and issues.

- At the end of this phase, the auditor will hold an Exit Meeting with the client to discuss findings and recommendations, address client questions, discuss corrective actions, and resolve any outstanding issues. A first draft of the findings and recommendations may be presented to the client during the exit meeting.

- **Reporting**

- Generally, the Information Security Audit Program will provide a draft audit report after completing fieldwork and analysis. Based on client response if changes are required to the draft, the auditor may issue a second draft. Once the client is satisfied that the terms of the audit are complied with the final report will be issued with the auditor's findings and recommendations.

- **Follow-through**

- Depending on expectations and agreements the auditor will evaluate the effectiveness of the corrective action taken by the client, and, if necessary, advise the client on alternatives that may be utilized to achieve desired improvements. In larger, more complex audit situations, follow-up may be repeated several times as additional changes are initiated. Additional audits may be performed to ensure adequate implementation of recommendations.
- The level of risk and severity of the control weakness or vulnerability dictate the time allowed between the reporting phase and the follow-up phase. The follow-up phase may require additional documentation for the audit client.

What systems does an audit cover?

- During a security audit, each system an organization uses may be examined for vulnerabilities in the following areas:

- **Network vulnerabilities**- Auditors look for weaknesses in any network component that an attacker could exploit to access systems or information or cause damage. Information as it travels between two points is particularly vulnerable. Security audits and regular network monitoring keep track of network traffic, including emails, instant messages, files and other communications. Network availability and access points are also included in this part of the audit.
- **Security controls-** With this part of the audit, the auditor looks at how effective a company's security controls are. That includes evaluating how well an organization has implemented the policies and procedures it has established to safeguard its information and systems. For example, an auditor may check to see if the company retains administrative control over its mobile devices. The auditor tests the company's controls to make sure they are effective and that the company is following its own policies and procedures.
- **Encryption-** This part of the audit verifies that an organization has controls in place to manage data encryption processes.

- **Software systems-** Here, software systems are examined to ensure they are working properly and providing accurate information. They are also checked to ensure controls are in place to prevent unauthorized users from gaining access to private data. The areas examined include data processing, software development and computer systems.
- **Architecture management capabilities-** Auditors verify that IT management has organizational structures and procedures in place to create an efficient and controlled environment to process information.
- **Telecommunications controls-** Auditors check that telecommunications controls are working on both client and server sides, as well as on the network that connects them.
- **Systems development audit-** Audits covering this area verify that any systems under development meet security objectives set by the organization. This part of the audit is also done to ensure that systems under development are following set standards.
- **Information processing-** These audits verify that data processing security measures are in place.

Steps involved in a security audit

These five steps are generally part of a security audit:

- **Agree on goals-** Include all stakeholders in discussions of what should be achieved with the audit.
- **Define the scope of the audit-** List all assets to be audited, including computer equipment, internal documentation and processed data.
- **Conduct the audit and identify threats-** List potential threats related to each Threats can include the loss of data, equipment or records through natural disasters, malware or unauthorized users.
- **Evaluate security and risks-** Assess the risk of each of the identified threats happening, and how well the organization can defend against them.
- **Determine the needed controls-** Identify what security measures must be implemented or improved to minimize risks.