CMT116 Common Risk Frameworks

Amir Javed

Module Structure

- Class test 30%

  - A computerized test that will assess students’ understanding of key cyber security and risks concepts, principles, as well as their knowledge of common security frameworks, standards and regulations, risk assessment and threat modelling methodologies.

  - To be scheduled in Week 7.

Today’s session

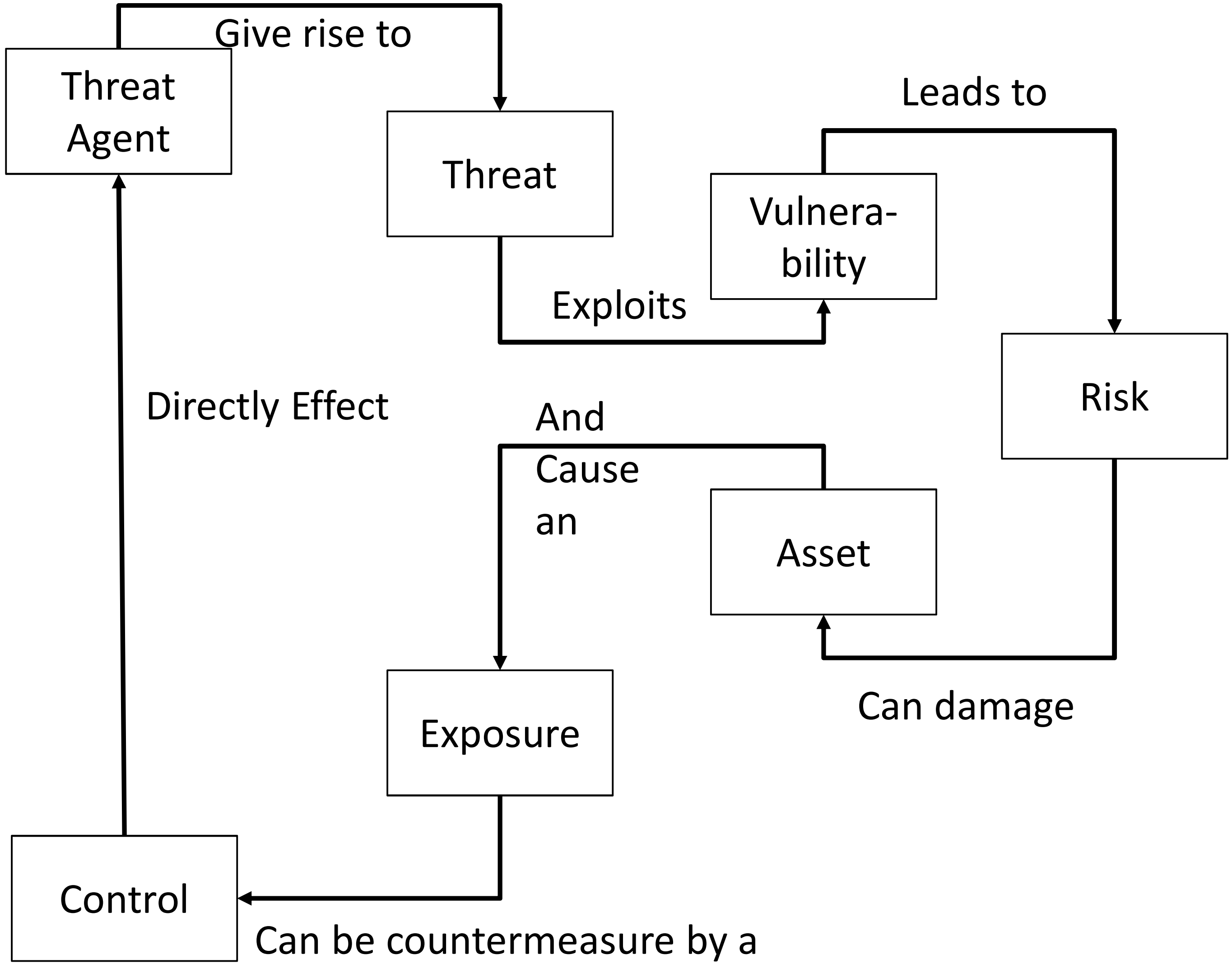
- Quick recap on what we did last week.
- Common security frameworks
- Discussion on in small groups between them.

Recap

Revise last session important points. Interactive session.

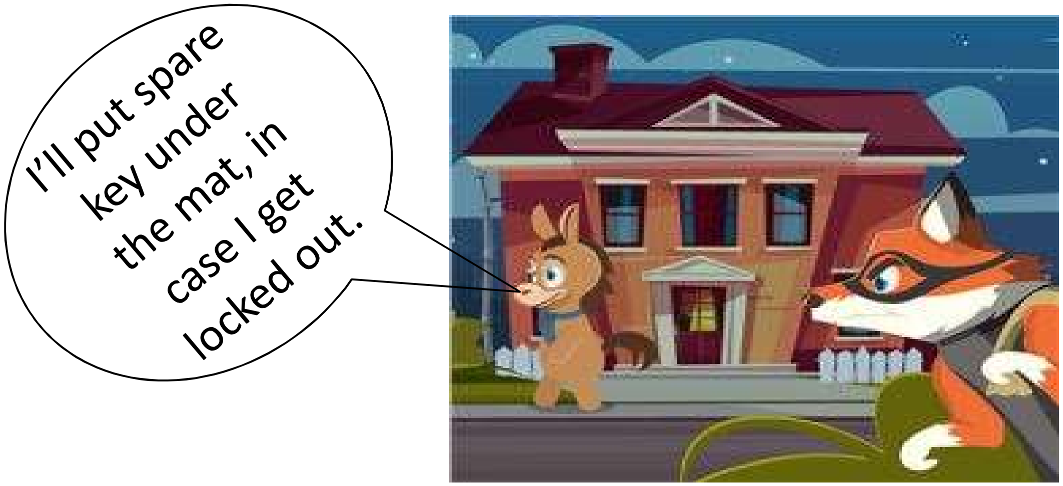
- Join at **www.kahoot.it** or with the **Kahoot! App**

Recap


Threat Agent
Give rise to
Threat
Leads to
Vulnera-bility
Exploits
Risk
Directly Effect
And Cause an
Asset
Can damage
Exposure
Control
Can be countermeasure by a

What not to do ?

