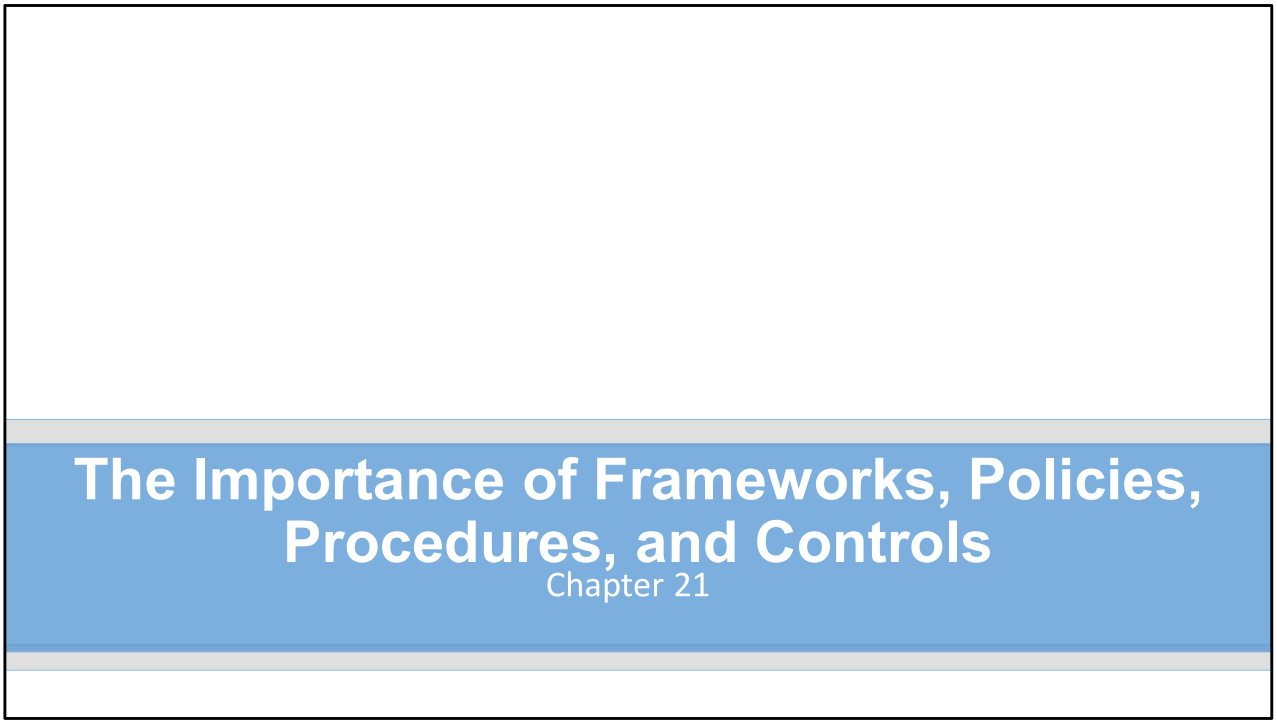


The Importance of Frameworks, Policies, Procedures, and Controls

Chapter 21

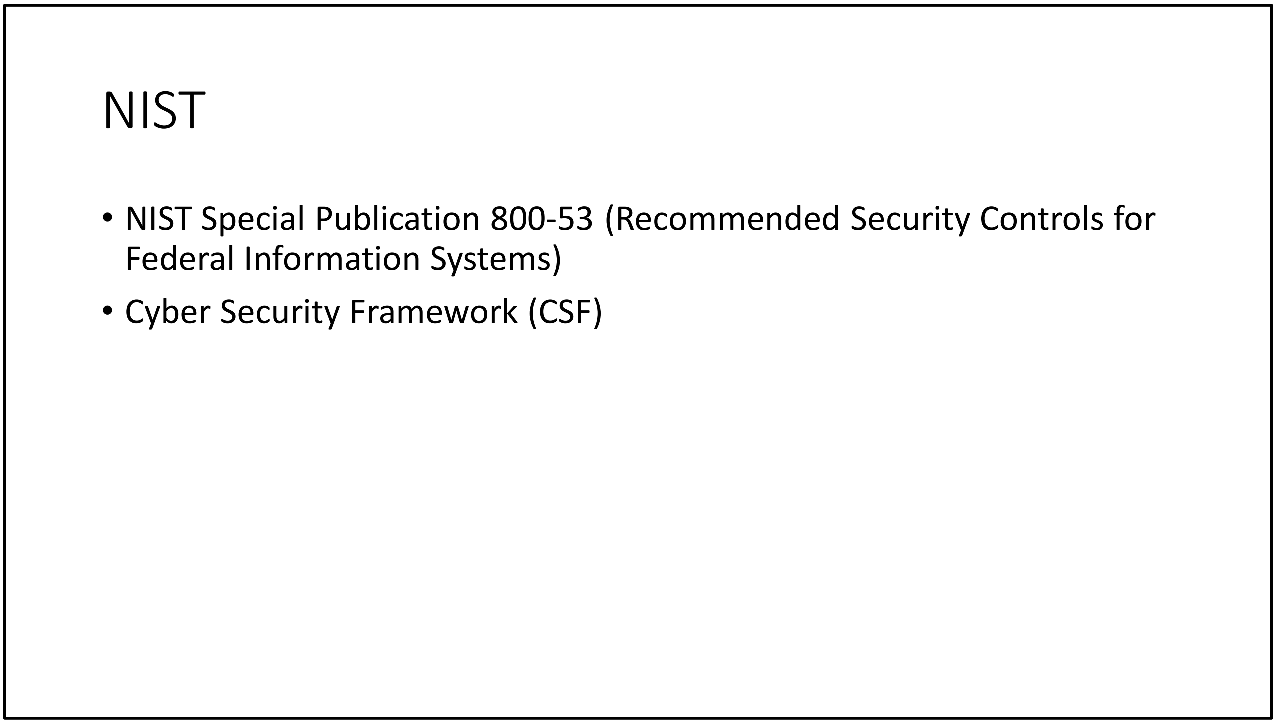
Episode 21.01

Frameworks

Objective: 5.3 Explain the importance of frameworks, policies, procedures, and controls.

• Frameworks

- Risk-based
- Prescriptive

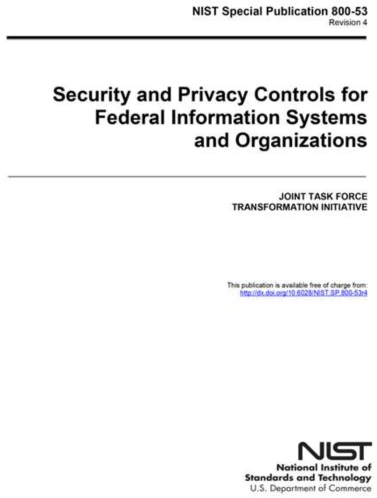


NIST

- NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems)
- Cyber Security Framework (CSF)

Security Guidelines

- NIST Special Publication 800-53
  - AKA - Recommended Security Controls for Federal Information Systems
  - Controls to be compliant with Federal Information Processing Standards (FIPS)
  - FIPS is used in government or military data processing



NIST Special Publication 800-53
Revision 4

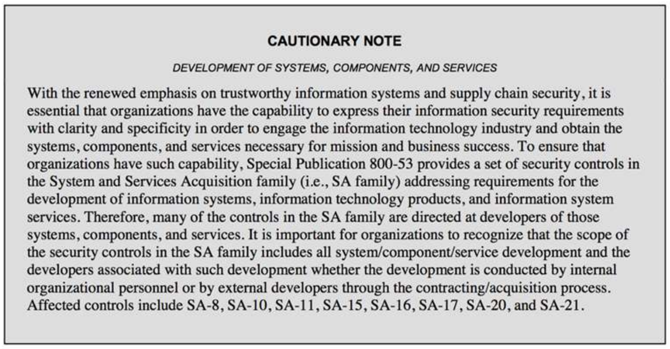
Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

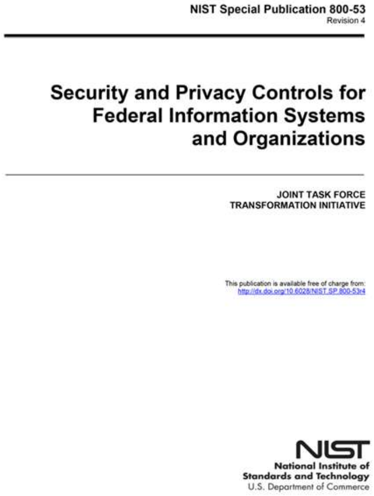
NIST Special Publication 800-53



CAUTIONARY NOTE

DEVELOPMENT OF SYSTEMS, COMPONENTS, AND SERVICES

With the renewed emphasis on trustworthy information systems and supply chain security, it is essential that organizations have the capability to express their information security requirements with clarity and specificity in order to engage the information technology industry and obtain the systems, components, and services necessary for mission and business success. To ensure that organizations have such capability, Special Publication 800-53 provides a set of security controls in the System and Services Acquisition family (i.e., SA family) addressing requirements for the development of information systems, information technology products, and information system services. Therefore, many of the controls in the SA family are directed at developers of those systems, components, and services. It is important for organizations to recognize that the scope of the security controls in the SA family includes all system/component/service development and the developers associated with such development whether the development is conducted by internal organizational personnel or by external developers through the contracting/acquisition process. Affected controls include SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, and SA-21.



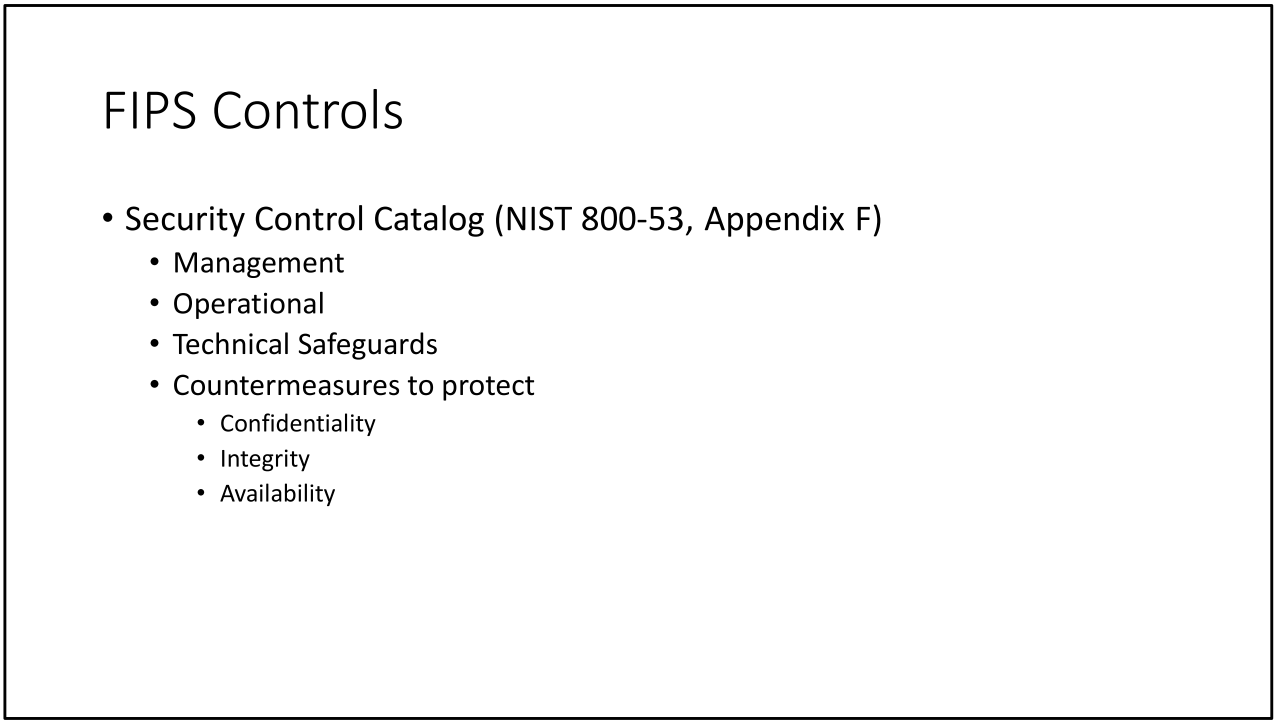
NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

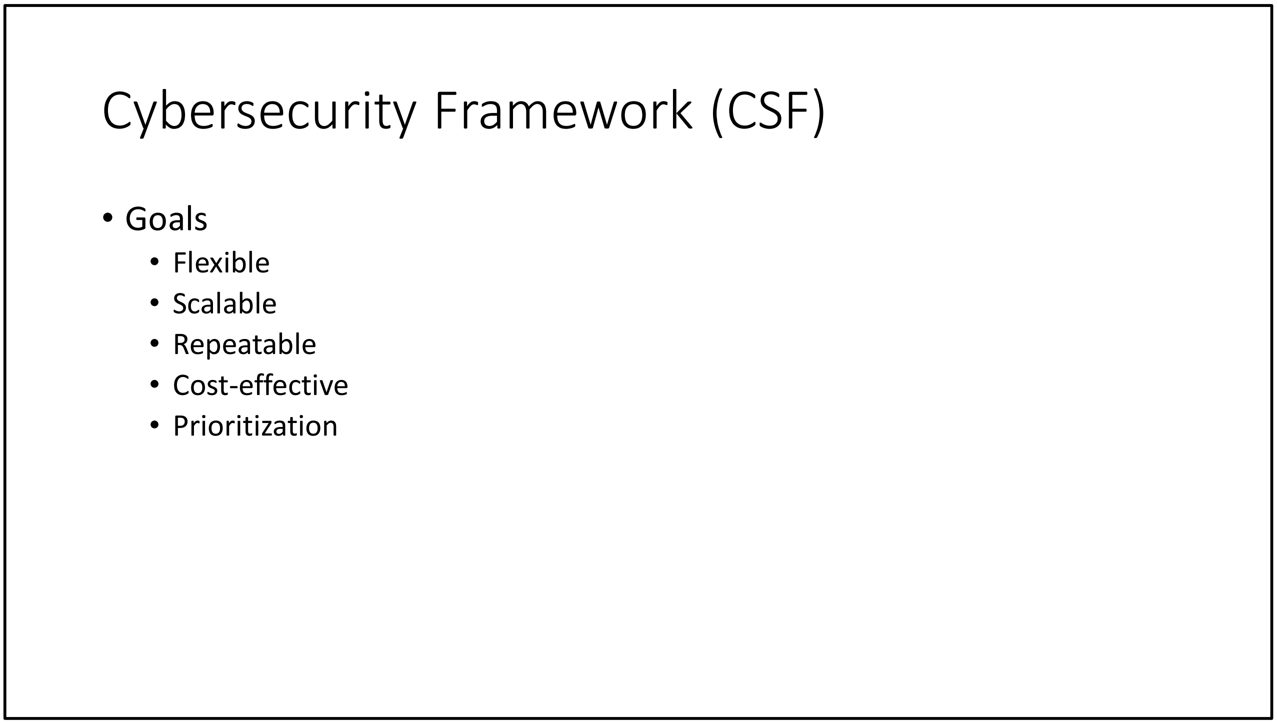
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



