**Background Terms**

**Management principles of ISMS**

An Information Security Management System (ISMS) is a systematic approach to managing an organisation's sensitive information and ensuring that it is protected from unauthorised access, use, disclosure, disruption, modification, or destruction. The management principles of ISMS are based on the ISO/IEC 27001 standard, which outlines a framework for establishing, implementing, maintaining, and continually improving information security (ISO, 2013).

**Define & Establish**

The "define & establish" phase involves defining the scope and objectives of the ISMS, as well as establishing the policies, procedures, and controls that will be used to meet these objectives (O'Hanley et al., 2014). This may include defining the roles and responsibilities of different stakeholders, as well as identifying any legal or regulatory requirements that must be met.

**Implement & operate**

The "implement & operate" phase involves putting the policies, procedures, and controls that were defined in the "define & establish" phase into action (O'Hanley et al., 2014). This may include training employees on the ISMS, setting up systems and processes to support the ISMS, and monitoring the ISMS to ensure that it is operating effectively.

**Monitor & Review**

The "monitor & review" phase involves regularly reviewing the ISMS to ensure that it is meeting its objectives and that any identified problems are being addressed (O'Hanley et al., 2014). This may include conducting risk assessments, reviewing log files and other monitoring data, and performing audits to ensure compliance with the ISMS.

**Maintain & Improve**

The "maintain & improve" phase involves maintaining the ISMS to ensure that it continues to meet the organisation's needs and improving it as needed. This may include updating policies and procedures, revising controls, and implementing new technologies to enhance the effectiveness of the ISMS (O'Hanley et al., 2014).

**Related laws and regulations**

In the United Kingdom, there are several laws and regulations that relate to the protection of sensitive information and the management of data in an organisation. Some examples of these laws and regulations include:

* The General Data Protection Regulation (GDPR), applies to the processing of personal data of individuals in the European Union (EU) and the export of personal data outside of the EU. The GDPR applies to all organisations that process personal data of individuals in the EU, regardless of the location of the organisation (GDPR, 2018).
* The Data Protection Act 2018, applies to the processing of personal data in the UK and supplements the GDPR. It also provides a legal framework for the UK to exit the EU (Data Protection Act, 2018).
* The Network and Information Systems Regulations 2018, which apply to certain types of organisations that rely on network and information systems for the delivery of their services. These organisations are required to take appropriate technical and organisational measures to manage the risks to the security of their systems (NIS, 2018).

**Key concepts of ISO/IEC 27001**

**Confidentiality:** Confidentiality is the protection of information from unauthorised disclosure. It is about ensuring that sensitive information is not accessed or shared by unauthorised individuals. This can include measures such as:

* Access controls are measures that are put in place to ensure that only authorised individuals have access to sensitive information.
* Encryption is the process of encoding information in such a way that it can only be accessed by individuals with the proper decryption keys. communication.
* Secure communication channels are channels that are designed to protect the confidentiality of information during transmission.

(ISO, 2013)

**Integrity:** Integrity refers to the accuracy and completeness of information. It is about ensuring that information is not modified or corrupted in an unauthorised manner. This can include measures such as:

* The use of checksums to detect whether the file has been modified. If the data in the file is changed, the checksum will also change, indicating that the file has been modified.
* A digital signature is a type of electronic signature that is used to verify the authenticity and integrity of a document or message.
* Data verification is the process of checking the accuracy and completeness of data.

(ISO, 2013)

**Availability:** Availability is the accessibility of information. It is about ensuring that authorised individuals can access information when needed.

* Redundant systems are backup systems that can take over in the event of a failure or outage.
* Backup and recovery procedures are processes that are put in place to ensure that information can be recovered in the event of a disaster or data loss.
* A disaster recovery plan is a document that outlines the steps that an organisation will take to recover from a disaster or other significant disruption.

(ISO,2013)

**Vulnerability:** Vulnerability is a weakness in a system or process that could be exploited by a threat. Vulnerabilities can arise from a variety of factors:

* Software flaws,
* Hardware defects,
* Human error.

(ISO,2013)

**Threat:** A threat is a potential danger that could exploit a vulnerability and cause harm to an organisation. Threats can come from a variety of sources:

* Cyber-attacks
* Natural disasters such as earthquakes.
* Human error

(ISO, 2013)

**Impact:** The impact of a security incident is the extent of the harm or damage that it causes. This can include financial loss, reputational damage, and other consequences. Determining the potential impact of a security incident can help organisations prioritise their efforts to prevent or mitigate such incidents.

* A security incident can result in financial loss, for example, an organisation may incur costs associated with recovering from a data breach, such as legal fees, remediation expenses, and lost revenue.

 (ISO, 2013)

**Control objectives and controls - ISO/IEC 27001**

The control objectives and controls of an Information Security Management System (ISMS) are defined in the ISO/IEC 27001 standard. The control objectives are the high-level goals that the ISMS are designed to achieve, and the controls are the specific measures that are implemented to achieve those goals.

**Preventive**

Preventive controls are measures that are put in place to prevent security incidents from occurring. Examples of preventive controls include:

* Access controls are measures that are put in place to ensure that only authorised individuals have access to sensitive information.
* Security training is training provided to employees to help them understand security risks and how to protect against them.
* Security policies are formal documents that outline an organisation's security rules and procedures.