- **Security through obscurity**
  - is assuming that your enemies are not as smart as you are and that they cannot figure out something that you feel is very tricky.
  - Don’t rely in trickery, for instance remap protocols on their firewalls so that HTTP is not coming into the environment over the well-known port 80, but instead 8080.



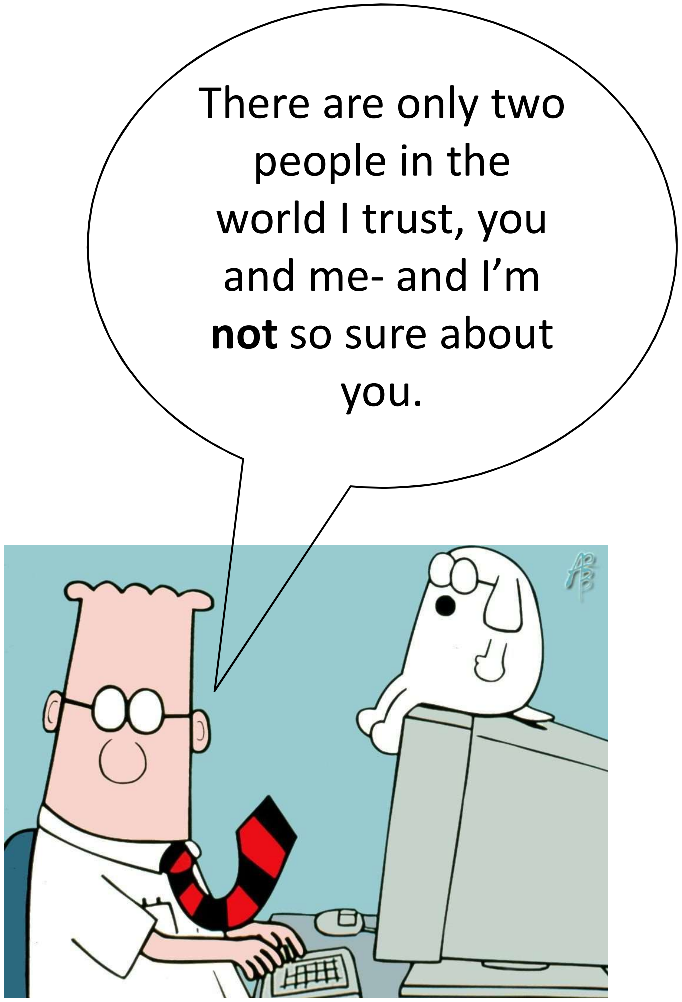
Some vendors work on the premise that since their product's code is compiled this provides more protection than products based upon open-source code because no one can view their original programming instructions.

Would you agree with this statement ?

The proper approach to security is to ensure the original software does not contain flaws

Best Practice

- A security program is a framework made up of many entities: logical, administrative, and physical protection mechanisms, procedures, business processes, and people that all work together to provide a protection level for an environment.
- Each has an important place in the framework, and if one is missing or incomplete, the whole framework may be affected.
- The program should work in layers: one layer provides support for the layer above it and protection for the layer below it.
- Using the framework, organizations are free to plug in different types of technologies, methods, and procedures to accomplish the necessary protection level for their environment.


There are only two people in the world I trust, you and me- and I'm **not** so sure about you.

Goal of Cyber Security Framework

- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state;
- Communicate among internal and external stakeholders about cybersecurity risk.

Common Security Frameworks

- ISO/IEC 27000
- NIST CSF
- ISA/IEC 62443
- The Control Objective for Information and related Technology (CobiT)
- Enterprise Architecture - *The Open Group Architecture Framework (TOGAF)*
- *NCSC CAF*

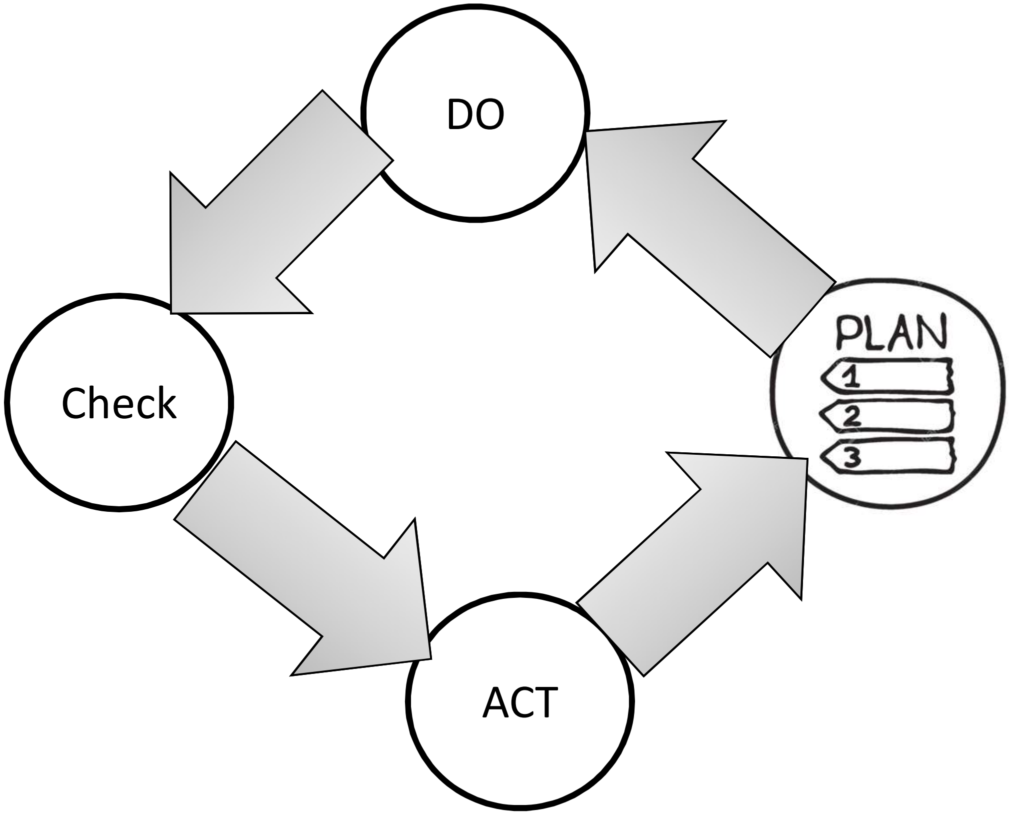
ISO/IEC 27000

A bit of history

- 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

The British seem to know what they are doing, let's follow them

ISO/IEC 27000



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

ISO/IEC 27000 - Provides

- **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.