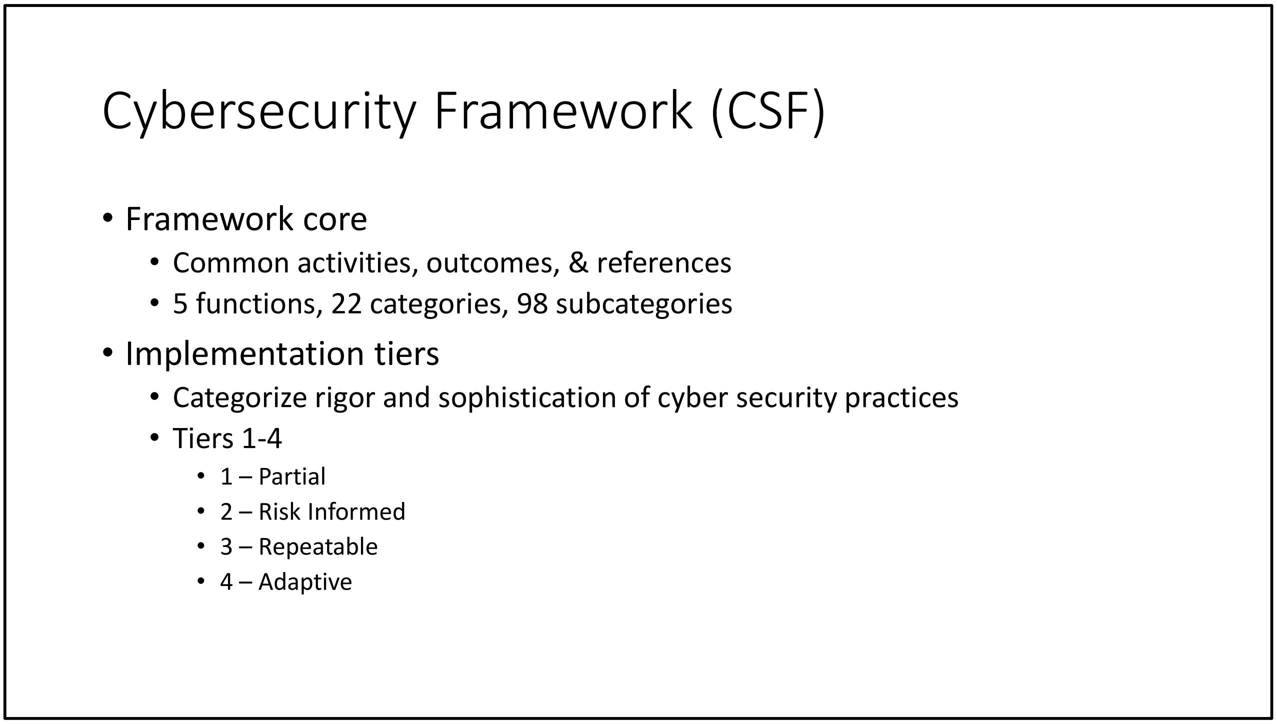
FIPS Controls

- Security Control Catalog (NIST 800-53, Appendix F)
  - Management
  - Operational
  - Technical Safeguards
  - Countermeasures to protect
    - Confidentiality
    - Integrity
    - Availability



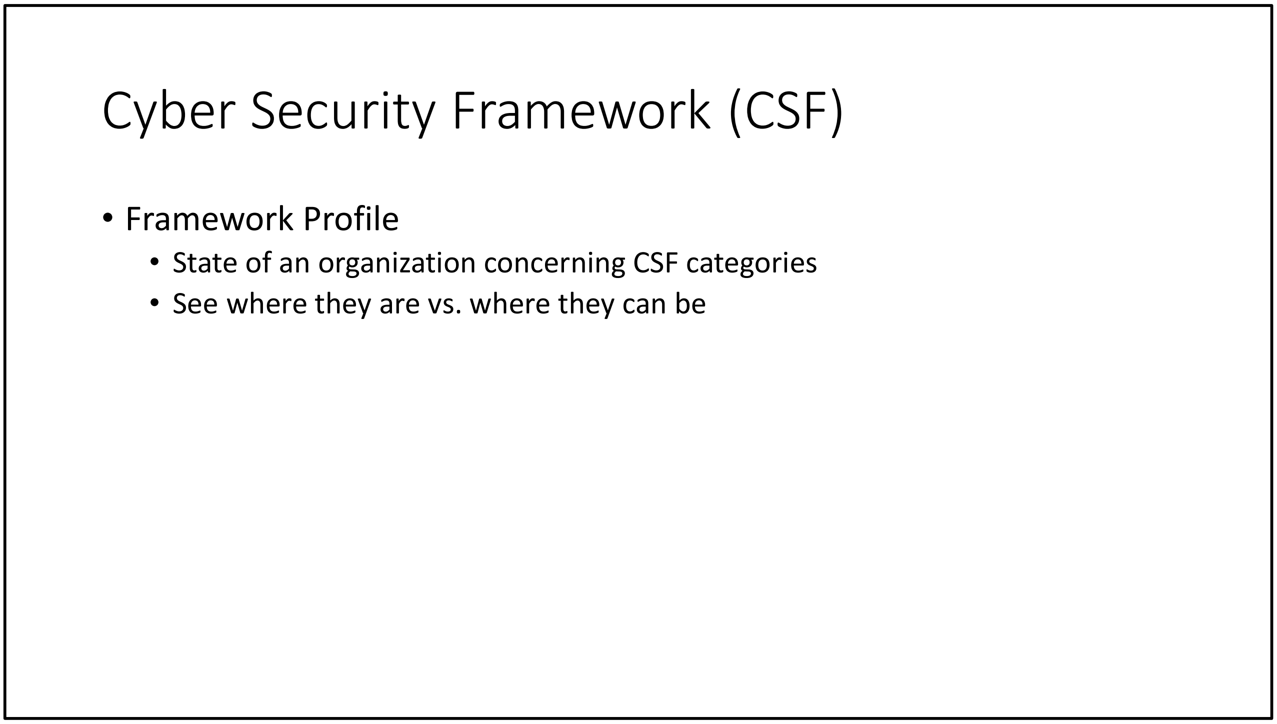
Cybersecurity Framework (CSF)

- Goals
  - Flexible
  - Scalable
  - Repeatable
  - Cost-effective
  - Prioritization



Cybersecurity Framework (CSF)

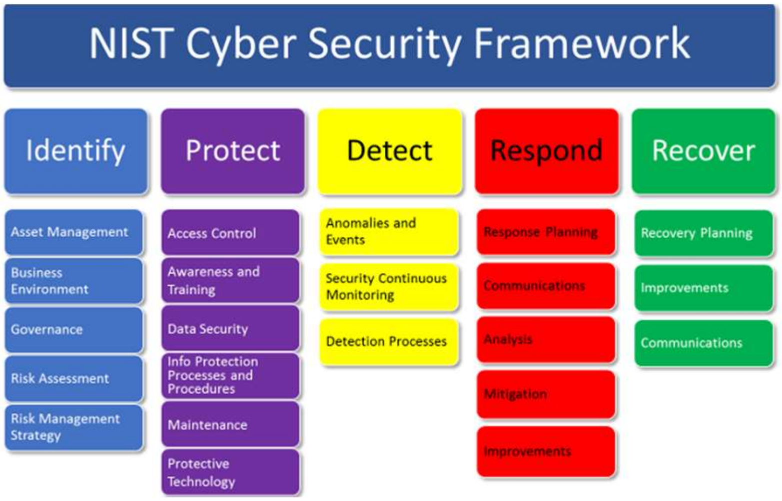
- Framework core
  - Common activities, outcomes, & references
  - 5 functions, 22 categories, 98 subcategories
- Implementation tiers
  - Categorize rigor and sophistication of cyber security practices
  - Tiers 1-4
    - 1 – Partial
    - 2 – Risk Informed
    - 3 – Repeatable
    - 4 – Adaptive



Cyber Security Framework (CSF)

- Framework Profile
  - State of an organization concerning CSF categories
  - See where they are vs. where they can be

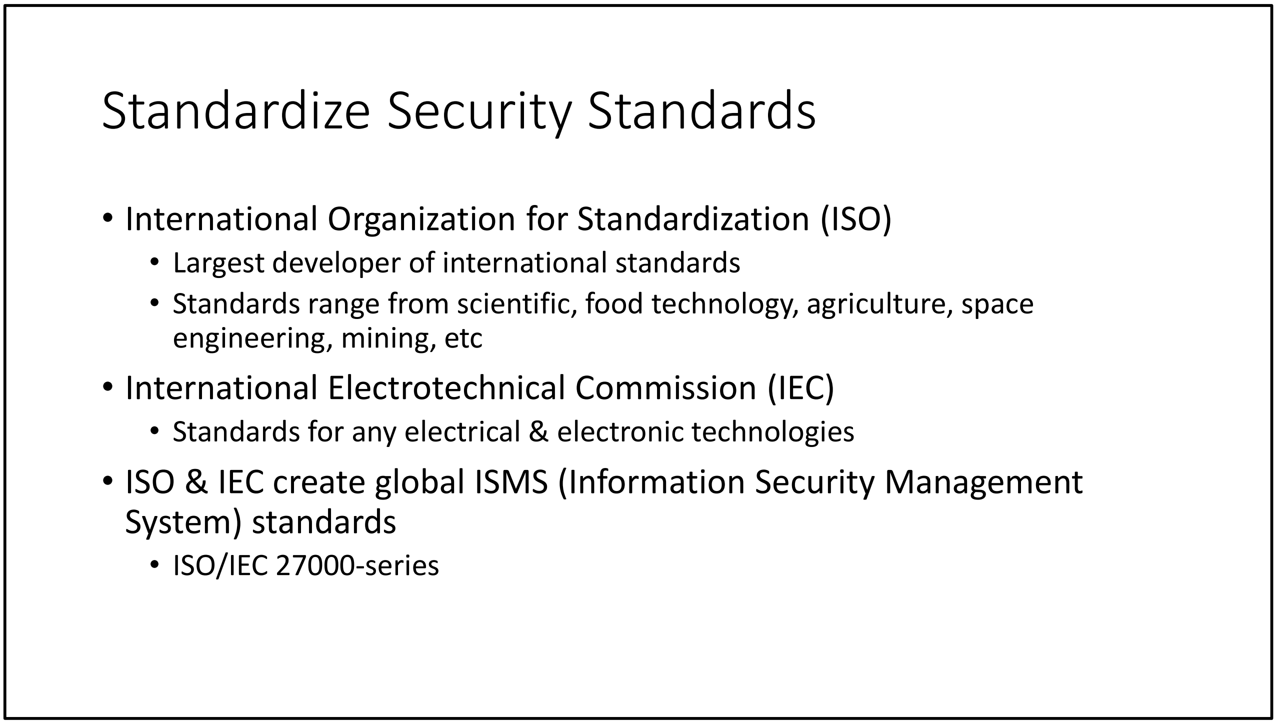
Framework Core



NIST Cyber Security Framework

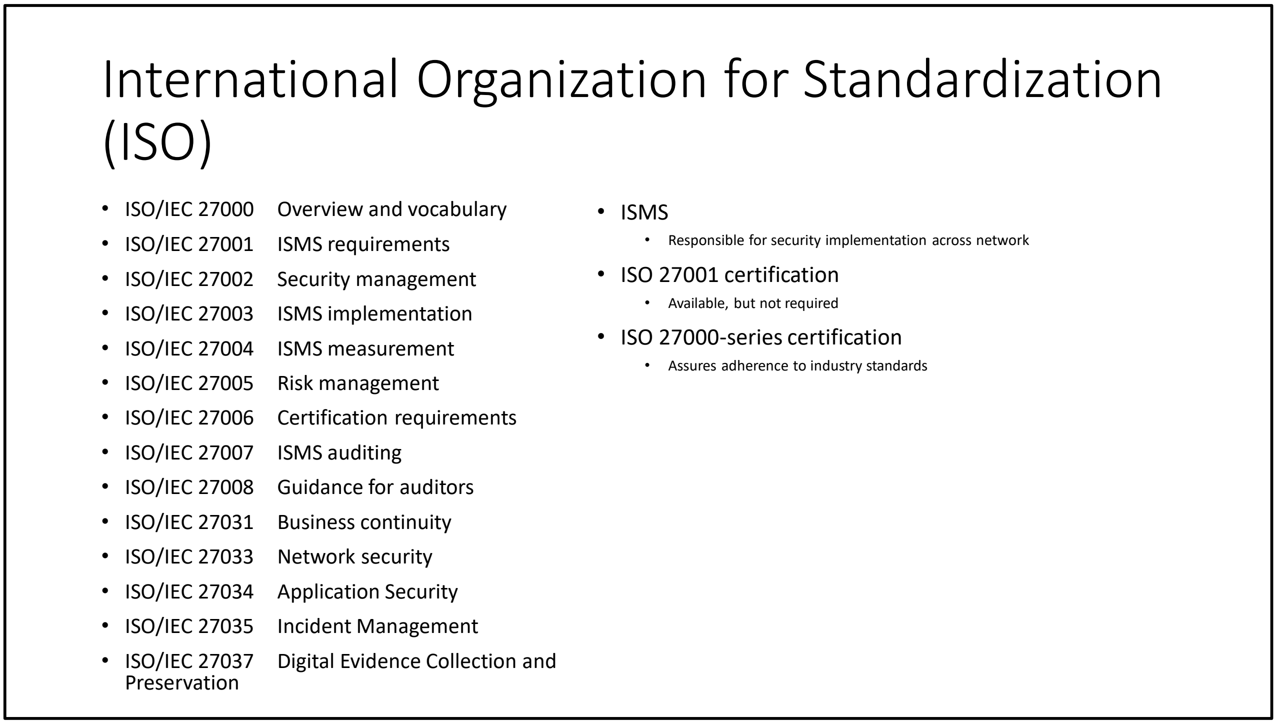
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

