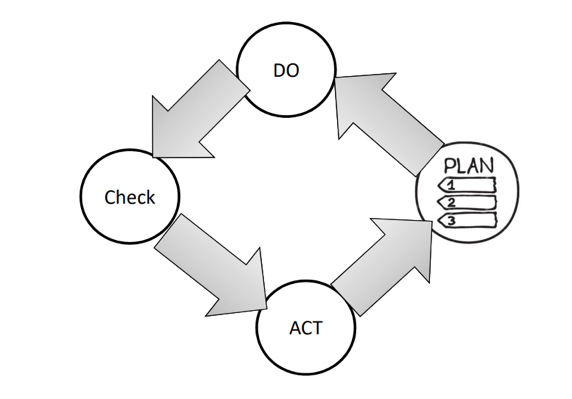
WEEK 2

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.

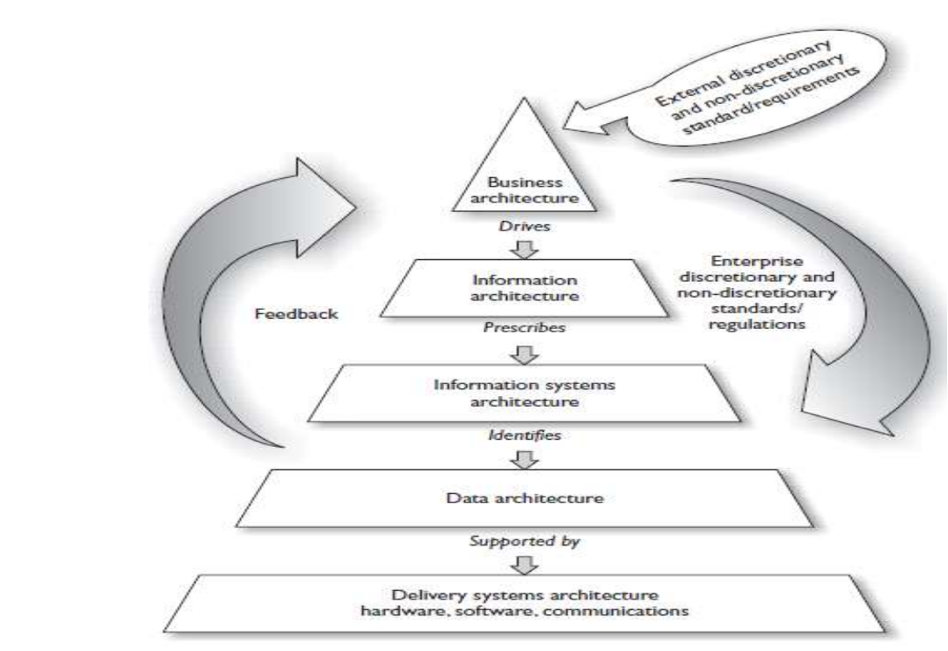
CobiT

The **Control Objective for Information and related Technology** (*CobiT*) and set of control objectives developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI).

* Defines goals for the controls that should be used to properly manage IT and to ensure that IT maps to business needs.
* *Divided into four categories:*
  + **Plan and Organise**
  + **Acquire and Implement**
  + **Deliver and Support**
  + **Monitor and Evaluate**
* CobiT provides the objective that the real-world implementations (controls) you chose to put into place need to meet.

Enterprise Architecture

* An enterprise architecture encompasses the **essential** and **unifying** **components** **of** an **organization**.
* It expresses the enterprise **structure** (*form*) and **behaviour** (*function*).
* It embodies the enterprise’s **components**, their **relationships** to each other, and to the environment.



TOGAF (The Open Group Architecture Framework)

* The US Department of Defence.
* TOGAF is a framework that can be used to develop the following architecture types:
  + **Business** Architecture (*process, activities*)
  + **Data** Architecture (*that must be organised, safeguarded*)
  + **Applications** Architecture (*custom or off the shelf software tools*)
  + **Technology** Architecture (*computer system or telephone networks*)

NIST CSF (National Institute of Standards and Technology)

Has **three** core **components**:

**THE FRAMEWORK CORE**

***Functions*** Organize basic cybersecurity activities at their highest level. These Functions are ***Identify****,* ***Protect****,* ***Detect****,* ***Respond****, and* ***Recover*** (*shown beneath*).

***Categories*** The subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.

***Subcategories*** Further divide a Category into specific outcomes of technical and/or management activities.

***Informative References*** Specific sections that illustrate a method to achieve the outcomes associated with each Subcategory

**THE FRAMEWORK CORE - FUNCTIONS**

* **Identify**
  + Develop an organizational **understanding** to **manage** **cybersecurity** **risk** to systems, people, assets, data, and capabilities.
* **Protect**
  + Develop and implement appropriate **safeguards** to ensure delivery of critical services.
* **Detect**
  + Develop and implement appropriate activities to identify the **occurrence** of a **cybersecurity** **event**.
* **Respond**
  + Develop and implement appropriate **activities** to **take** **action** **regarding** a **detected** **cybersecurity** **incident**.
* **Recover**
  + Develop and implement appropriate activities to maintain **plans** for **resilience** and to **restore** any capabilities or **services** that were **impaired** due to a **cyber** **security** **incident**.