ISO/IEC 27000 Provides

- **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

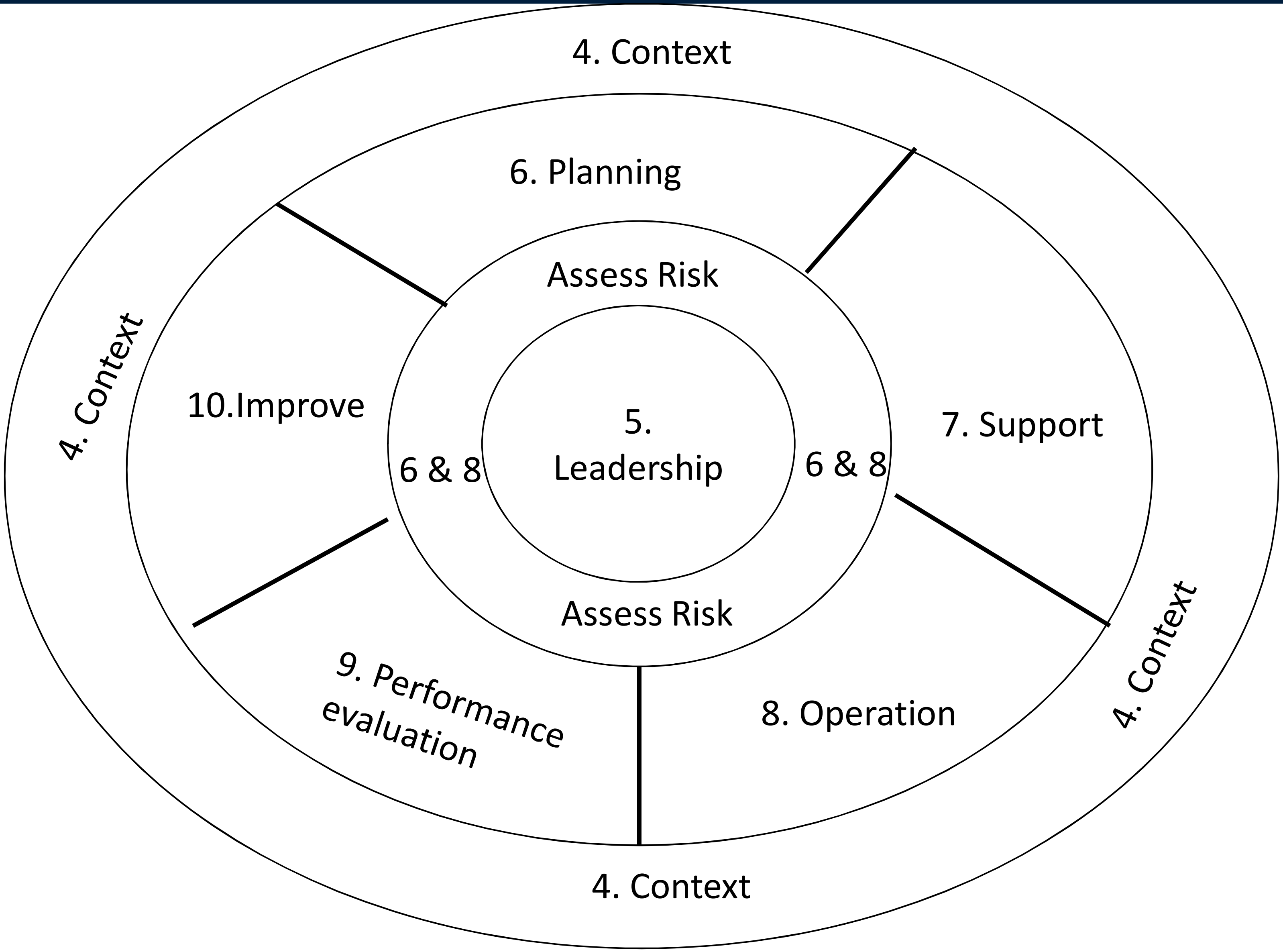
ISO/IEC 27001 Requirement

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

ISO/IEC 27001 Requirement

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

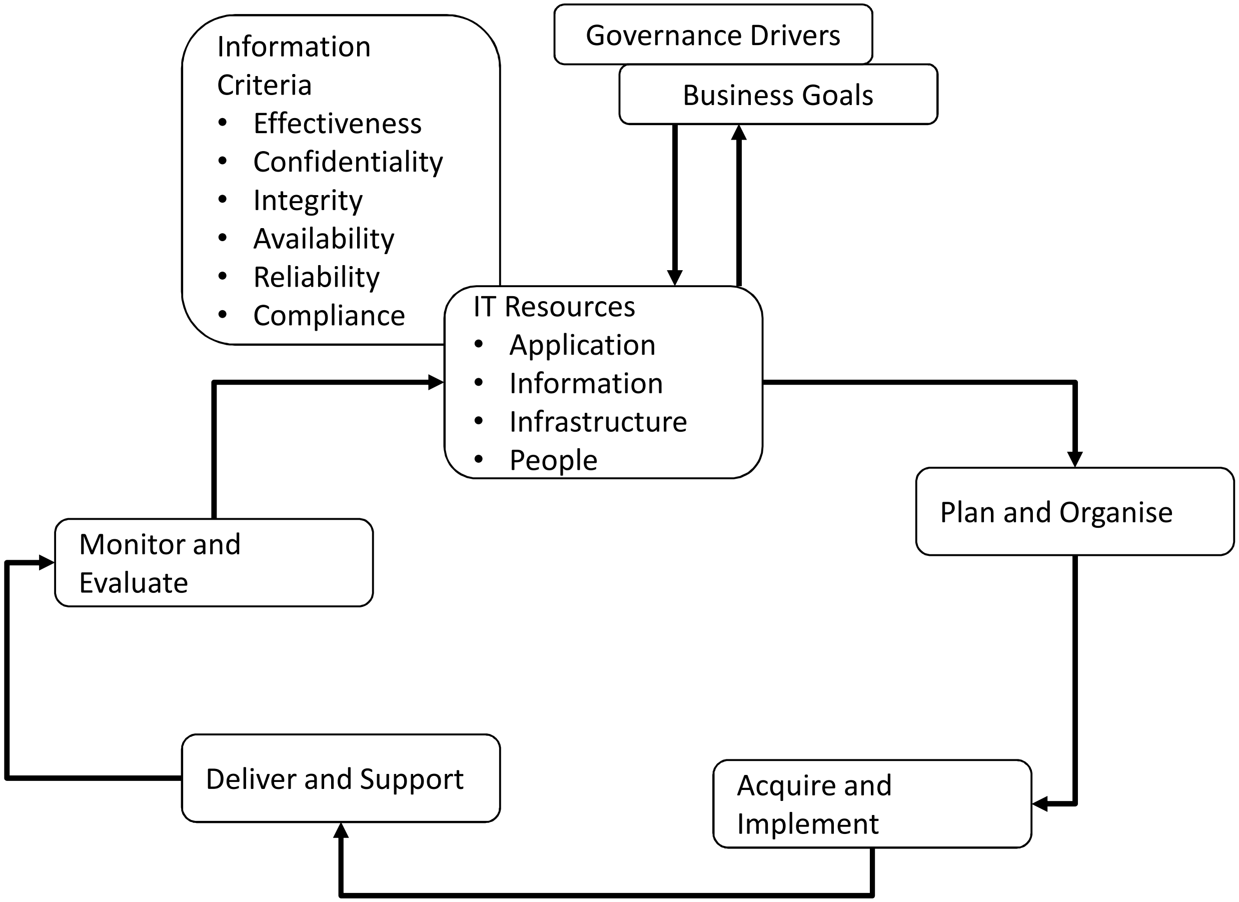
ISO/IEC 27001 Requirement



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).
- It defines goals for the controls that should be used to properly manage IT and to ensure that IT maps to business needs.
- It is divided into four categories
  - Plan and Organize,
  - Acquire and Implement,
  - Deliver and Support, and
  - Monitor and Evaluate

CobiT



Information Criteria
• Effectiveness
• Confidentiality
• Integrity
• Availability
• Reliability
• Compliance
Governance Drivers
Business Goals
IT Resources
• Application
• Information
• Infrastructure
• People
Plan and Organise
Monitor and Evaluate
Deliver and Support
Acquire and Implement

Plan and Organize

- PO1 Define a strategic IT plan
- PO2 Define the information architecture
- PO3 Determine the technological direction
- PO4 Define the IT processes, organization, and relationships
- PO5 Manage the IT investment
- PO6 Communicate management aims and directions
- PO7 Manage IT human resources
- PO8 Manage quality
- PO9 Assess and manage risks
- PO10 Manage projects

Acquire and Implement

- AI1 Identify automated solutions
