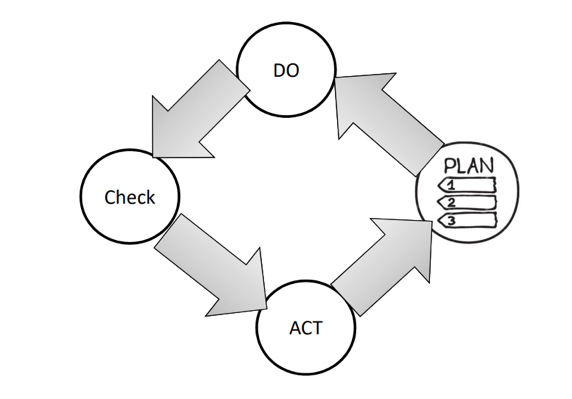
WEEK 2

COMMON SECURITY FRAMEWORKS

ISO/IEC 27000

* ISO/IEC 2700 was adapted from British standard 7799 (*BS7799*).
* BS7799 was developed to guide organizations on how to **design**, **implement** and **maintain** **policies**, **process**, and **technologies** to **manage** **risk**.
* It consisted on **two** **parts**:
  + Part **one** outlined **control** **objectives** and how to **achieve** **them**.
  + Part **two** outlines how a **security** **program** can be **set** **up**.
* It laid foundation on how security should cover:
* Information security policy for the organization.
* Creation of information security infrastructure.
* Asset classification and control.
* Personal security.
* Communication and operation.
* Access control.



ISO/IEC 27000: PLAN

* Define the **scope** of the ISMS.
* Define ISMS **policy.**
* Define **approach** to risk assessment.
* **Identify** the **risks.**
* **Analyse** and **evaluate** the risks.
* **Identify** and **evaluate** options for the **treatment** of risk.
* Management **approves** **residual** **risks.**
* Management **authorizes** **ISMS.**
* Select control **objectives** and **controls.**

ISO/IEC 27000: DO

* **Formulate** risk treatment **plan**.
* **Implement** risk treatment **plan**.
* **Implement** **controls**.
* Implement **training** and **awareness** programs.
* Manage **operations**.
* Manage **resources**.
* Implement procedures to **direct**/**respond** to **security** **incidents**.

ISO/IEC 27000: CHECK

* **Execute** **monitoring** procedures.
* Undertake regular **reviews** of ISMS effectiveness.
* Measure **effectiveness** of controls.
* Review **level** of **residual** and **acceptable** risk.
* Conduct **internal** ISMS **audit**.
* Regular management **review**.
* **Update** security **plans**.
* Record **actions** and **events**.

ISO/IEC 27000: ACT

* Implement identified **improvements**.
* Take **corrective**/**preventative** **action**.
* Apply **lessons** **learned** (*including other organizations*).
* **Communicate** **results** to interested parties.
* Ensure **improvements** to **achieve** **objectives**.

ISO/IEC 27000: PROVIDES

* **Information security policy for the organization:**
  + **Map** of **business** **objectives** to **security**, management’s **support**, security **goals**, and **responsibilities**.
* **Creation of information security infrastructure**
  + **Create** and **maintain** an organizational security **structure** through the use of a security **forum**, a security **officer**, defining security **responsibilities**, **authorization** **processes**, **outsourcing**, and independent **reviews**.
* **Asset classification and control**
  + Develop a security infrastructure to protect organizational **assets** through **accountability** and **inventory**, **classification**, and **handling** **procedures**.
* **Personnel security**
  + Reduce risks that are inherent in human interaction by **screening** **employees**, defining **roles** and **responsibilities**, **training** employees properly, and **documenting** the **ramifications** of not meeting expectations.
* **Physical and environmental security**
  + Protect the organization’s assets by properly choosing a facility **location**, **erecting** and **maintaining** a security **perimeter**, implementing **access** **control**, and **protecting** **equipment**.
* **Communications and operations management**
  + Carry out operations security through **operational** **procedures**, proper **change** **control**, **incident** **handling**, **separation** of **duties**, **capacity** **planning**, **network** **management**, and **media** **handling**.
* **Access control**
  + Control access to assets based on **business** **requirements**, **user** **management**, **authentication** **methods**, and **monitoring**.
* **System development and maintenance**
  + Implement security in **all phases of a system’s lifetime** through **development** of security **requirements**, **cryptography**, **integrity** protection, and **software** development **procedures**.
* **Business continuity management**
  + Counter **disruptions** of normal operations by using **continuity** **planning** and **testing**.
* **Compliance** 
  + Comply with **regulatory**, **contractual**, and **statutory requirements** by using **technical** **controls**, system **audits**, and **legal** **awareness**.

ISO/IEC 27000 SERIES

**ISO/IEC 27000 Overview** and **vocabulary.**

**ISO/IEC 27001** ISMS **requirements.**

**ISO/IEC 27002** Code of **practice** for **information security management.**

**ISO/IEC 27003** **Guideline** for **ISMS implementation.**

**ISO/IEC 27004** **Guideline** for information security management **measurement** and **metrics** **framework**.

**ISO/IEC 27005** Guideline for information security **risk** **management.**

**ISO/IEC 27033-1**  Guideline for **network security.**

ISO/IEC 27001 REQUIREMENT

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
   1. Understanding the organization and its context.
   2. Understanding the needs and expectations of interested parties.
   3. Determining the scope of the information security management system.
   4. Information security management system.
5. Leadership
   1. Leadership and commitment.
   2. Policy.
   3. Organizational roles, responsibilities and authorities
6. Planning
   1. Actions to address risks and opportunities.
   2. Information security objectives and planning to achieve them.
7. Support
   1. Resources.
   2. Competence.
   3. Awareness.
   4. Communication.
   5. Documented information.
8. Operation.
   1. Operational planning and control.
   2. Information security risk assessment and treatment.
9. Performance evaluation
   1. Monitoring, measurement, analysis and evaluation.
   2. Internal audit and management review.
10. Improvement
    1. Nonconformity and corrective action.
    2. Continual improvement.