http://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html



Standardize Security Standards

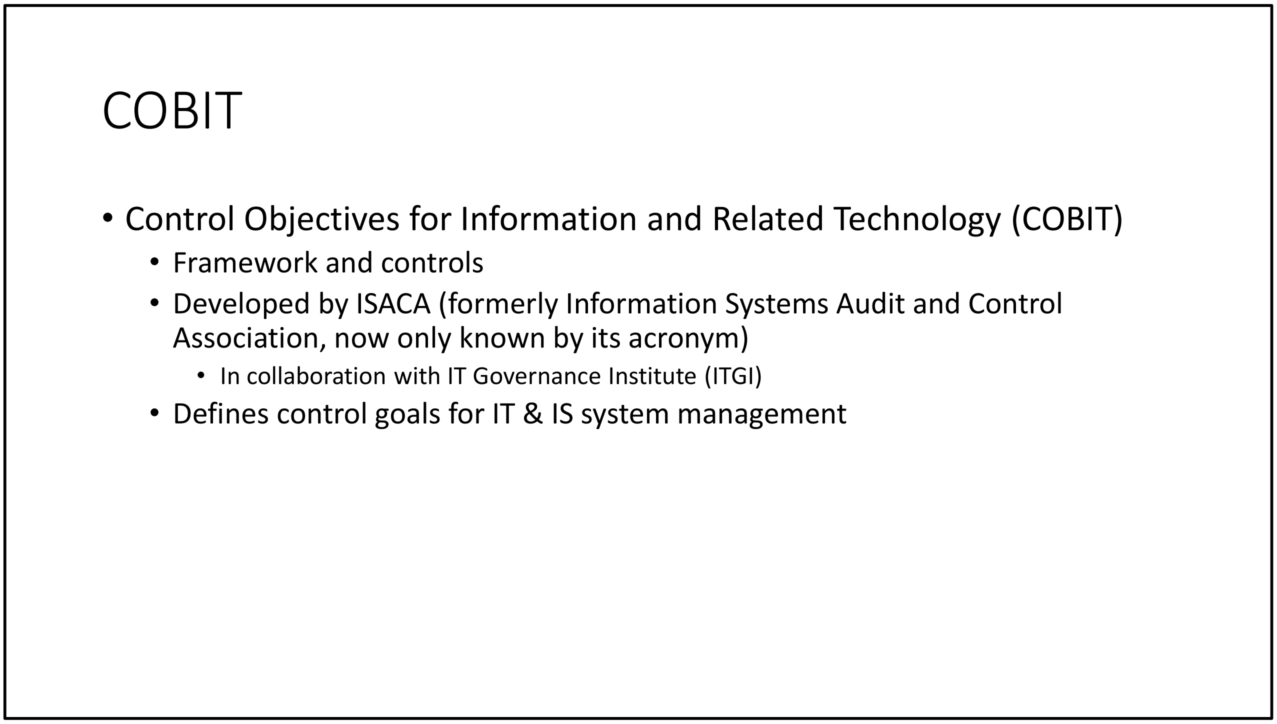
- International Organization for Standardization (ISO)
  - Largest developer of international standards
  - Standards range from scientific, food technology, agriculture, space engineering, mining, etc
- International Electrotechnical Commission (IEC)
  - Standards for any electrical & electronic technologies
- ISO & IEC create global ISMS (Information Security Management System) standards
  - ISO/IEC 27000-series



International Organization for Standardization (ISO)

- ISO/IEC 27000 Overview and vocabulary
- ISO/IEC 27001 ISMS requirements
- ISO/IEC 27002 Security management
- ISO/IEC 27003 ISMS implementation
- ISO/IEC 27004 ISMS measurement
- ISO/IEC 27005 Risk management
- ISO/IEC 27006 Certification requirements
- ISO/IEC 27007 ISMS auditing
- ISO/IEC 27008 Guidance for auditors
- ISO/IEC 27031 Business continuity
- ISO/IEC 27033 Network security
- ISO/IEC 27034 Application Security
- ISO/IEC 27035 Incident Management
- ISO/IEC 27037 Digital Evidence Collection and Preservation

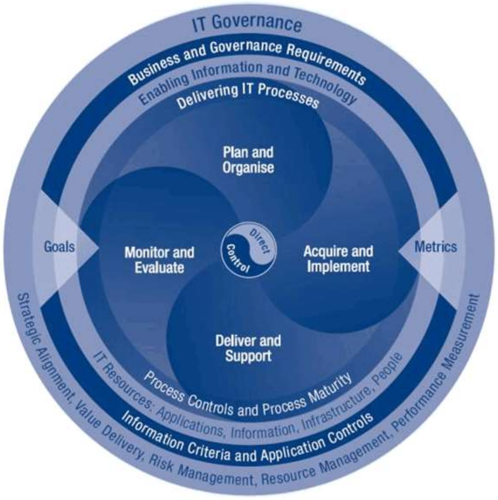
- ISMS
  - Responsible for security implementation across network
- ISO 27001 certification
  - Available, but not required
- ISO 27000-series certification
  - Assures adherence to industry standards



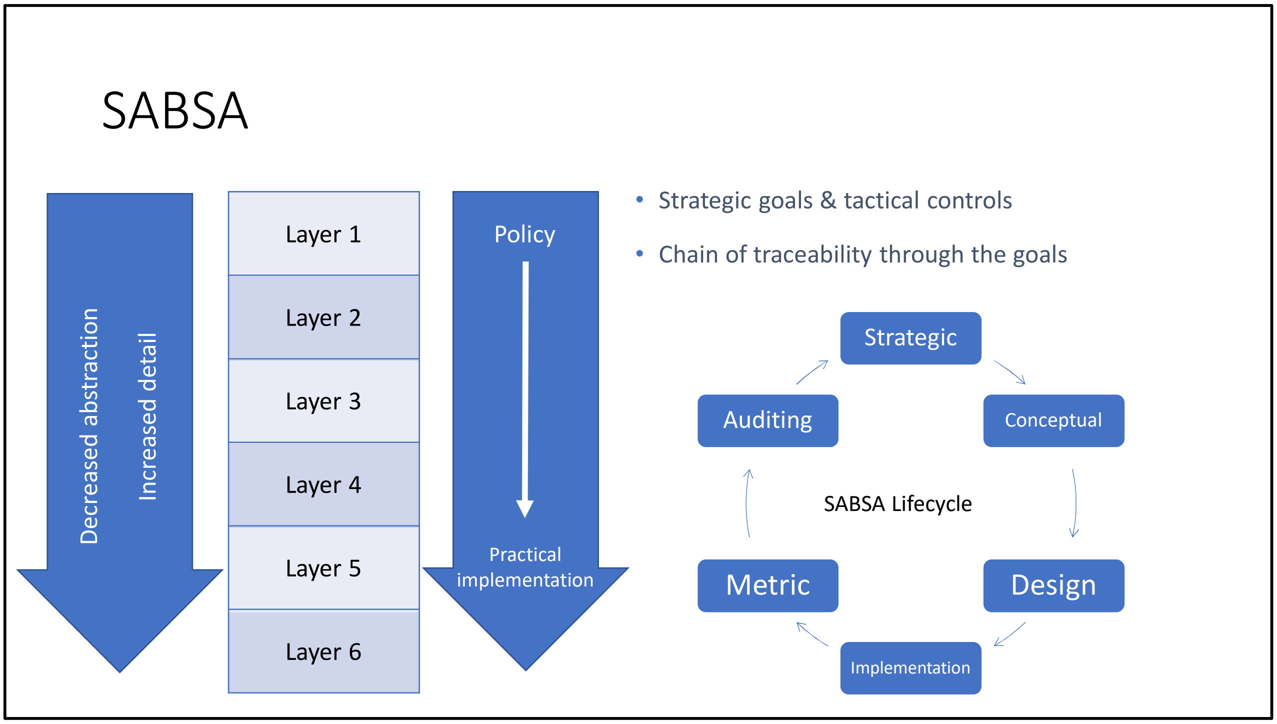
COBIT

- Control Objectives for Information and Related Technology (COBIT)
  - Framework and controls
  - Developed by ISACA (formerly Information Systems Audit and Control Association, now only known by its acronym)
    - In collaboration with IT Governance Institute (ITGI)
  - Defines control goals for IT & IS system management

Control Objectives for Information and Related Technology (COBIT)


IT Governance
Business and Governance Requirements
Enabling Information and Technology
Delivering IT Processes
Plan and Organise
Goals
Monitor and Evaluate
Direct
Control
Acquire and Implement
Metrics
Deliver and Support
Process Controls and Process Maturity
IT Resources: Applications, Information, Infrastructure, People
Information Criteria and Application Controls
Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement

http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx



SABSA

Decreased abstraction

Increased detail

Layer 1

Layer 2

Layer 3

Layer 4

Layer 5

Layer 6

Policy

Practical implementation

- Strategic goals & tactical controls
- Chain of traceability through the goals

SABSA Lifecycle

Strategic

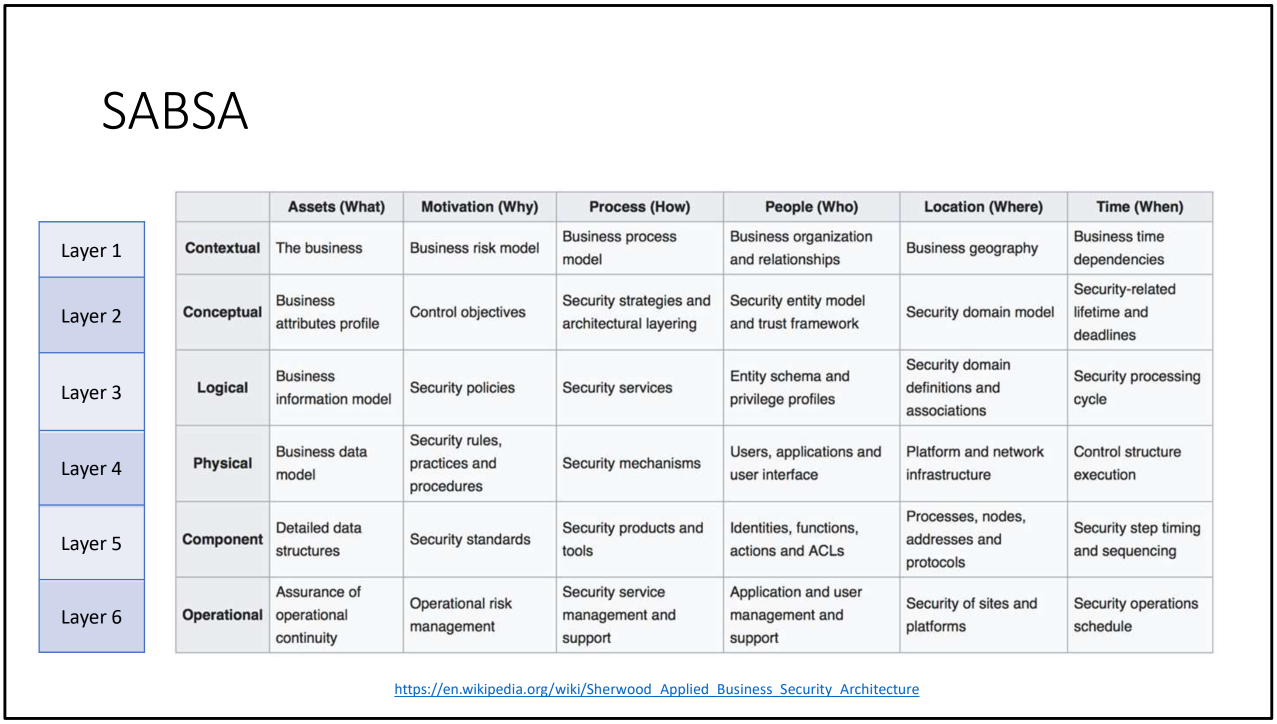
Conceptual

Design

Implementation

Metric

Auditing



SABSA

Layer 1

Layer 2

Layer 3

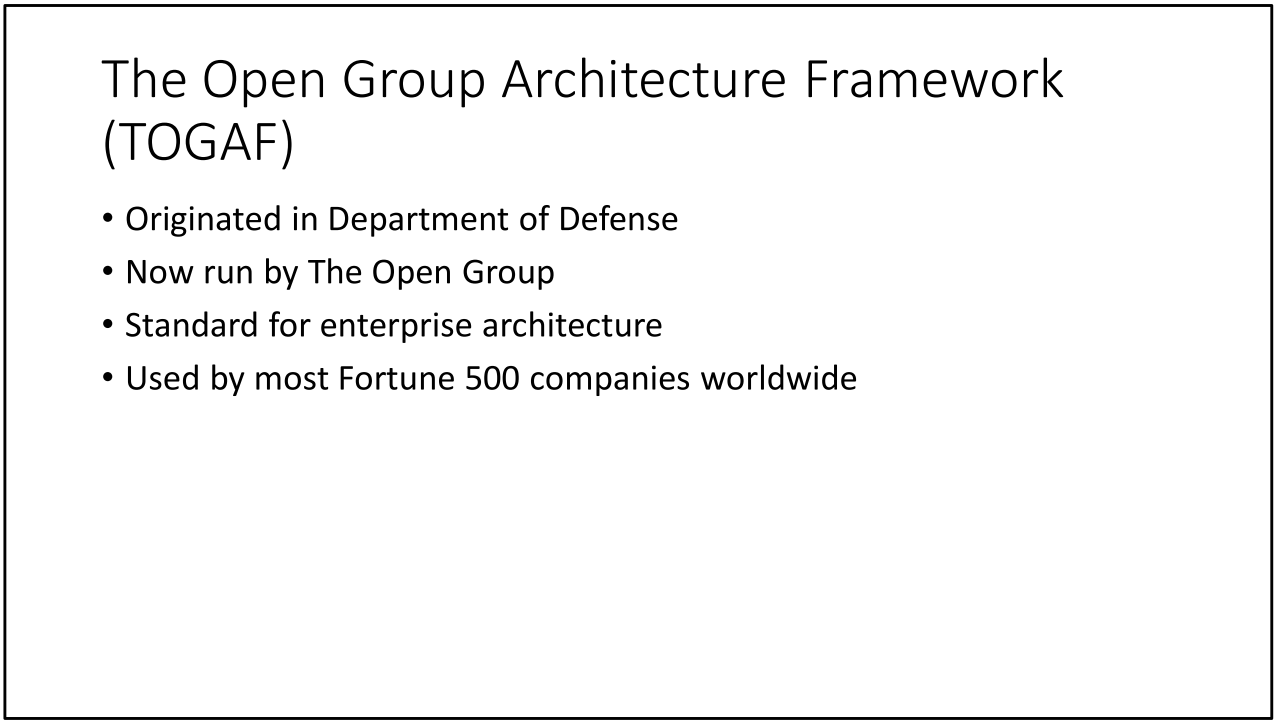
Layer 4

Layer 5

Layer 6

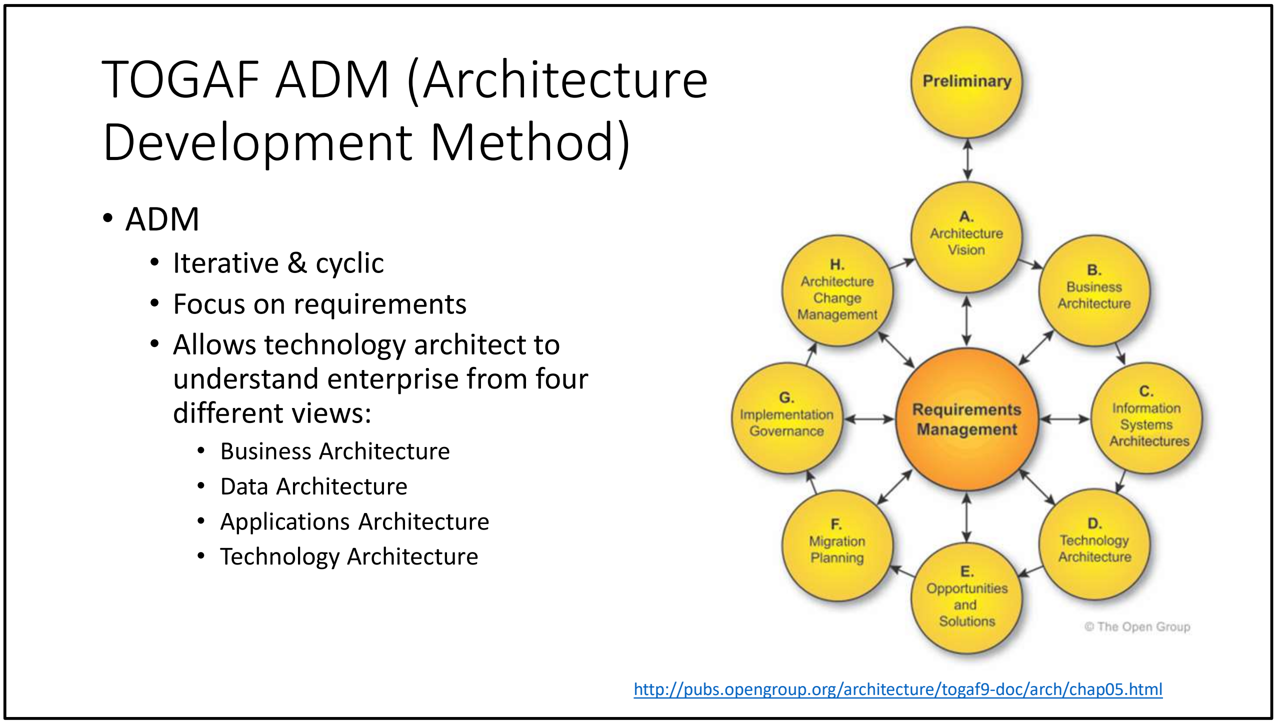
	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The business	Business risk model	Business process model	Business organization and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetime and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices and procedures	Security mechanisms	Users, applications and user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions and ACLs	Processes, nodes, addresses and protocols	Security step timing and sequencing
Operational	Assurance of operational continuity	Operational risk management	Security service management and support	Application and user management and support	Security of sites and platforms	Security operations schedule

https://en.wikipedia.org/wiki/Sherwood_Applied_Business_Security_Architecture



The Open Group Architecture Framework (TOGAF)

- Originated in Department of Defense
- Now run by The Open Group
- Standard for enterprise architecture
- Used by most Fortune 500 companies worldwide

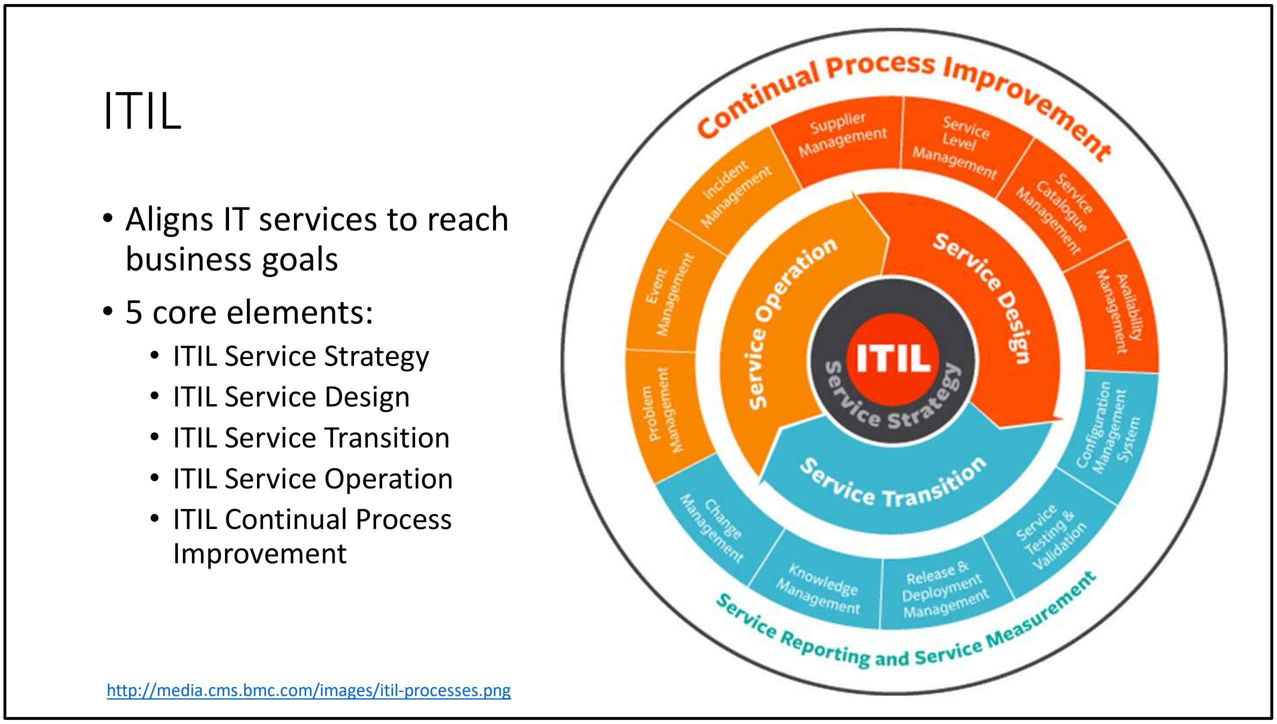


TOGAF ADM (Architecture Development Method)

- ADM
  - Iterative & cyclic
  - Focus on requirements
  - Allows technology architect to understand enterprise from four different views:
    - Business Architecture
    - Data Architecture
    - Applications Architecture
    - Technology Architecture

Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management
© The Open Group

http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap05.html



ITIL

- Aligns IT services to reach business goals
- 5 core elements:
  - ITIL Service Strategy
  - ITIL Service Design
  - ITIL Service Transition
  - ITIL Service Operation
  - ITIL Continual Process Improvement

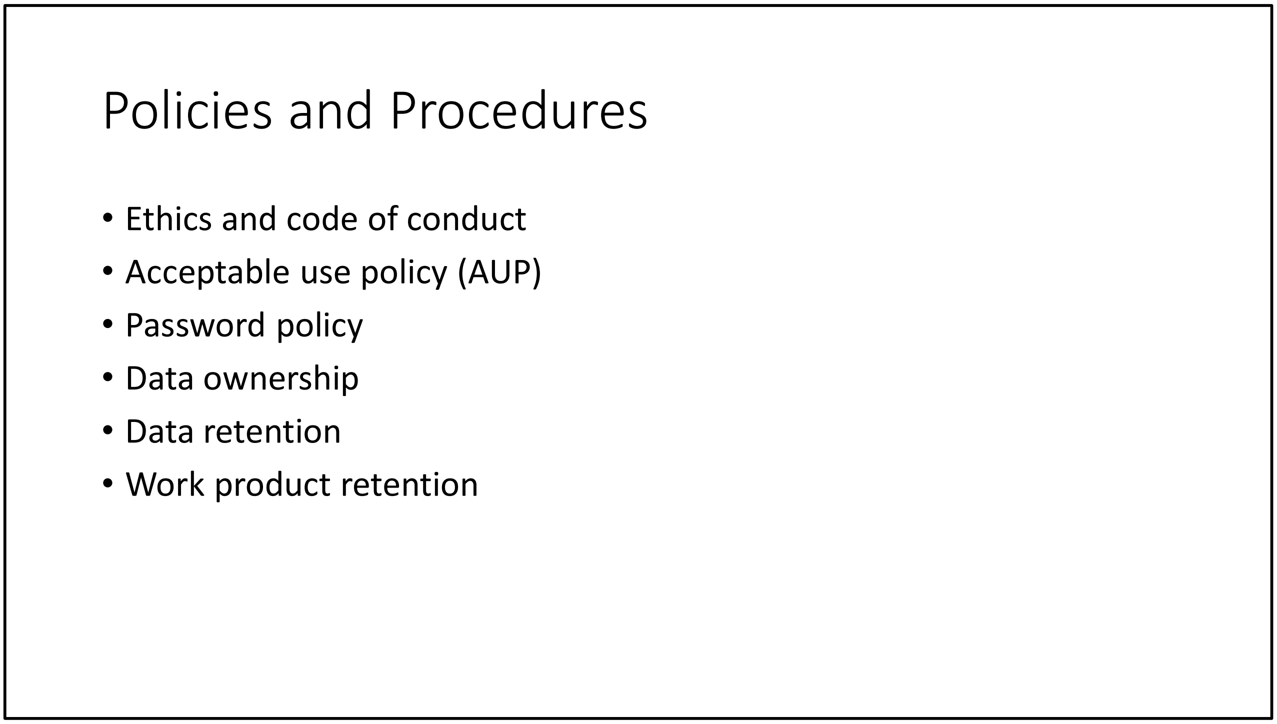
http://media.cms.bmc.com/images/itil-processes.png

Episode 21.02

Policies and Procedures

Objective: 5.3 Explain the importance of frameworks, policies, procedures, and controls.

• Policies and procedures
- Code of conduct/ethics
- Acceptable use policy (AUP)
- Password policy
- Data ownership
- Data retention
- Account management
- Continuous monitoring
- Work product retention



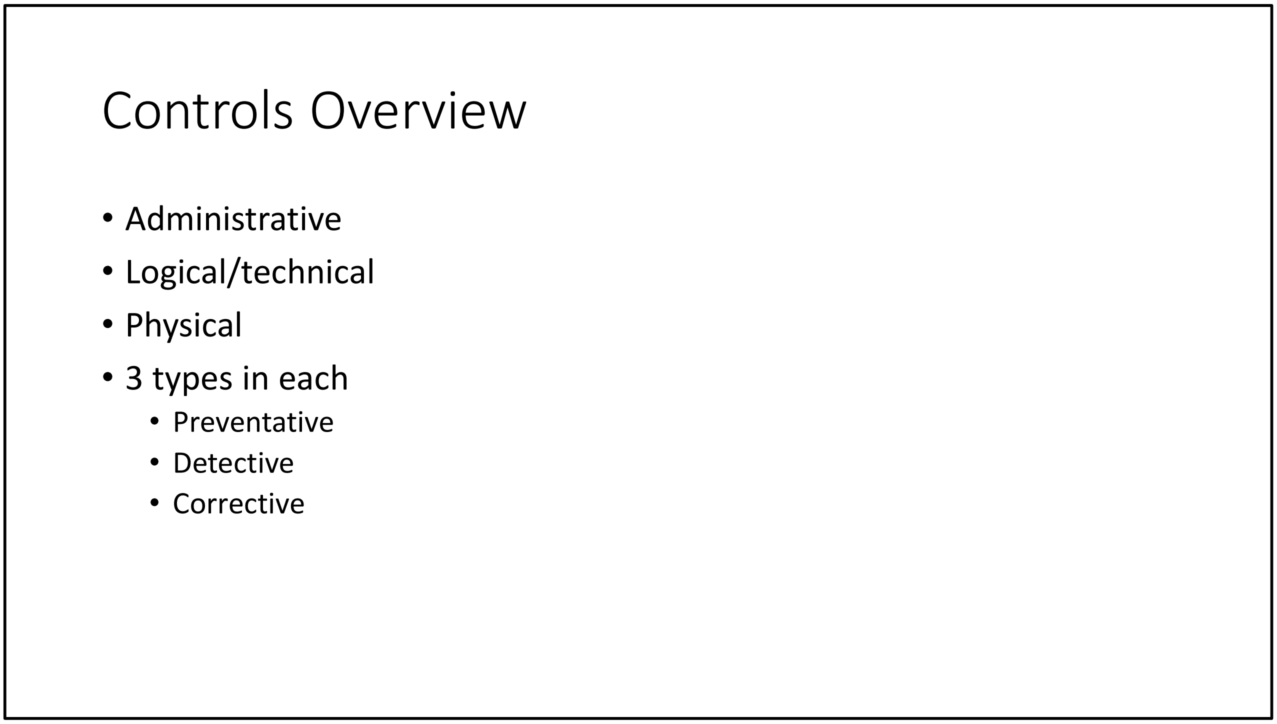
Policies and Procedures

- Ethics and code of conduct
- Acceptable use policy (AUP)
- Password policy
- Data ownership
- Data retention
- Work product retention