- AI2 Acquire and maintain application software
- AI3 Acquire and maintain technology infrastructure
- AI4 Enable operation and use
- AI5 Procure IT resources
- AI6 Manage changes
- AI7 Install and accredit solutions and changes

Deliver and Support

- DS1 Define service levels
- DS2 Manage third-party services
- DS3 Manage performance and capacity
- DS4 Ensure continuous service
- DS5 Ensure systems security
- DS6 Identify and attribute costs
- DS7 Educate and train users
- DS8 Manage service desk and incidents
- DS9 Manage the configuration
- DS10 Manage problems
- DS11 Manage data
- DS12 Manage the physical environment
- DS13 Manage operations

Monitor and Evaluate

- ME1 Monitor and evaluate IT performance
- ME2 Monitor and evaluate internal control
- ME3 Ensure regulatory compliance
- ME4 Provide IT governance

Role of CobiT

So how does CobiT fit into the big picture?

When you develop your security policies that are aligned with the ISO/IEC 27000 series, these are high-level documents that have statements like, “Unauthorized access should not be permitted.” But who is authorized? How do we authorize individuals? How are we implementing access control. ?

CobiT provides the objective that the real-world implementations (controls) you chose to put into place need to meet.

Why we need Enterprise Architecture

“net profits,” “risk universes,” “portfolio strategy,” “hedging,” “commodities,”

