
ESTD1845
QUEEN'S
UNIVERSITY
BELFAST

Network Security Administration

Dr. Sandra Scott-Hayward

CSC3064 Lecture 15

School of Electronics, Electrical Engineering and Computer Science

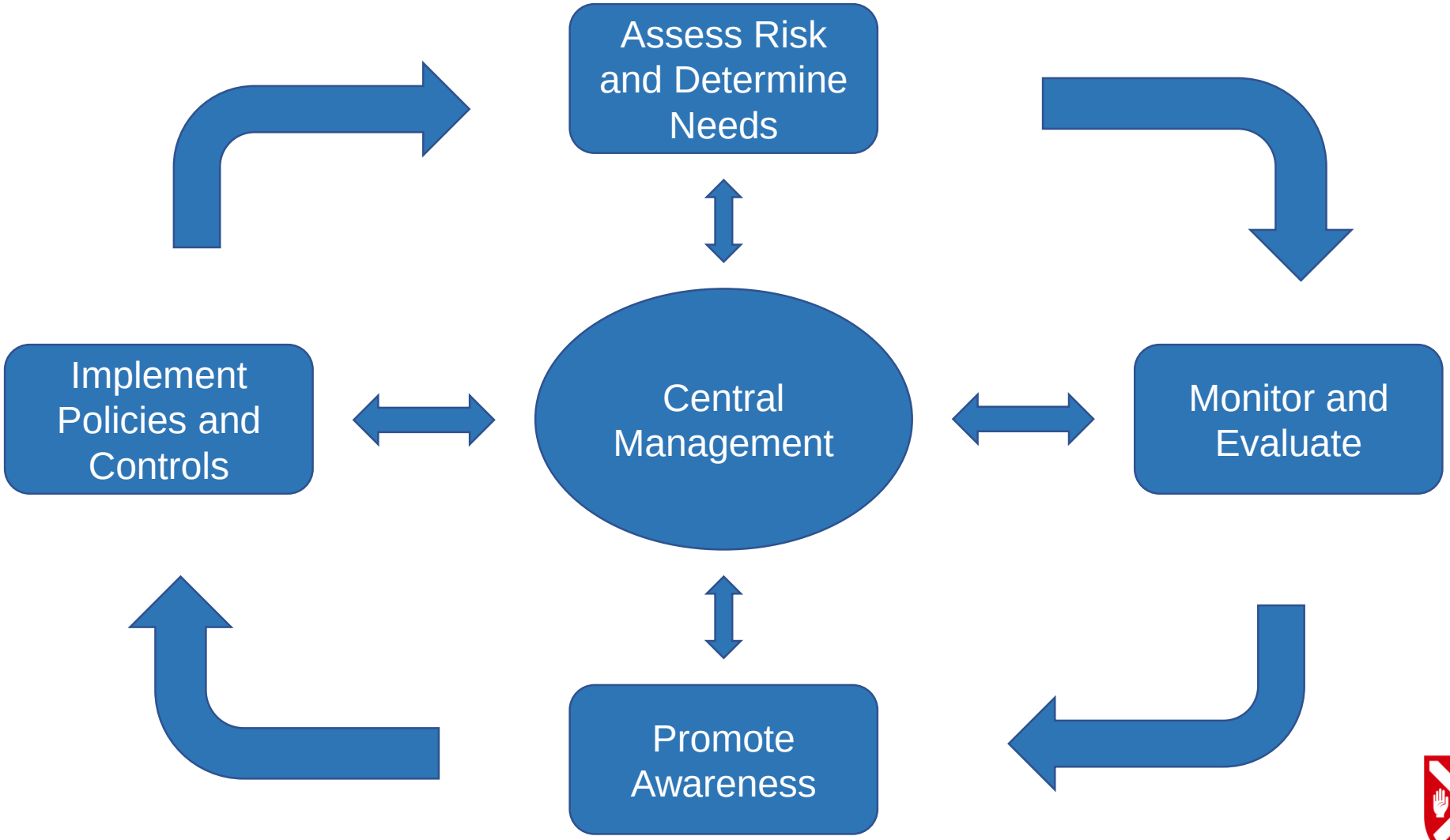
Session Overview

- Security Governance, Policy, Standards
- Access Control and Security Policy
- Risk Management
- Security Lifecycle Management
- Network Security Testing

References:
Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.
Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.
Official (ISC)^2 Guide to the CISSP® CBK®, CRC Press, 2013.