Episode 21.03

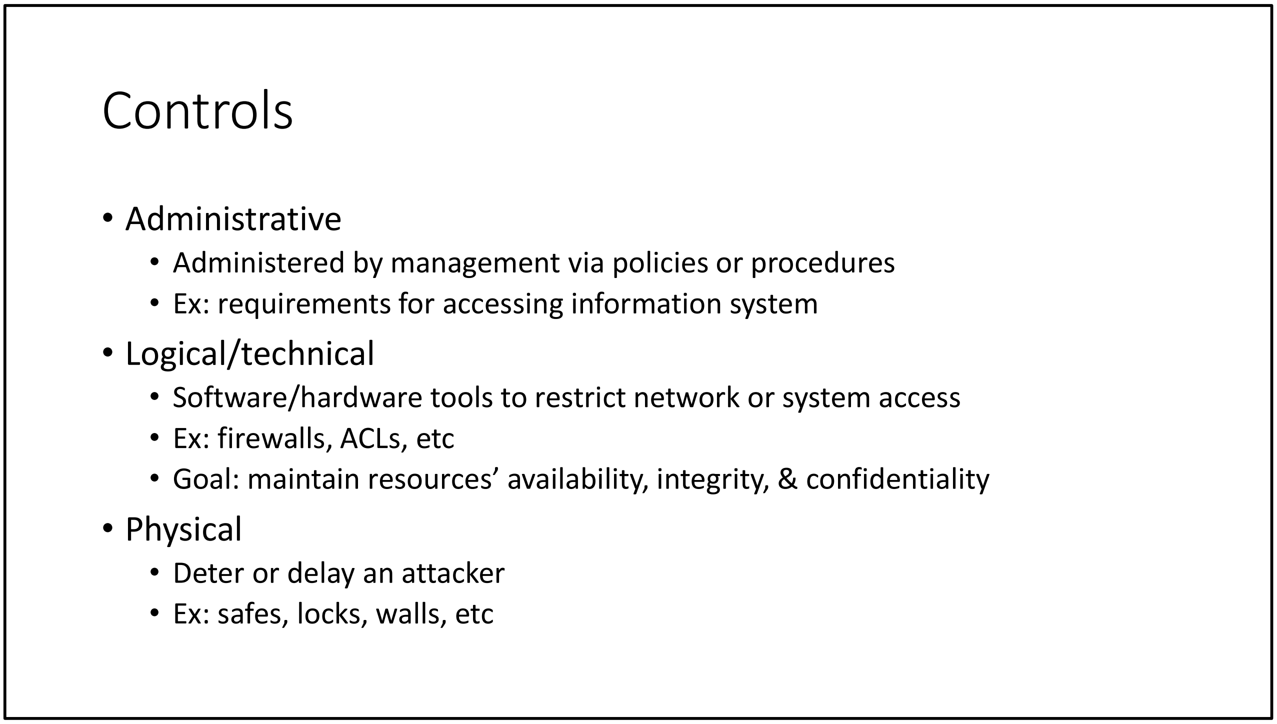
Controls and Procedures

Objective: 5.3 Explain the importance of frameworks, policies, procedures, and controls.
• Control types
- Managerial
- Operational
- Technical
- Preventative
- Detective
- Responsive
- Corrective



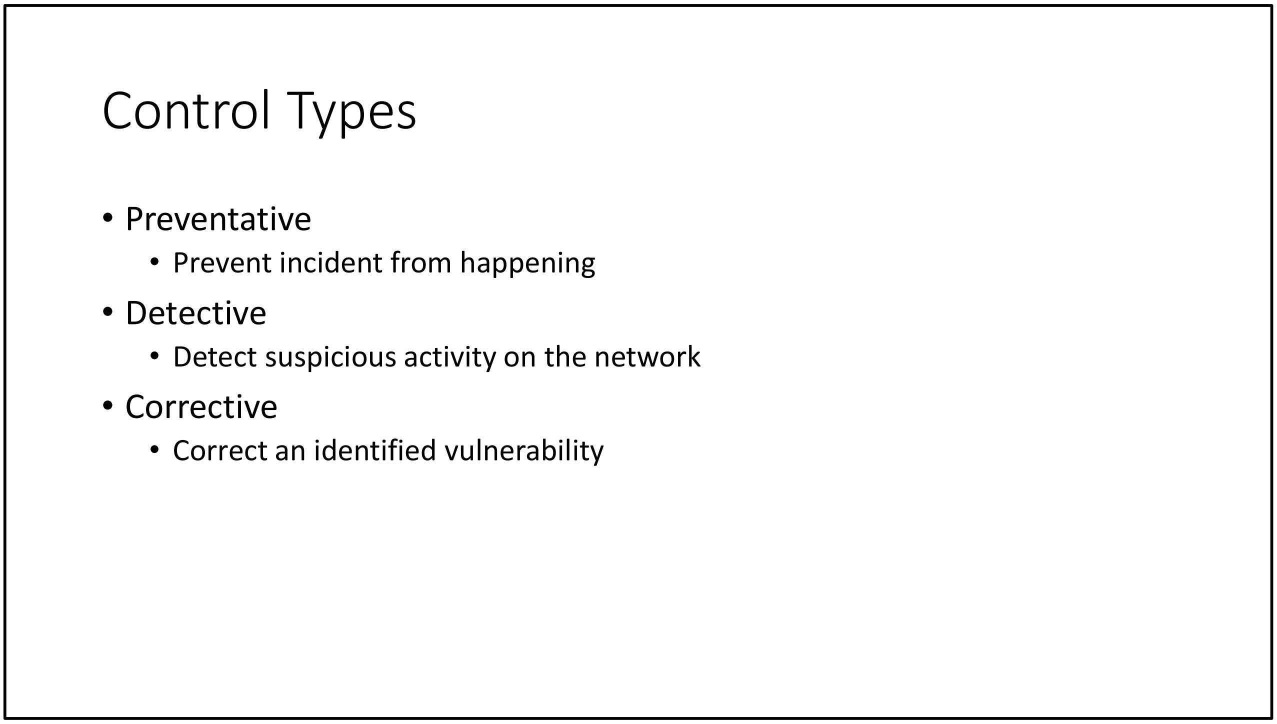
Controls Overview

- Administrative
- Logical/technical
- Physical
- 3 types in each
  - Preventative
  - Detective
  - Corrective



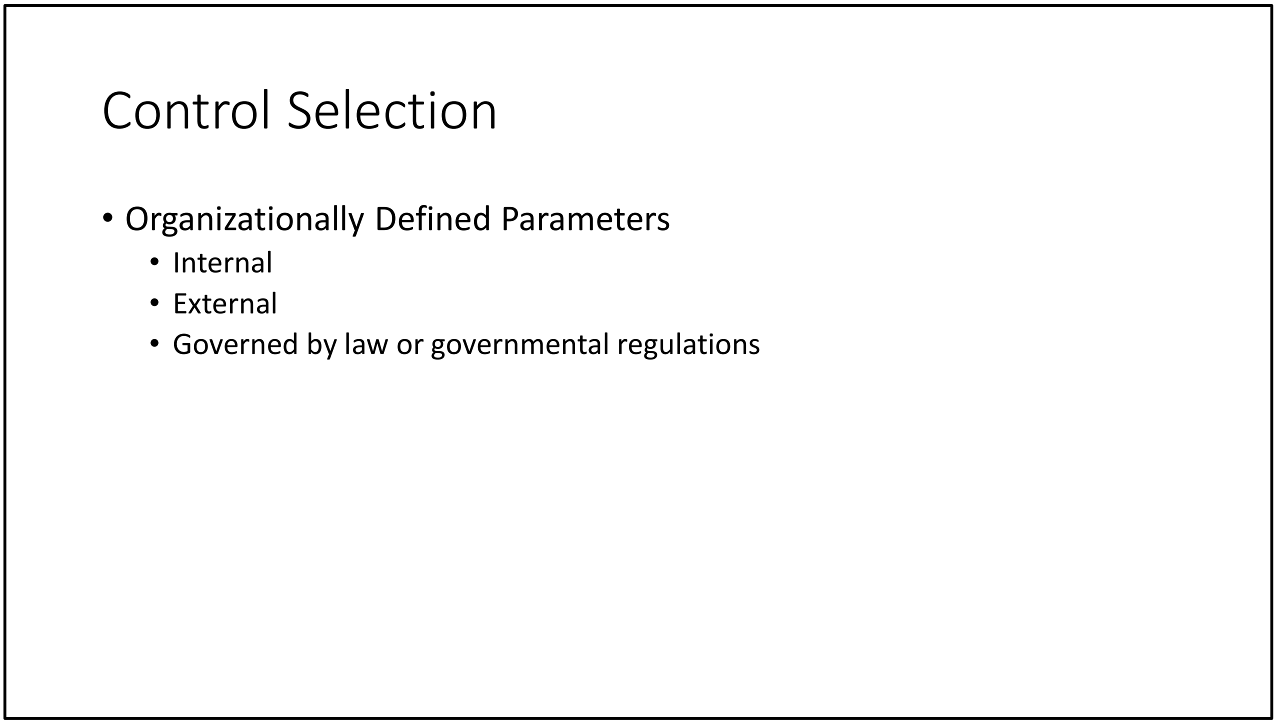
Controls

- Administrative
  - Administered by management via policies or procedures
  - Ex: requirements for accessing information system
- Logical/technical
  - Software/hardware tools to restrict network or system access
  - Ex: firewalls, ACLs, etc
  - Goal: maintain resources’ availability, integrity, & confidentiality
- Physical
  - Deter or delay an attacker
  - Ex: safes, locks, walls, etc



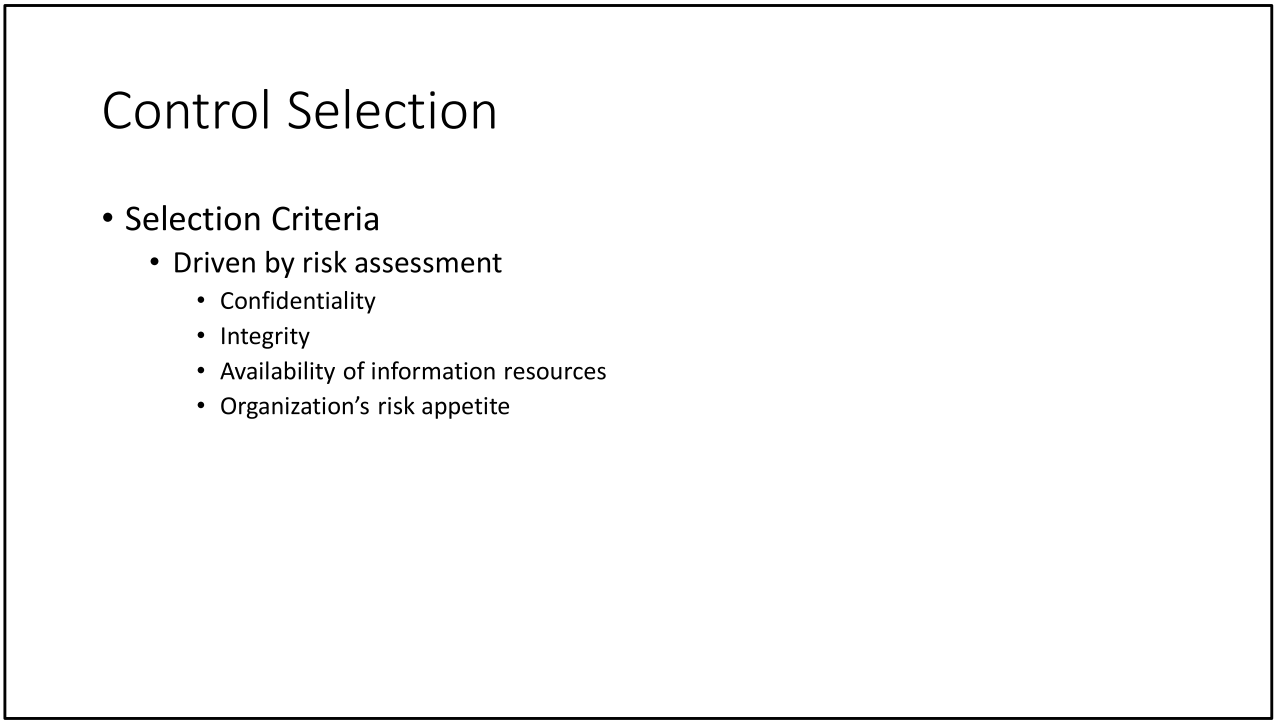
Control Types

- Preventative
  - Prevent incident from happening
- Detective
  - Detect suspicious activity on the network
- Corrective
  - Correct an identified vulnerability