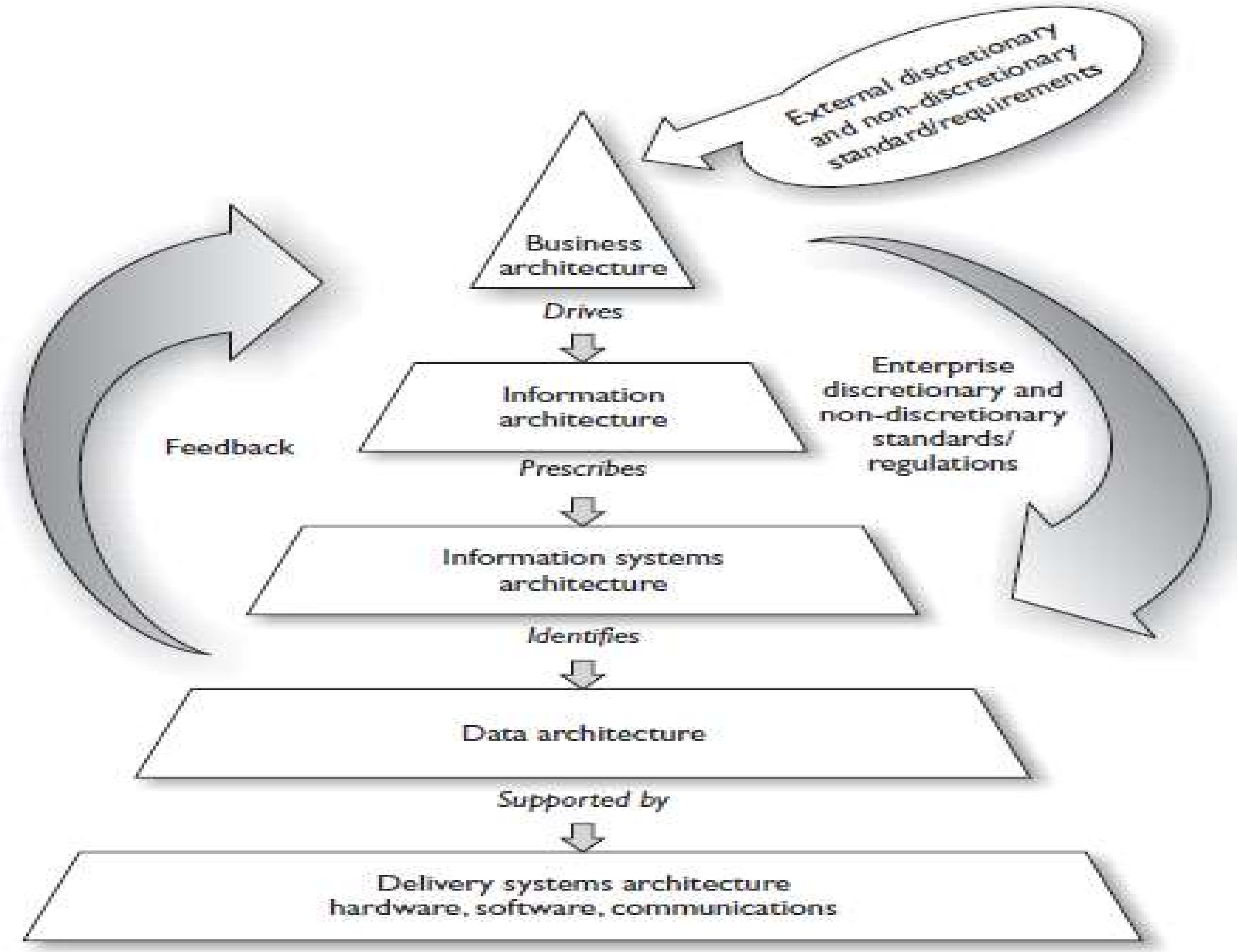
“deep packet inspection,” “level three devices,” “cross-site scripting,” “load balancing,”

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.

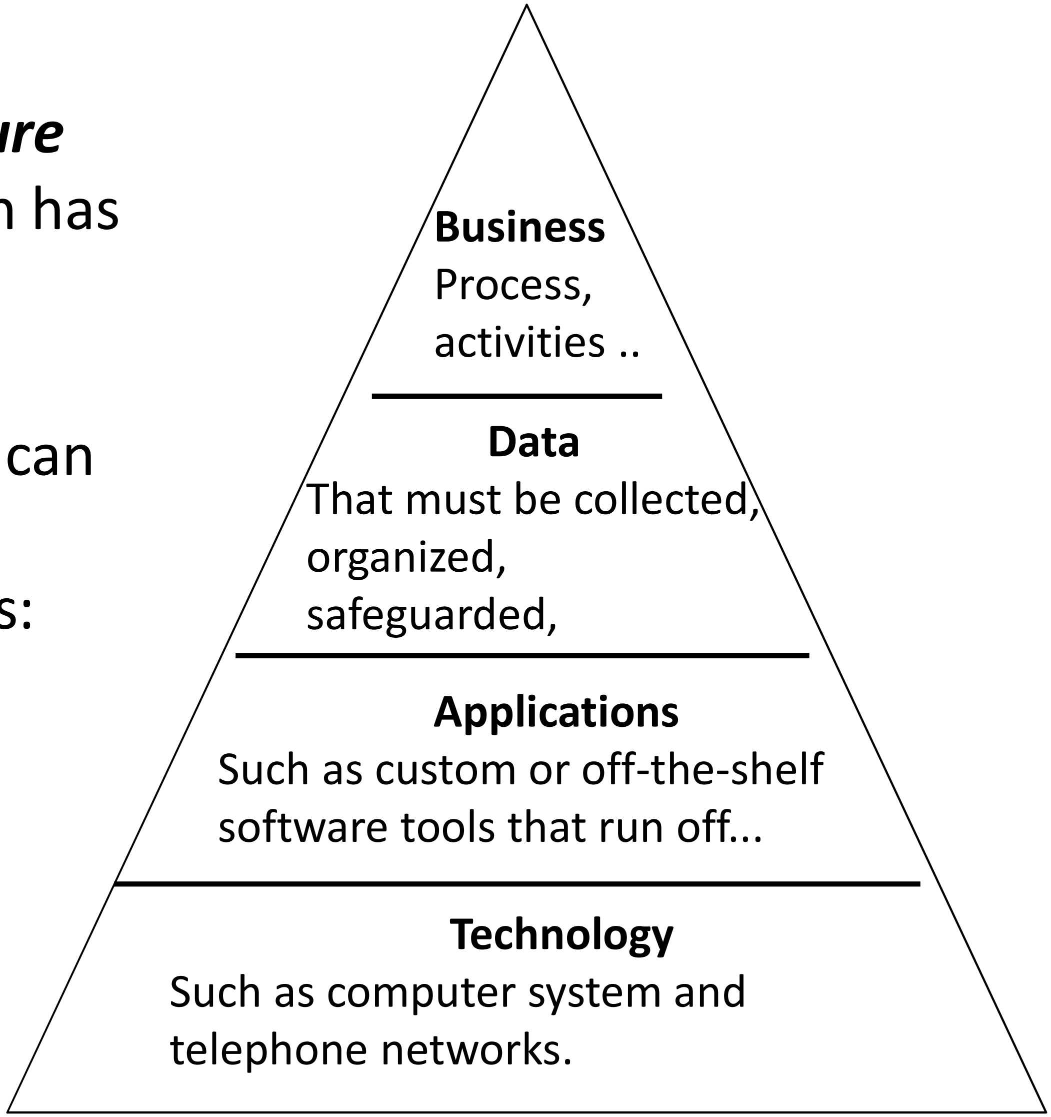
Note : You use the framework as a guideline on how to build an architecture that best fits your company's needs

Enterprise Architecture


External discretionary and non-discretionary standard/requirements
Business architecture
Drives
Information architecture
Prescribes
Information systems architecture
Identifies
Data architecture
Supported by
Delivery systems architecture hardware, software, communications
Feedback
Enterprise discretionary and non-discretionary standards/ regulations

TOGAF

- ***The Open Group Architecture Framework (TOGAF)***, which has its origins in the U.S. Department of Defence.
- TOGAF is a framework that can be used to develop the following architecture types:
  - – Business Architecture
  - – Data Architecture
  - – Applications Architecture
  - – Technology Architecture



Business
Process,
activities ..