**THE FRAMEWORK CORE - IDENTIFY FUNCTIONS**

* **Asset Management**
  + **Inventory** of **assets**, **map data flow**, **prioritize assets**, and **establish** **workforce** **roles**.
* **Business Environment**
  + Identify **supply** **chain**, organization **mission** and **requirement** for **critical** **services**
* **Governance**
  + Establish **security** **policy**, **information** **security** **roles**/**responsibilities**, **risk** **management** process.
* **Risk Assessment**
  + Identify **threat/vulnerability source**, current **threat**, potential **risk/impact** and risk responses.
* **Risk Management Strategies**
  + Establish **risk management process** and **organization’s risk tolerance.**
* **Supply Chain Risk Management**
  + Identify **suppliers/partners and execute contracts**, **assessments**, and **response/recovery** testing.

**THE FRAMEWORK CORE - PROTECT FUNCTIONS**

* **Identity Management**
  + Manage user/device/process **creds**, physical/remote **access**, **permissions** and **segmentations**.
* **Awareness and Training**
  + **Train** users, admins, third parties, executives, and security **personnel**.
* **Data Security**
  + Protect data, assets, and capacity from **leakage**, **integrity** and **development/testing**
* **Information Protection Process and Procedures**
  + Implement SDLC, **baselines**, change control, backups, IR, and vuln management.
* **Maintenance** 
  + Perform, approve, and log all local and **remote** **maintenance** in a secure manner
* **Protective Technology**
  + Implement **protections** for **logs**, **removable** **media**, **network**, and **systems**.

**THE FRAMEWORK CORE - DETECT FUNCTIONS**

**Anomalies and Events**

* **Collect**, **correlate**, **baseline** and analyse **data flows** and **events**.
* Use multiple **sources** and **sensors**.
* Establish **incident** **thresholds**.

**Security Continuous Monitoring**

* Monitor for **malicious activity** in network, physical **spaces**, user **activities**, **devices**.
* Perform **vulnerability scans.**

**Detection Processes**

* Define **detection** **roles**, **activities** and **communications**.
* Test **detection processes**.
* Continuously improve **detection capabilities**.

**THE FRAMEWORK CORE - RESPOND FUNCTIONS**

**Response Planning**

* **Execute** and **maintain response plan**.

**Communications**

* **Coordinate** incident **roles**, **stakeholders** and **information** **sharing**.

**Analysis**

* Investigate **events**, perform **forensics**, understand **impacts**, and establish reporting channels.

**Mitigation**

* **Contain**, **mitigate** and **document** **events** and **incidents**.

**Improvement**

* Perform **lessons** **learned** and **update** **response** **strategies**.

**THE FRAMEWORK CORE - RESPOND FUNCTIONS**

**Recovery Planning**

* Execute **recovery plan** during incident.