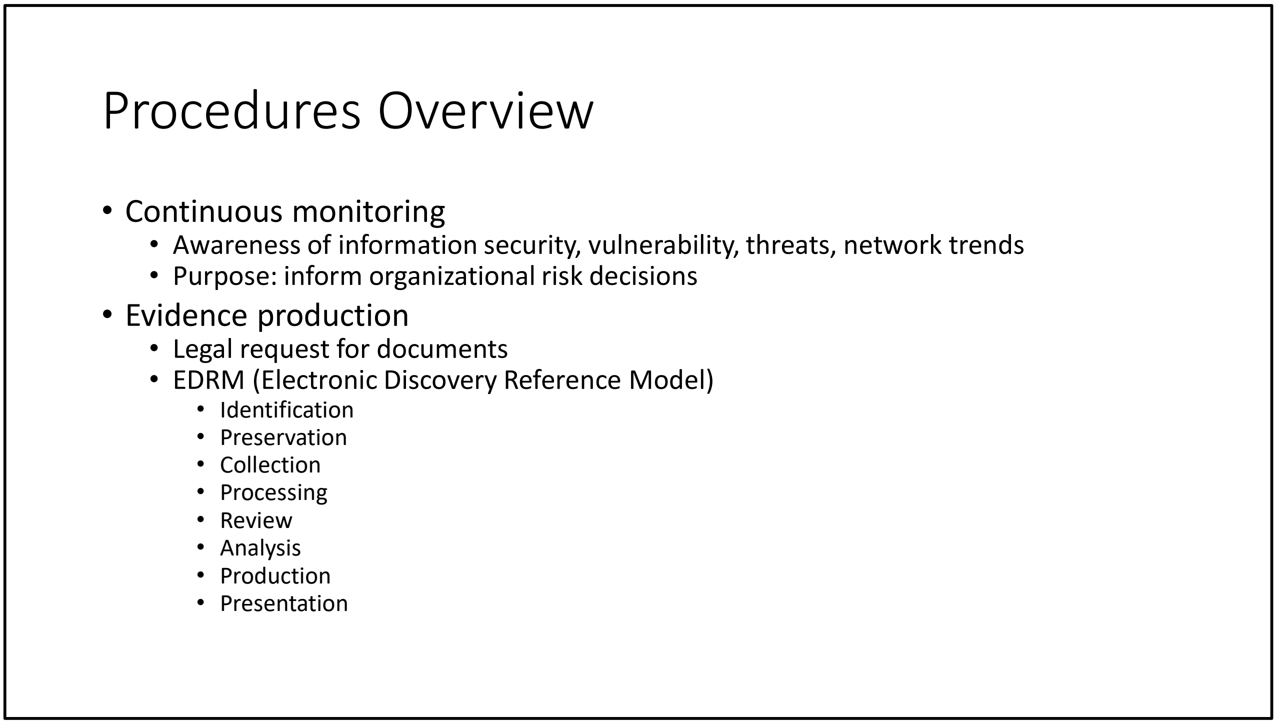
Control Selection

- Organizationally Defined Parameters
  - Internal
  - External
  - Governed by law or governmental regulations



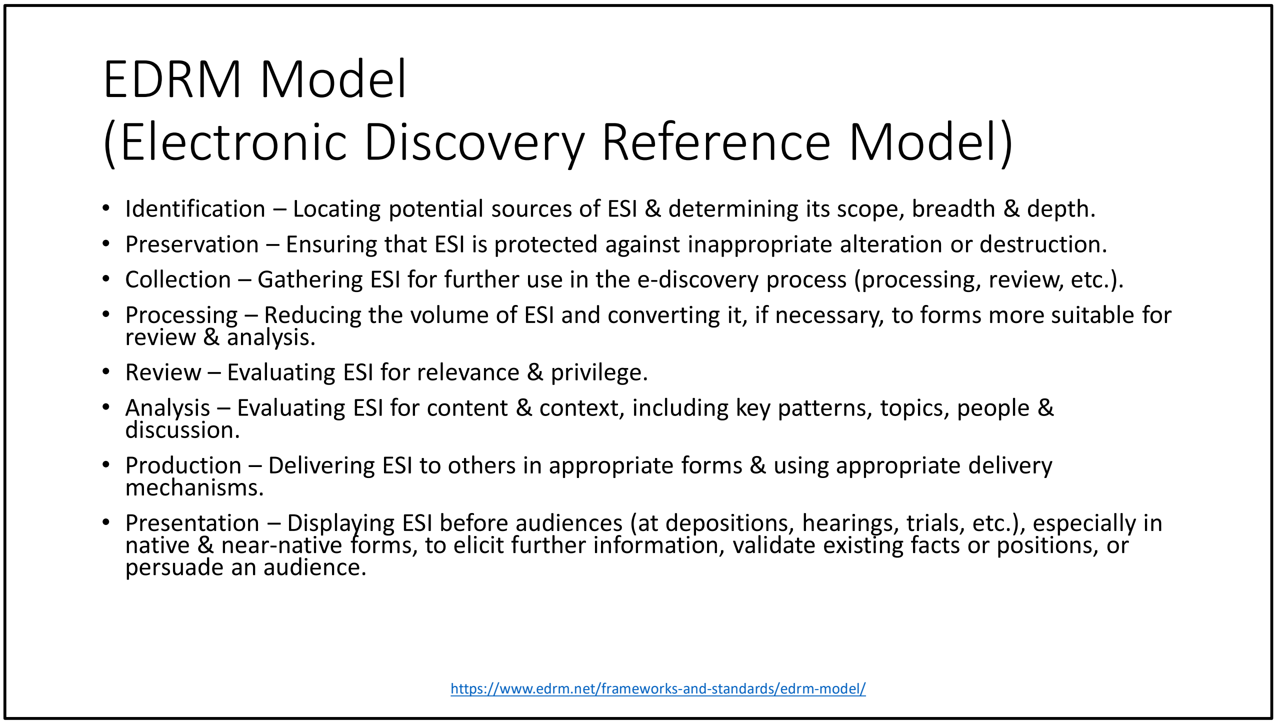
Control Selection

- Selection Criteria
  - Driven by risk assessment
    - Confidentiality
    - Integrity
    - Availability of information resources
    - Organization’s risk appetite



Procedures Overview

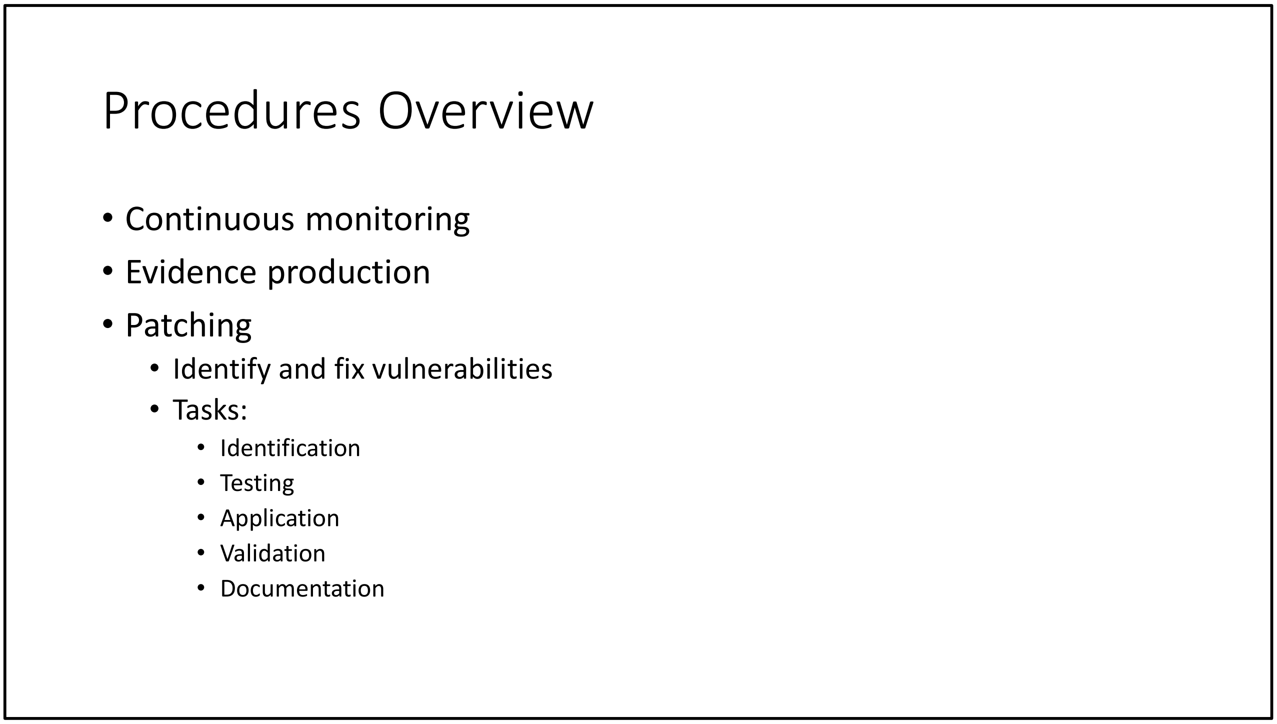
- Continuous monitoring
  - Awareness of information security, vulnerability, threats, network trends
  - Purpose: inform organizational risk decisions
- Evidence production
  - Legal request for documents
  - EDRM (Electronic Discovery Reference Model)
    - Identification
    - Preservation
    - Collection
    - Processing
    - Review
    - Analysis
    - Production
    - Presentation



EDRM Model
(Electronic Discovery Reference Model)

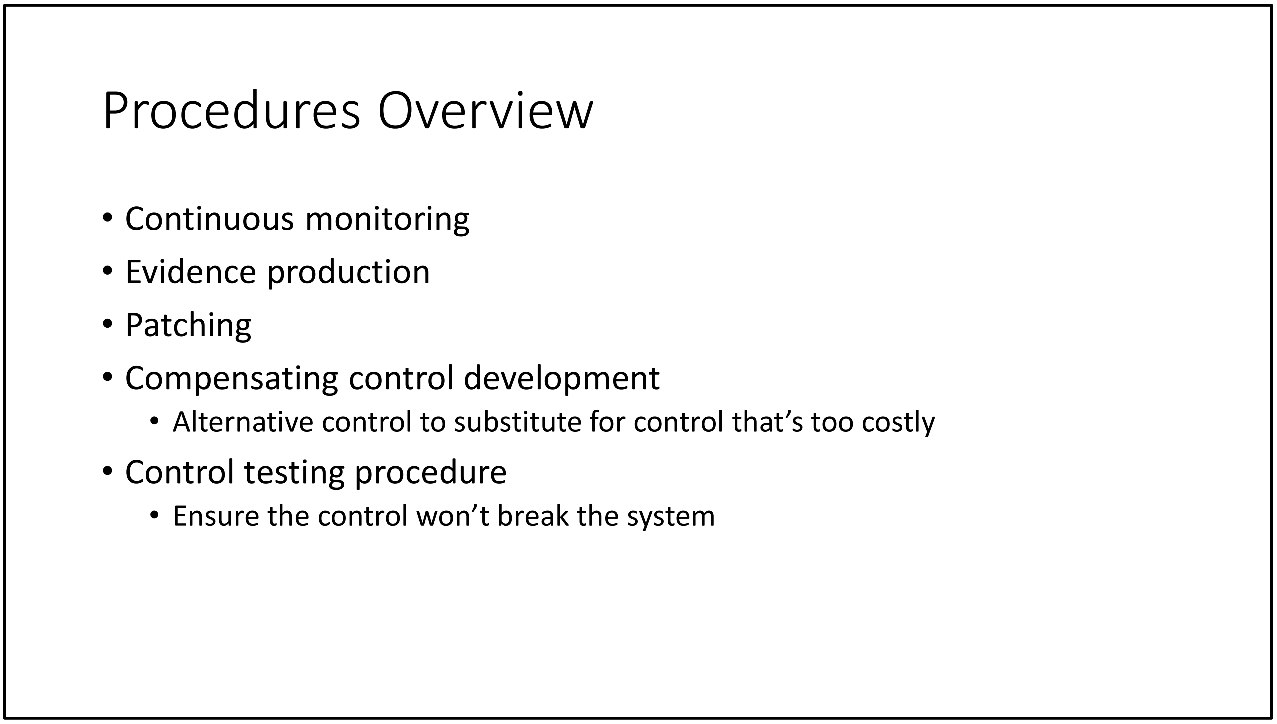
- Identification – Locating potential sources of ESI & determining its scope, breadth & depth.
- Preservation – Ensuring that ESI is protected against inappropriate alteration or destruction.
- Collection – Gathering ESI for further use in the e-discovery process (processing, review, etc.).
- Processing – Reducing the volume of ESI and converting it, if necessary, to forms more suitable for review & analysis.
- Review – Evaluating ESI for relevance & privilege.
- Analysis – Evaluating ESI for content & context, including key patterns, topics, people & discussion.
- Production – Delivering ESI to others in appropriate forms & using appropriate delivery mechanisms.
- Presentation – Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native & near-native forms, to elicit further information, validate existing facts or positions, or persuade an audience.