Data
That must be collected,
organized,
safeguarded,

Applications
Such as custom or off-the-shelf
software tools that run off...

Technology
Such as computer system and
telephone networks.

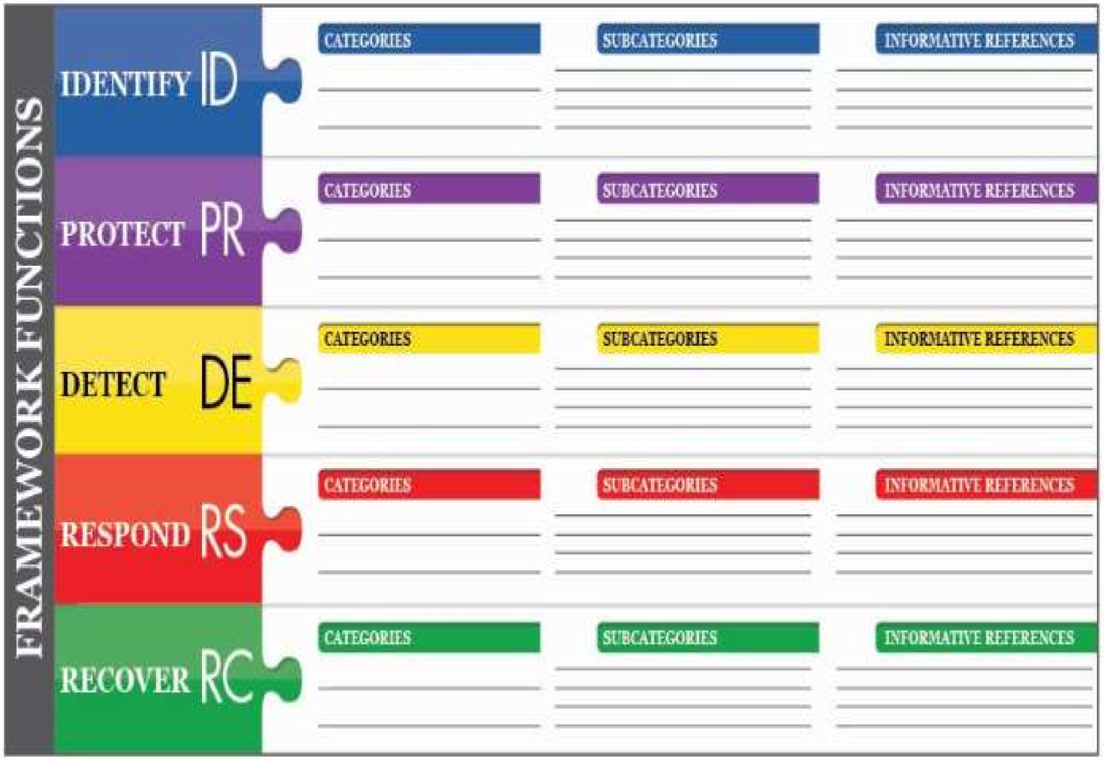
NIST CSF

- *Developed by* The National Institute of Standards and Technology (NIST) in collaboration with industry, academia and government.
- Has industry specific implementations and guides
- Has over 30% adoption in North America
- Currently being used in Japan, Philippines, Italy and other countries
- Has three core components
  - The Framework Core
  - Framework Implementation Tiers
  - Framework Profile

Source : https://nist.gov/cyberframework

The Framework Core

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are *Identify, Protect, Detect, Respond, and Recover*
- **Categories** are 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** are 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.

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.

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, least privilege, network, and systems.

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.