(Will Kenton, 2021)

**Detective**

Detective controls are measures that are put in place to detect security incidents after they have occurred. Examples of detective controls include:

* An intrusion detection system (IDS) is a type of security software that is designed to detect unauthorised access or activity on a computer system or network.
* Log review is the process of examining log files, which are records of activity on a computer system or network.
* A vulnerability assessment is a review of an organisation's systems and networks to identify vulnerabilities that could be exploited by threats.

(Will Kenton, 2021)

**Corrective**

Corrective controls are measures that are put in place to address security incidents after they have occurred. Examples of corrective controls include:

* Incident response plans: An incident response plan is a document that outlines the steps that an organisation will take to respond to a security incident.
* Disaster recovery plans: A disaster recovery plan is a document that outlines the steps that an organisation will take to recover from a disaster or other significant disruption.
* Patch management is the process of identifying, testing, and applying software updates and patches to fix vulnerabilities or address other issues.

(Walkowski.D, 2019)

**Countermeasures**

Countermeasures are used to prevent or mitigate the impact of an information security incident. An ISMS is designed to identify and evaluate the risks to an organisation's sensitive information and implement appropriate countermeasures to protect against those risks.

**Risk Treatment Plan**

The Risk Treatment Plan (RTP) is a key component of an organisation's implementation of ISO 27001. It outlines the steps the organisation will take to address identified security threats and is a mandatory requirement for the ISO 27001 implementation process. The RTP is the final stage of the ISO 27001 risk assessment process. ISO 27001 recommends that organisations take one of four actions to manage risks: modify the risk by implementing controls, avoid the risk, share the risk with a third party, or retain the risk. Organisations can determine the best way to modify a risk by reviewing the controls listed in Annex A of ISO 27001, which includes 114 controls divided into 14 sections (ISO,2013).

**Disaster Recovery**

Disaster recovery is the process of resolving disruptions and restoring normal operations. This includes identifying the cause of the incident, setting specific deadlines to prevent further damage, and developing technical plans to address the problem. Disaster recovery plans often include recovery time objectives (RTOs), indicating how long it will take for a product, service, or activity to become available again after an incident. Organisations must be able to resume operations within this time frame or risk further disruptions. For example, if an office flood damages servers, disaster recovery plans would include restoring systems from backups with an RTO of a certain number of days or weeks. Business continuity planning is closely tied to disaster recovery, as BCPs are created based on estimated recovery times. Once all issues are resolved and the organisation returns to its original setup, the BCP is no longer in effect.

**Business Continuity**

Business continuity involves ensuring that an organisation can continue to function during disruptions by implementing temporary solutions. A business continuity plan (BCP) would outline steps to secure important assets and provide alternative work arrangements in the event of an office flood. BCPs generally focus on maintaining network connections, online systems, and other essential business operations to minimise disruptions and quickly restore productivity (Sahebjamnia et al., 2015).

**Internal Audit**

Internal ISO 27001 audits are a thorough examination of an organisation's information security management system (ISMS) to determine if it meets the requirements of the ISO 27001 standard. Unlike a certification evaluation, it is conducted by the organisation's employees and the results are used to improve the ISMS. The requirements for an internal audit are outlined in Clause 9.2 of ISO 27001 (ISO, 2013). The audit allows for the identification of areas for improvement by comparing current practices to the standard (Sahebjamnia et al., 2015).

**Control objectives and controls (PII Controllers) - ISO/IEC 27701**

The control objectives and controls for personal data controllers are defined in the ISO/IEC 27701 standard. Personal data controllers are organisations that determine the purposes and means of processing personal data. The control objectives are the high-level goals that the privacy information management system (PIMS) is designed to achieve, and the controls are the specific measures that are implemented to achieve those goals (Sahebjamnia et al., 2015).

**Bibliography:**

Data Protection Act, 2018. Data Protection Act 2018. [online] GOV.UK. Available at: < [https://www.gov.uk/government/collections/data-protection-act-2018>](https://www.gov.uk/government/collections/data-protection-act-2018%3e) [Accessed 28 December 2022].

GDPR, 2018. Guide to the General Data Protection Regulation. [online] GOV.UK. Available at: < [https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation>](https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation%3e) [Accessed 28 December 2022].

International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. Geneva, Switzerland.

International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. Geneva, Switzerland.

Kenton. W, (27/05/2021), *Detective Control: Definition, Examples, Vs. Preventive Control*, [Accessed 14/01/2023], <<https://www.investopedia.com/terms/d/detective-control.asp#:~:text=Key%20Takeaways,as%20assessments%20of%20current%20controls>.>

NIS Regulations, 2018. [The Network and Information Systems Regulations. [online] GOV>UK. Available at < https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018> [Accessed 28 December 2022].](The%20Network%20and%20Information%20Systems%20Regulations.%20%5bonline%5d%20GOV%3eUK.%20Available%20at%20%3c%20https:/www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018%3e%20%5bAccessed%2028%20December%202022%5d.%0d)

O'Hanley, R., O'Hanley, R. and Tiller, J.S. (2014) Information Security Management Handbook, sixth edition, volume 7. Taylor & Francis Group LLC.

Sahebjamnia, N., Torabi, S.A. and Mansouri, S.A. (2015) “Integrated Business Continuity and disaster recovery planning: Towards organizational resilience,” European Journal of Operational Research, 242(1), pp. 261–273. Available at: <https://doi.org/10.1016/j.ejor.2014.09.055.>

Walkowski.D, (2019), *What Are Security Controls?*, <<https://www.f5.com/labs/learning-center/what-are-security-controls#:~:text=Corrective%20controls%20include%20any%20measures,process%2C%20or%20rebooting%20a%20system>.> [Accessed 14/01/2023].