https://www.edrm.net/frameworks-and-standards/edrm-model/



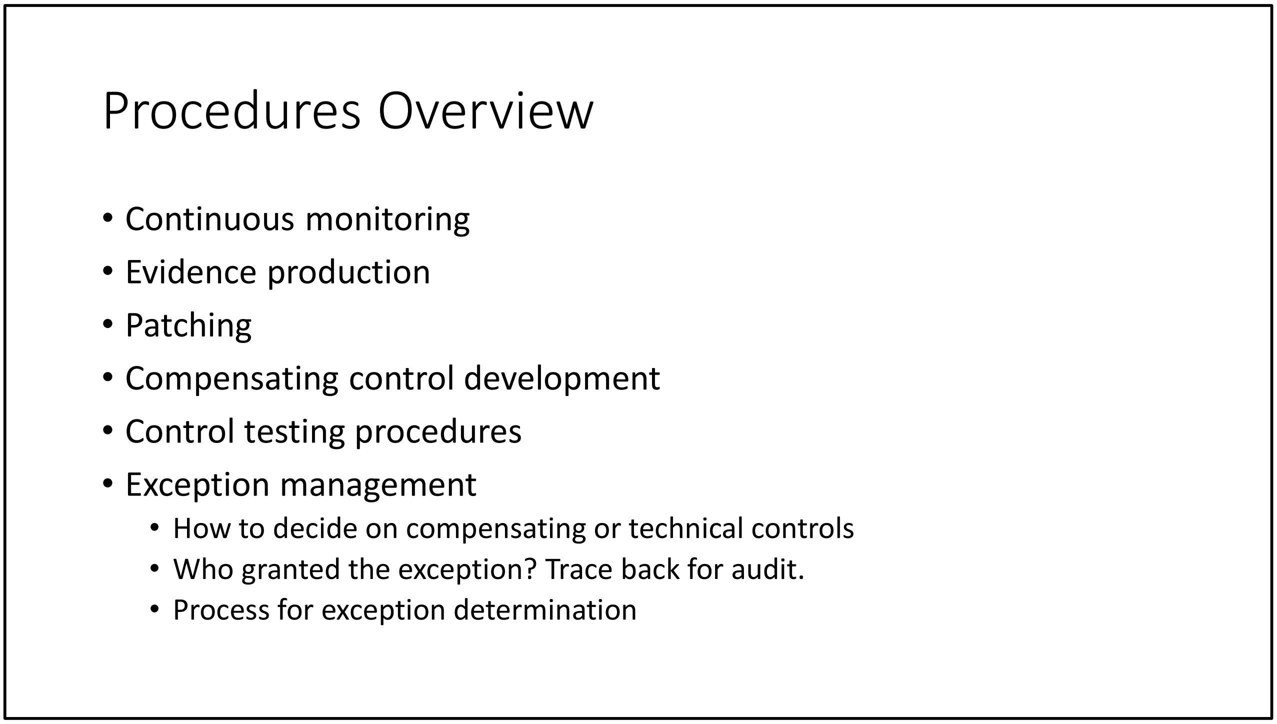
Procedures Overview

- Continuous monitoring
- Evidence production
- Patching
  - Identify and fix vulnerabilities
  - Tasks:
    - Identification
    - Testing
    - Application
    - Validation
    - Documentation



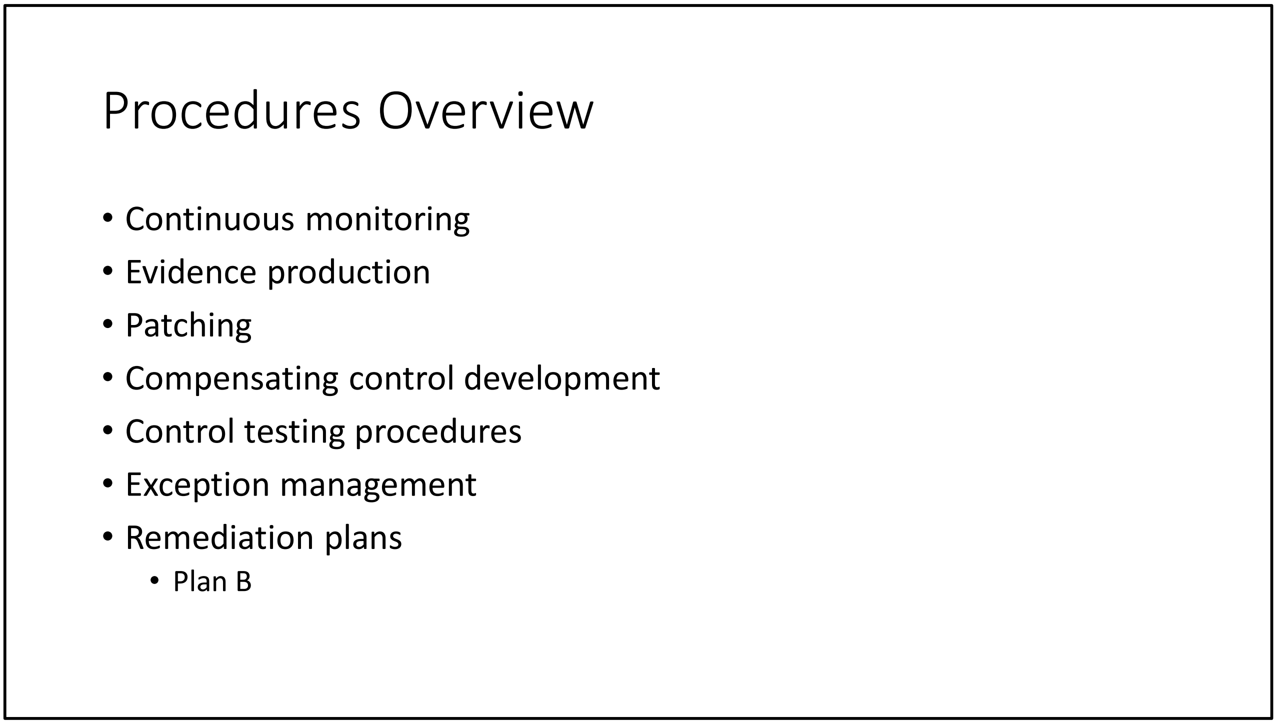
Procedures Overview

- Continuous monitoring
- Evidence production
- Patching
- Compensating control development
  - Alternative control to substitute for control that’s too costly
- Control testing procedure
  - Ensure the control won’t break the system



Procedures Overview

- Continuous monitoring
- Evidence production
- Patching
- Compensating control development
- Control testing procedures
- Exception management
  - How to decide on compensating or technical controls
  - Who granted the exception? Trace back for audit.
  - Process for exception determination



Procedures Overview

- Continuous monitoring
- Evidence production
- Patching
- Compensating control development
- Control testing procedures
- Exception management
- Remediation plans
  - Plan B

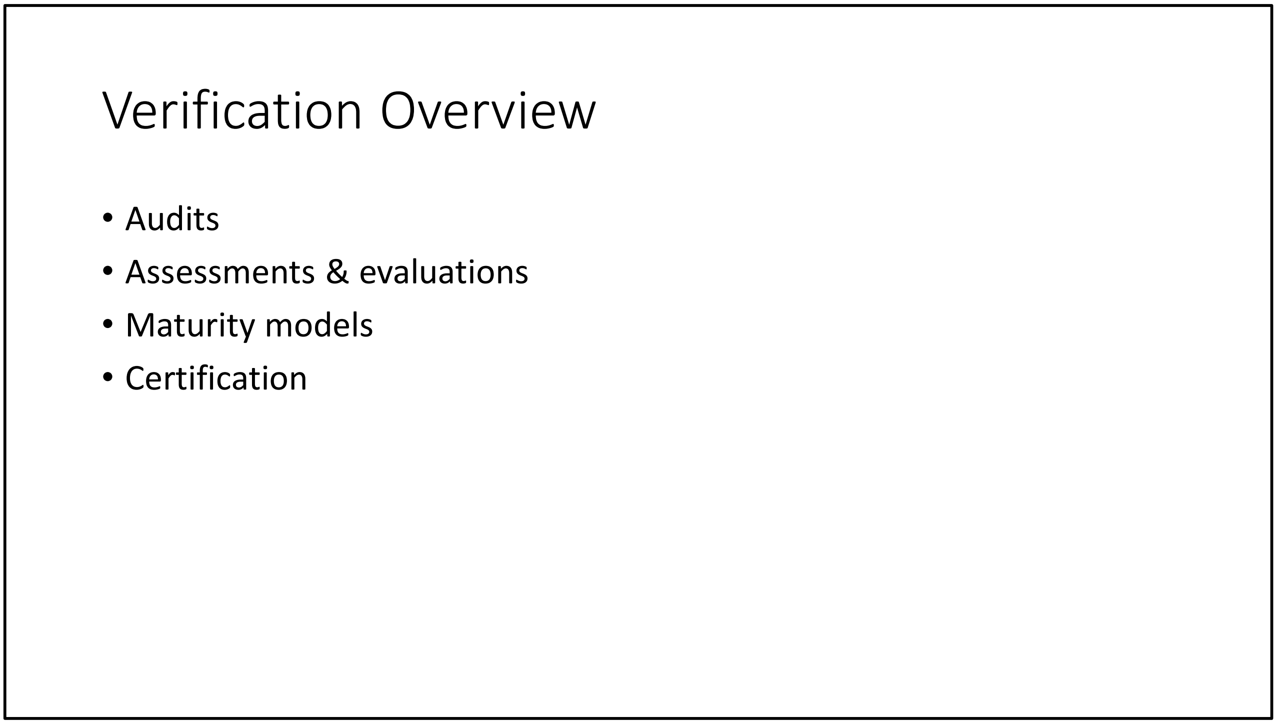
Episode 21.04

Verification

Objective: 5.3 Explain the importance of frameworks, policies, procedures, and controls.

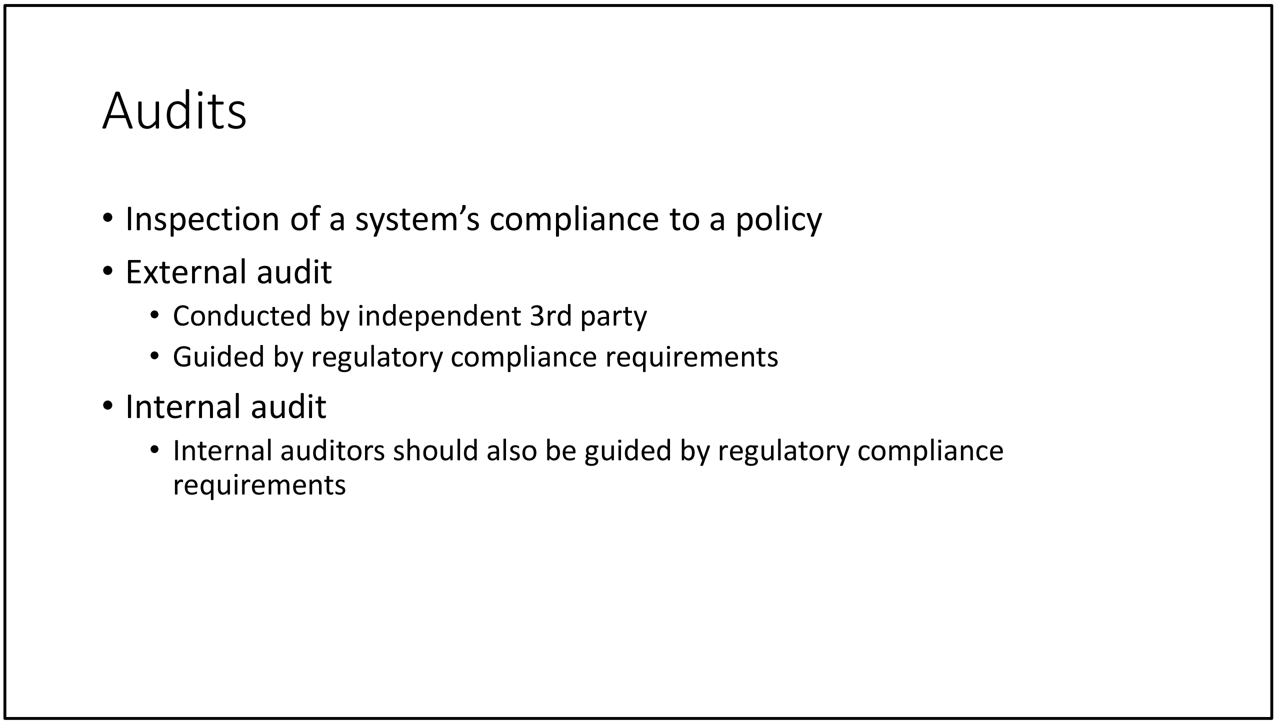
- Audits and assessments

- Regulatory
- Compliance



Verification Overview

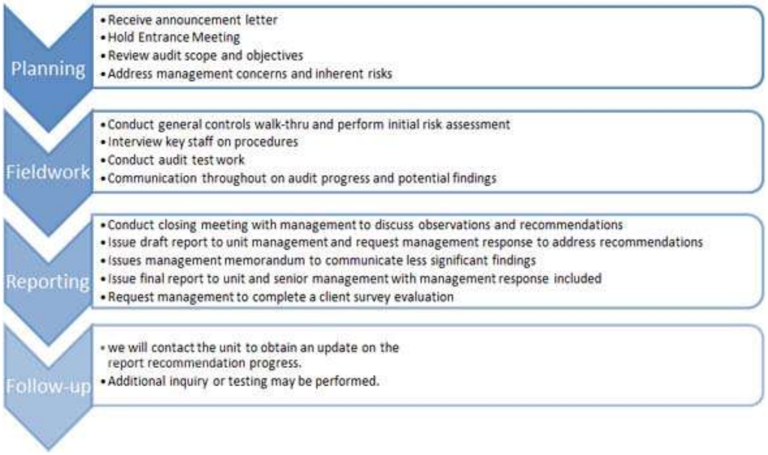
- Audits
- Assessments & evaluations
- Maturity models
- Certification



Audits

- Inspection of a system's compliance to a policy
- External audit
  - Conducted by independent 3rd party
  - Guided by regulatory compliance requirements
- Internal audit
  - Internal auditors should also be guided by regulatory compliance requirements

Audits



Planning

- Receive announcement letter
- Hold Entrance Meeting
- Review audit scope and objectives
- Address management concerns and inherent risks