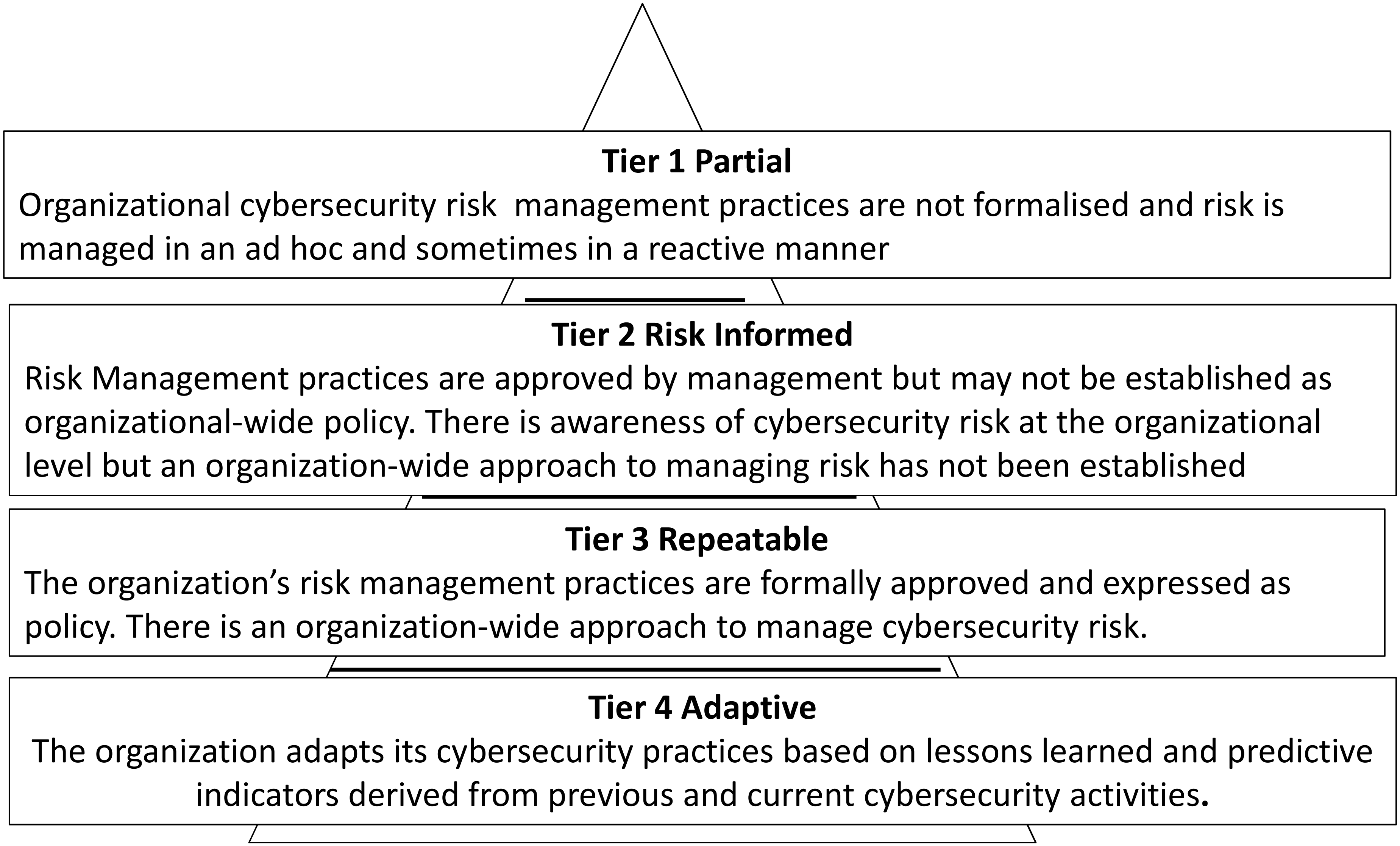
Respond Functions

- **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

Recover 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



Tier 1 Partial

Organizational cybersecurity risk management practices are not formalised and risk is managed in an ad hoc and sometimes in a reactive manner

Tier 2 Risk Informed

Risk Management practices are approved by management but may not be established as organizational-wide policy. There is awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing risk has not been established

Tier 3 Repeatable

The organization’s risk management practices are formally approved and expressed as policy. There is an organization-wide approach to manage cybersecurity risk.

Tier 4 Adaptive

The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.

Implementation Steps

- Step 1 Prioritise and Scope
  - Identify business/mission objectives and strategic priorities
  - Describe cyber security risks
  - Determine organizational components to use Framework
- Step 2 Orient
  - Identify the system assets, requirement, and risk management approaches
  - Determine how to evaluate current risk management and cyber security posture
- Step 3 Create Current Profile
  - Map current cyber security and risk management practices to a Framework implementation Tier

Implementation Steps

- Step 4 Conduct a risk Assessment
  - Identify cyber-security risks
  - Evaluate and analyse risk
  - Identify risk above tolerance
- Step 5 Create a target profile
  - Describe desired cyber-security outcomes
  - Account for unique risks
  - Develop Target Profile
  - Develop Target implementation Tier

Implementation Steps

- Step 6 Determine, analyse and prioritize gaps
  - Compare Current Profile and Target Profile
  - Determine resources to address gaps and create a prioritise Action plan

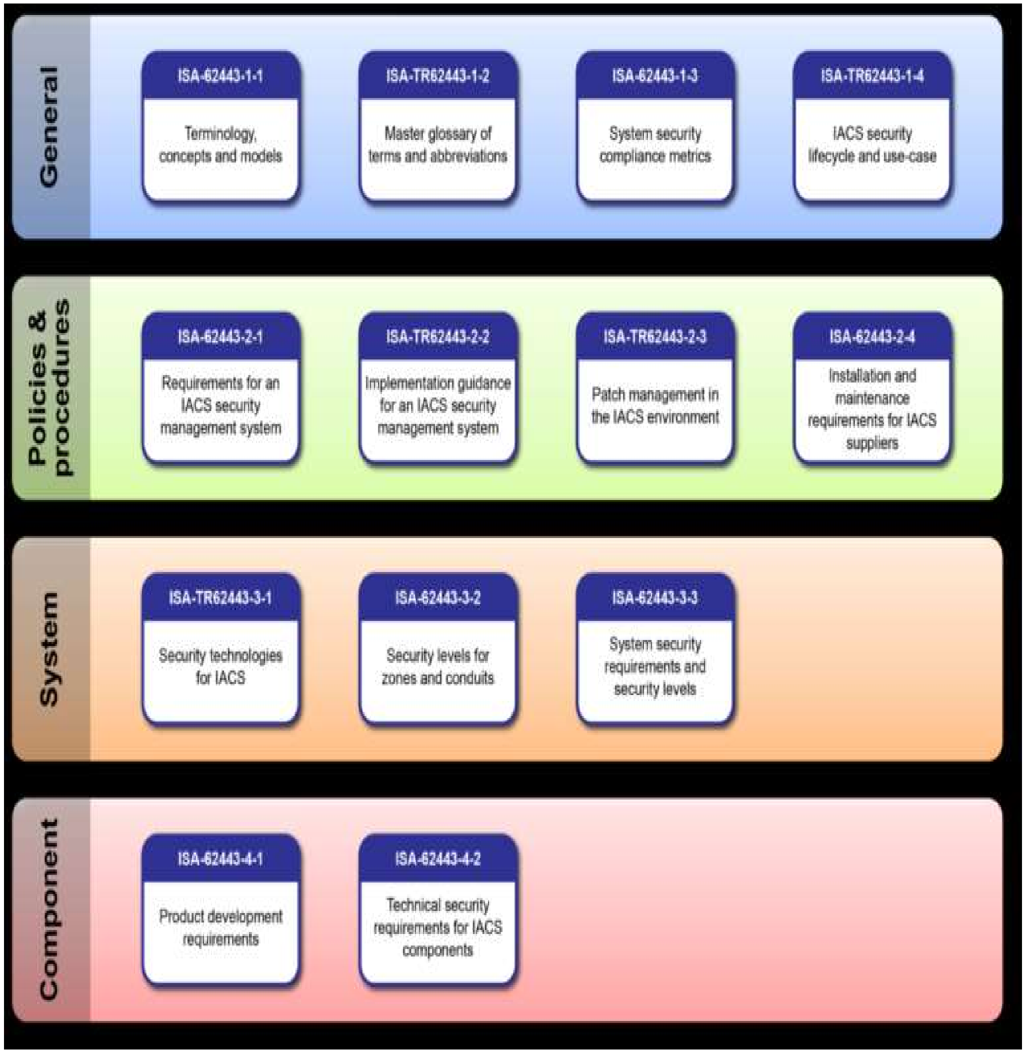
- Step 7 Implement action plan
  - Implement necessary actions
  - Monitor cyber-security practices against Target Profile.