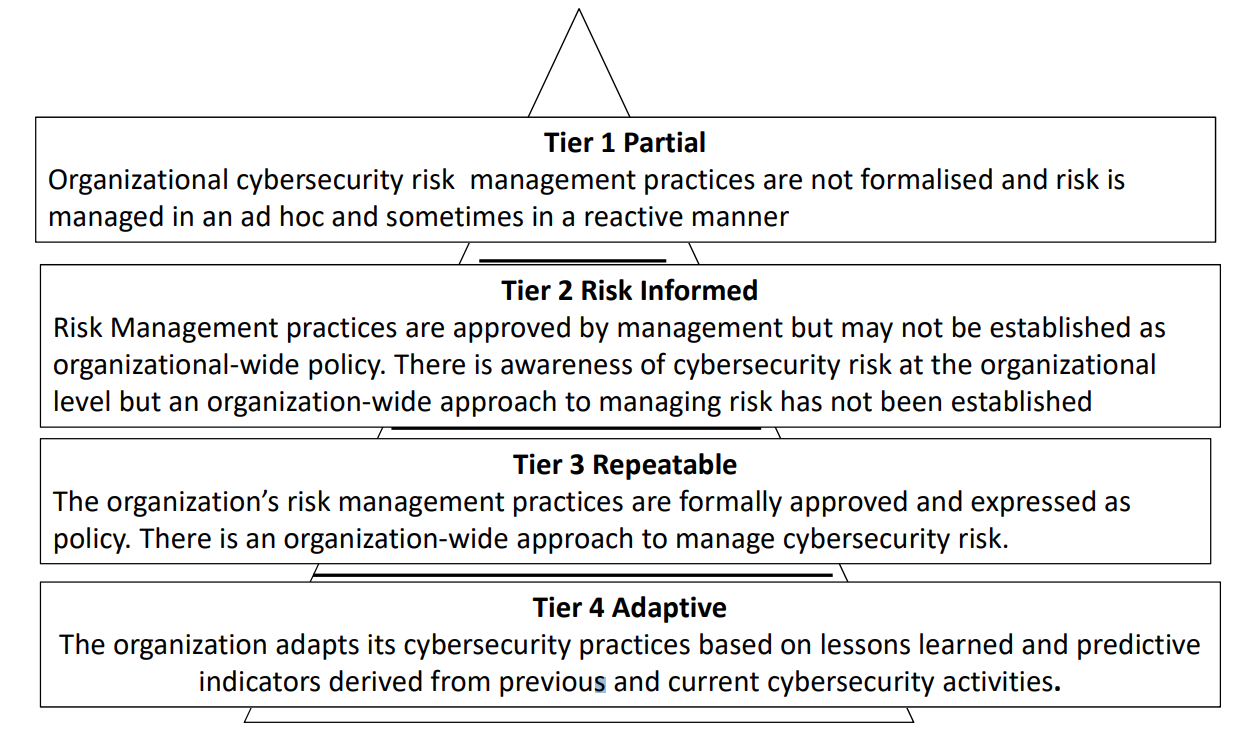
**Improvements**

* Incorporate **lessons** **learned** and **update**.

**Communications**

* **Manage** public **relations**, repair **reputation** and **communicate** with **stakeholders**.

FRAMEWORK IMPLEMENTATION TIERS



FRAMEWORK IMPLEMENTATION STEPS

|  |  |  |
| --- | --- | --- |
| **STEP NUMBER** | **STEP** | **DESCRIPTION** |
| 1 | *Prioritise and Scope* | * Identify business/mission objectives and strategic priorities. * Describe cyber security risks * Determine organizational components to use Framework |
| 2 | *Orient* | * Identify the system assets, requirement, and risk management approaches. * Determine how to evaluate current risk management and cyber security posture |
| 3 | *Create Current Profile* | * Map current cyber security and risk management practices to a Framework implementation Tier |
| 4 | *Conduct Risk Assessment* | * Identify cyber-security risks. * Evaluate and analyse risk. * Identify risk above tolerance. |
| 5 | *Create Target Profile* | * Describe desired cyber-security outcomes. * Account for unique risks. * Develop Target Profile. * Develop Target implementation Tier |
| 6 | *Determine, Analyse and Prioritise Gaps* | * Compare Current Profile and Target Profile. * Determine resources to address gaps and create a prioritise Action plan. |
| 7 | *Implement Action Plan* | * Implement necessary actions. * Monitor cyber-security practices against Target Profile. |

ISA/IEC 62443

* Formerly known as **ISA 99**.
* Used as the **global** **standard** for the **security** of **Industrial Control System (ICS)** **networks**.
* Helps organizations to **reduce** both the **risk of failure and exposure** of ICS **networks** to **cyberthreats**.
* IEC 62443 consists of thirteen documents which are organized into four groups:
  + ***General, Policies and Procedures, System, and Component***

**ISA/IEC 62443 – System Requirement**

* The three documents within the System group concern the **design** **choices**, **modifications** or **adjustments** required to **enhance** the **security** of an ICS network.
* The first document provides an **overview** of **existing** **network** security **technologies**, their **advantages** and **limitations**.
* The second addresses security risk **assessment** and **network** **design**.
* The third document describes **general** **system** **security** **requirements** such as **authentication**, data **confidentiality** and system **integrity**, etc.

**ISA/IEC 62443 – Component Requirement**

* The Component group consists of **two** **documents**.
* The first deals with a **development process for ICS products**, aimed at **reducing** the number of security **vulnerabilities** in **control system solutions**.
* The second document specifies the **technical requirements** for **securing** the **individual** **components** of an ICS **network**.

NCSC CAF Guidance

**National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)**

* Organisations within the UK Critical National Infrastructure (CNI).
* Organisations subject to NIS Directive cyber regulation.
* Organisations managing cyber-related risks to public safety.

The CAF Collection consists of a set of **14 cyber security & resilience principles**, together with guidance on using and **applying** the **principles**, and the **Cyber Assessment Framework (CAF)** itself.

**Resources related to cyber and safety provided by the NCSC.**

* A set of cyber security and resilience principles for managing cyber-related risks to safety.
* A collection of supporting guidance.
* A Cyber Assessment Framework (CAF) incorporating indicators of good practice.

CAF - Principles and Guidance

**Protecting against Cyber-attack**

* Service protection policies and processes.
* Identity and access control.
* Data security.
* System security.
* Resilient networks and systems.
* Staff awareness and training

**Detecting cyber security events**

* Security monitoring
* Proactive security event discovery

**Minimising the impact of cyber security incidents**

* Response and recovery planning
* Lessons learned