Fieldwork

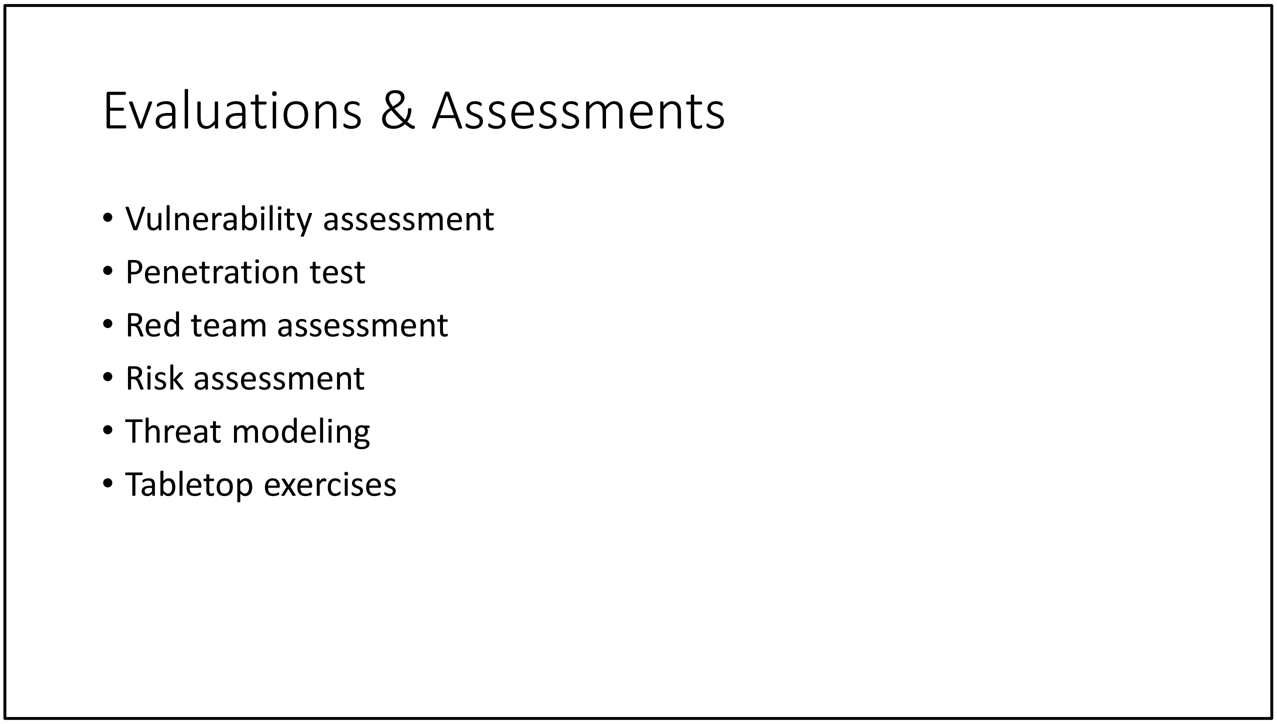
- Conduct general controls walk-thru and perform initial risk assessment
- Interview key staff on procedures
- Conduct audit test work
- Communication throughout on audit progress and potential findings

Reporting

- Conduct closing meeting with management to discuss observations and recommendations
- Issue draft report to unit management and request management response to address recommendations
- Issues management memorandum to communicate less significant findings
- Issue final report to unit and senior management with management response included
- Request management to complete a client survey evaluation

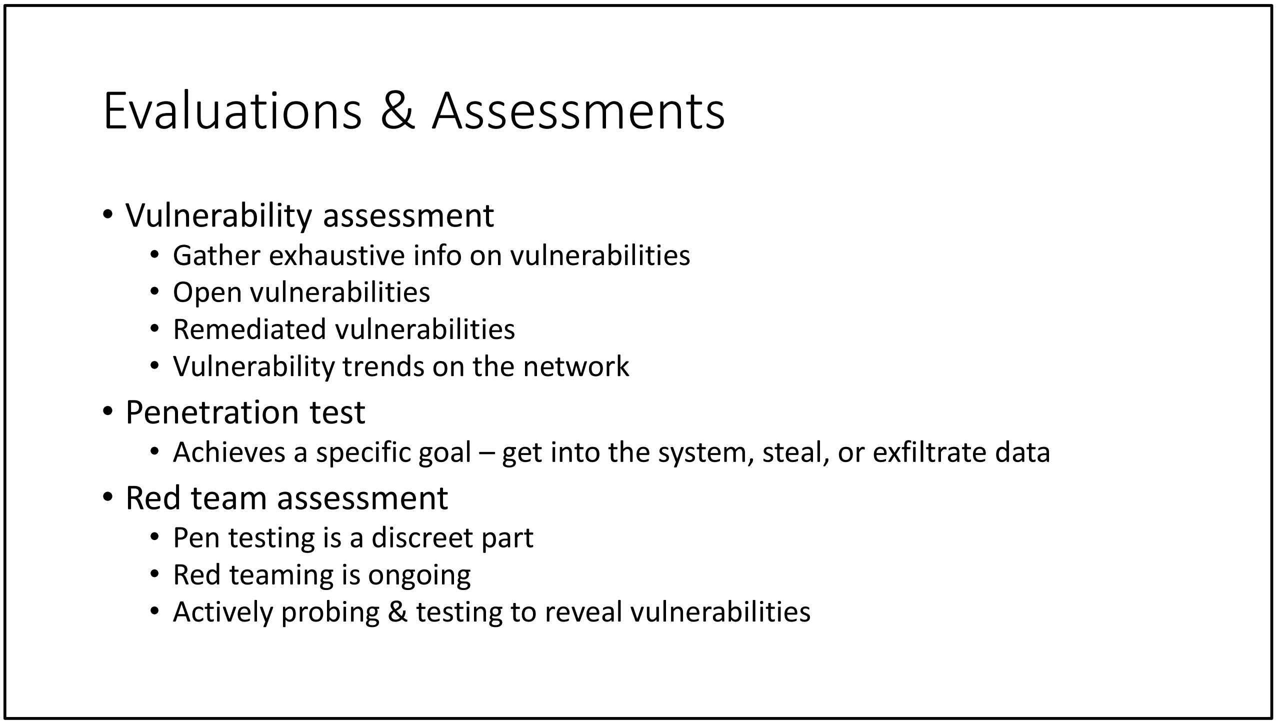
Follow-up

- we will contact the unit to obtain an update on the report recommendation progress.
- Additional inquiry or testing may be performed.



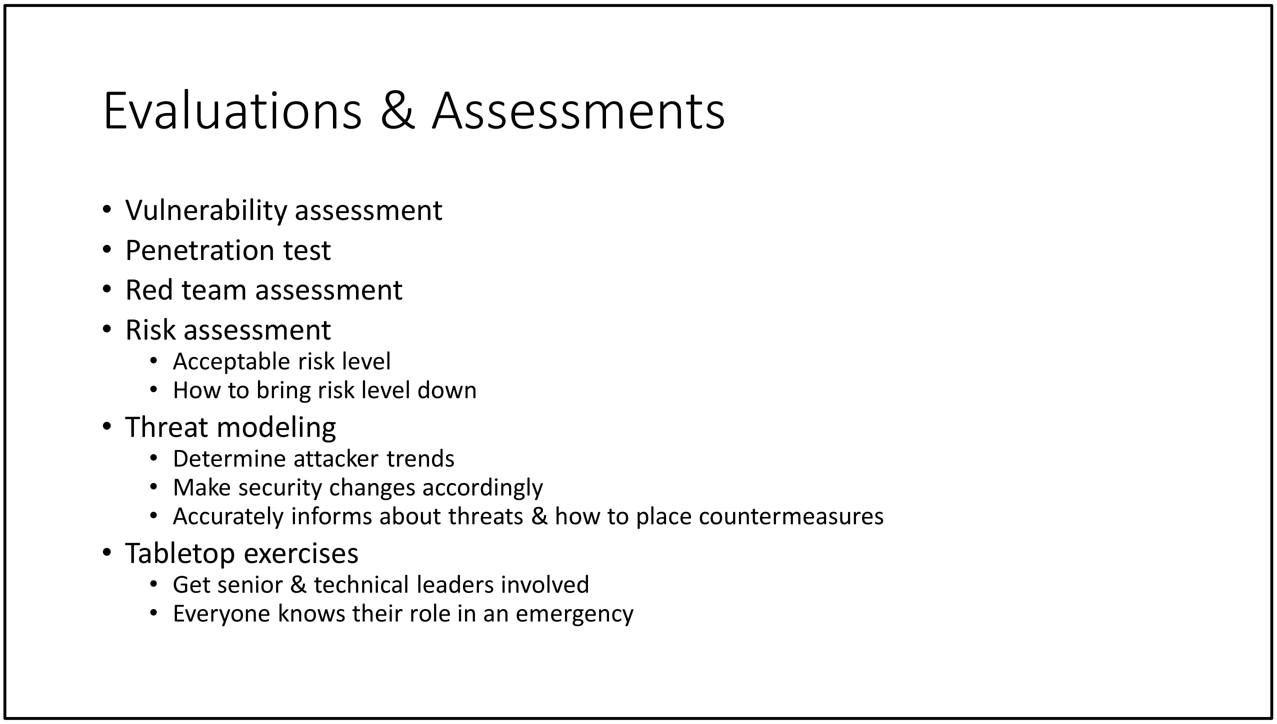
Evaluations & Assessments

- Vulnerability assessment
- Penetration test
- Red team assessment
- Risk assessment
- Threat modeling
- Tabletop exercises



Evaluations & Assessments

- Vulnerability assessment
  - Gather exhaustive info on vulnerabilities
  - Open vulnerabilities
  - Remediated vulnerabilities
  - Vulnerability trends on the network
- Penetration test
  - Achieves a specific goal – get into the system, steal, or exfiltrate data
- Red team assessment
  - Pen testing is a discreet part
  - Red teaming is ongoing
  - Actively probing & testing to reveal vulnerabilities

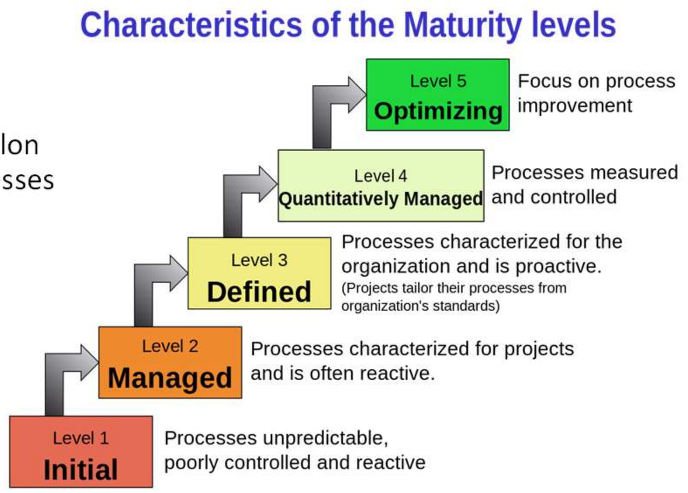


Evaluations & Assessments

- Vulnerability assessment
- Penetration test
- Red team assessment
- Risk assessment
  - Acceptable risk level
  - How to bring risk level down
- Threat modeling
  - Determine attacker trends
  - Make security changes accordingly
  - Accurately informs about threats & how to place countermeasures
- Tabletop exercises
  - Get senior & technical leaders involved
  - Everyone knows their role in an emergency

Maturity Models

- Capability Maturity Model Integration (CMMI)
  - Developed by Carnegie Mellon University to improve processes across organization



Characteristics of the Maturity levels

Level 5 **Optimizing** Focus on process improvement

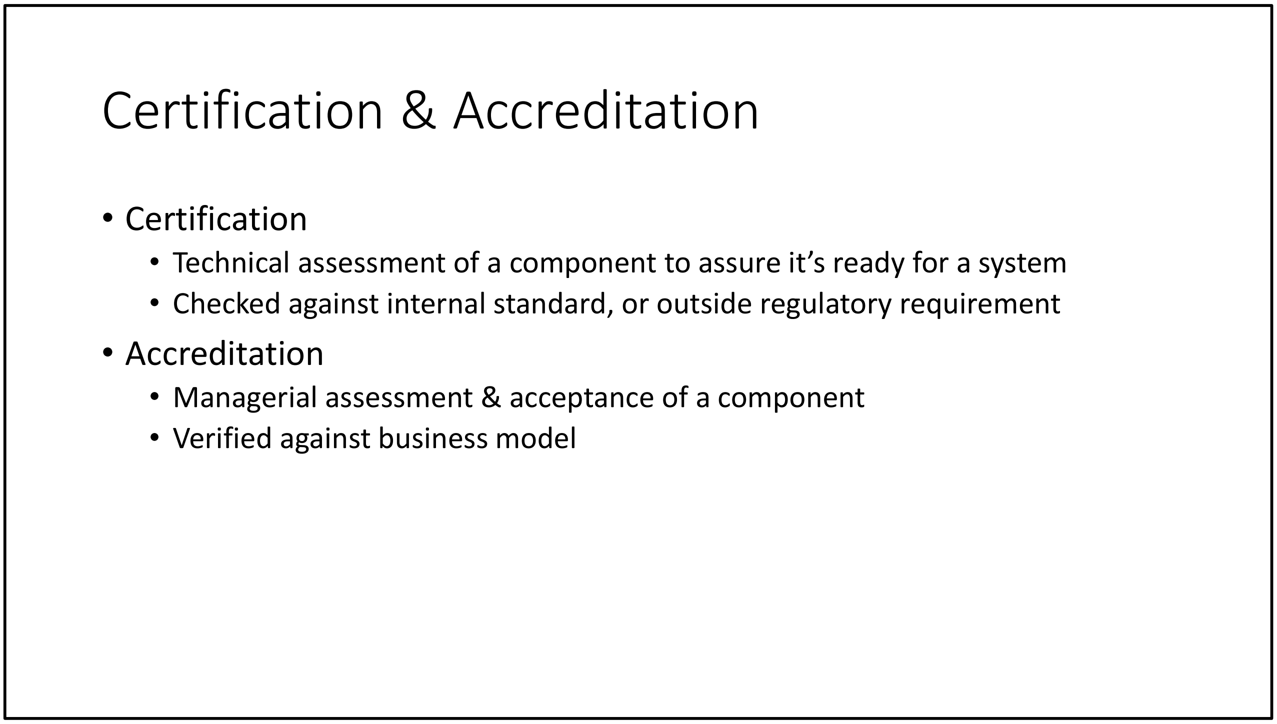
Level 4 **Quantitatively Managed** Processes measured and controlled

Level 3 **Defined** Processes characterized for the organization and is proactive. (Projects tailor their processes from organization's standards)

Level 2 **Managed** Processes characterized for projects and is often reactive.

Level 1 **Initial** Processes unpredictable, poorly controlled and reactive

https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration



Certification & Accreditation

- Certification
  - Technical assessment of a component to assure it’s ready for a system
  - Checked against internal standard, or outside regulatory requirement
- Accreditation
  - Managerial assessment & acceptance of a component
  - Verified against business model