Note:

1. Improve your bit by bit, not everything at once
2. Planning is important but planning by itself provides no actual protection.

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**.



General

ISA-62443-1-1 Terminology, concepts and models

ISA-TR62443-1-2 Master glossary of terms and abbreviations

ISA-62443-1-3 System security compliance metrics

ISA-TR62443-1-4 IACS security lifecycle and use-case

Policies & procedures

ISA-62443-2-1 Requirements for an IACS security management system

ISA-TR62443-2-2 Implementation guidance for an IACS security management system

ISA-TR62443-2-3 Patch management in the IACS environment

ISA-62443-2-4 Installation and maintenance requirements for IACS suppliers

System

ISA-TR62443-3-1 Security technologies for IACS

ISA-62443-3-2 Security levels for zones and conduits

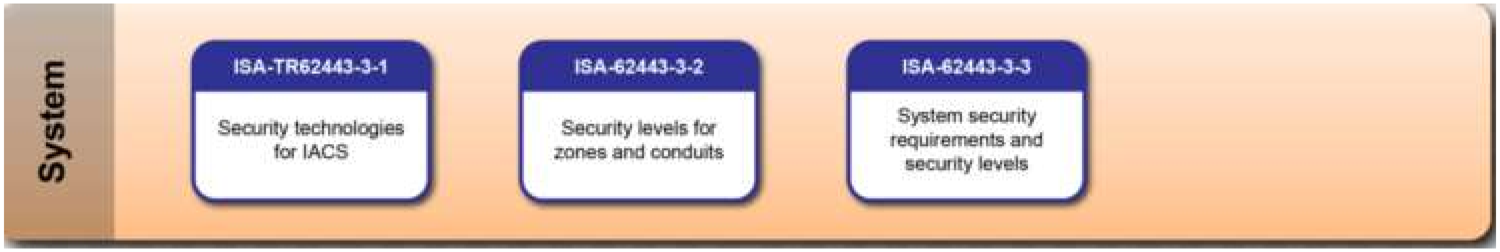
ISA-62443-3-3 System security requirements and security levels

Component

ISA-62443-4-1 Product development requirements

ISA-62443-4-2 Technical security requirements for IACS components

ISA/IEC 62443 – System Requirement



System

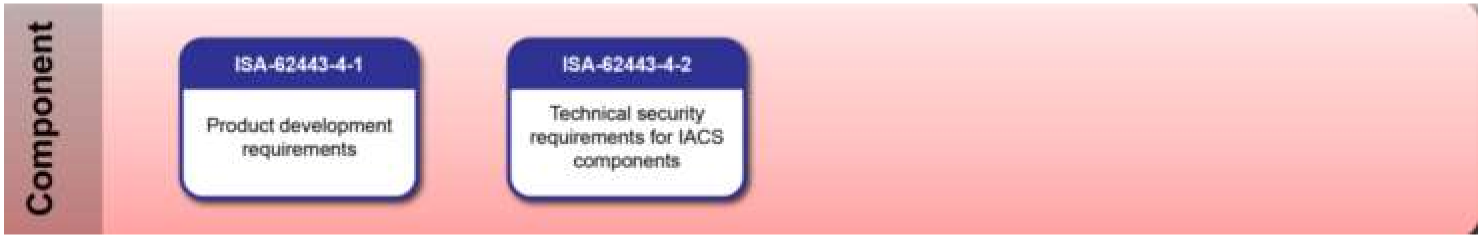
ISA-TR62443-3-1
Security technologies for IACS

ISA-62443-3-2
Security levels for zones and conduits

ISA-62443-3-3
System security requirements and security levels

- 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.
- third document describes general system security requirements such as authentication, data confidentiality and system integrity, etc.

ISA/IEC 62443 – Component Requirement


Component
ISA-62443-4-1
Product development requirements
ISA-62443-4-2
Technical security requirements for IACS components

- 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.

Source https://www.ncsc.gov.uk/collection/caf/introduction

NCSC CAF Guidance

- **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

Source https://www.ncsc.gov.uk/collection/caf/introduction

CAF - Principles and guidance

- **Managing security risk**
  - Governance
  - Risk management
  - Asset management
  - Supply chain

Source https://www.ncsc.gov.uk/collection/caf/introduction

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

Source https://www.ncsc.gov.uk/collection/caf/introduction

CAF - Principles and guidance

- **Detecting cyber security events**
  - Security monitoring
  - Proactive security event discovery
- **Minimising the impact of cyber security incidents**
  - Response and recovery planning
  - Lessons learned

Source https://www.ncsc.gov.uk/collection/caf/introduction

Discussion

Sam has just been hired as the new security officer for a pharmaceutical company. The company has experienced many data breaches and has charged Sam with ensuring that the company is better protected. The company currently has the following classifications in place: public, confidential, and secret. There is a data classification policy that outlines the classification scheme and the definitions for each classification, but there is no supporting documentation the technical staff can follow to know how to meet these goals. The company has no data loss prevention controls in place and only conducts basic security awareness training once a year. Talking to the business unit managers, he finds out that only half of them even know where the company's policies are located and none of them know their responsibilities pertaining to classifying data.

1. By hiring Sam what the company has successfully accomplished ? (hint : think of the type of control)
2. What should Sam address first in this situation?
3. Among the Security Framework discussed today, which one should Sam use to improve the security of the company? (Compare and contrast existing frameworks)