QUEEN'S UNIVERSITY BELFAST

Security management



QUEEN'S UNIVERSITY BELFAST

Security governance

Management should:

- Write security policies with business input
- Ensure that roles and responsibilities are defined and clearly understood
- Identify threats and vulnerabilities
- Implement security infrastructures and control frameworks (standards, guidelines, and procedures)
- Ensure that policy is approved by the governing body
- Establish priorities and implement security projects in a timely manner
- Monitor breaches
- Conduct periodic reviews and tests
- Reinforce awareness education as critical
- Build security into the systems development life cycle

QUEEN'S UNIVERSITY BELFAST

Security roles and responsibilities

Security is the responsibility of everyone within the company.

End User
- Adherence to security policies

Executive Management
- Overall responsibility for protection of information assets

Information Systems Security Professional
- Coordinates drafting of security policies, standards and supporting guidelines, procedures and baselines

Security Officer
- Directs, coordinates, plans, and organizes information security activities

IS/IT Professional
- Design, test, and implement security controls

Network/Systems Administrator
- Configures network/server H/W and OS to ensure information available and accessible (patch and vulnerability management).

Data/Information/Business Owner
- Responsible for protection of information assets

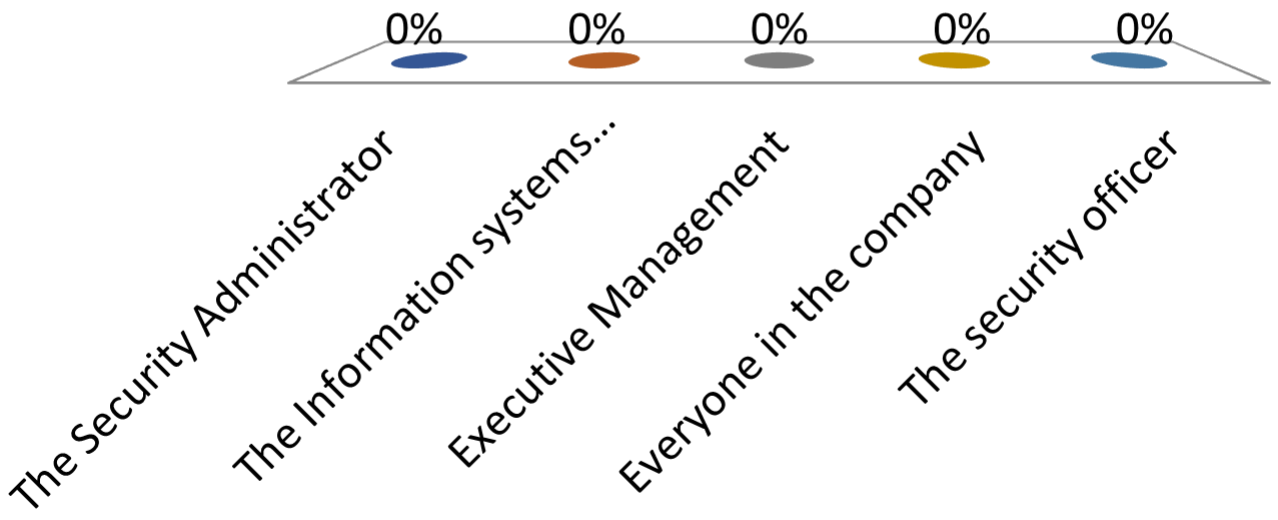
Information Systems Auditor
- Checks compliance with security policies etc.

Security Administrator
- Manages user access request process, controls access to authorized individuals

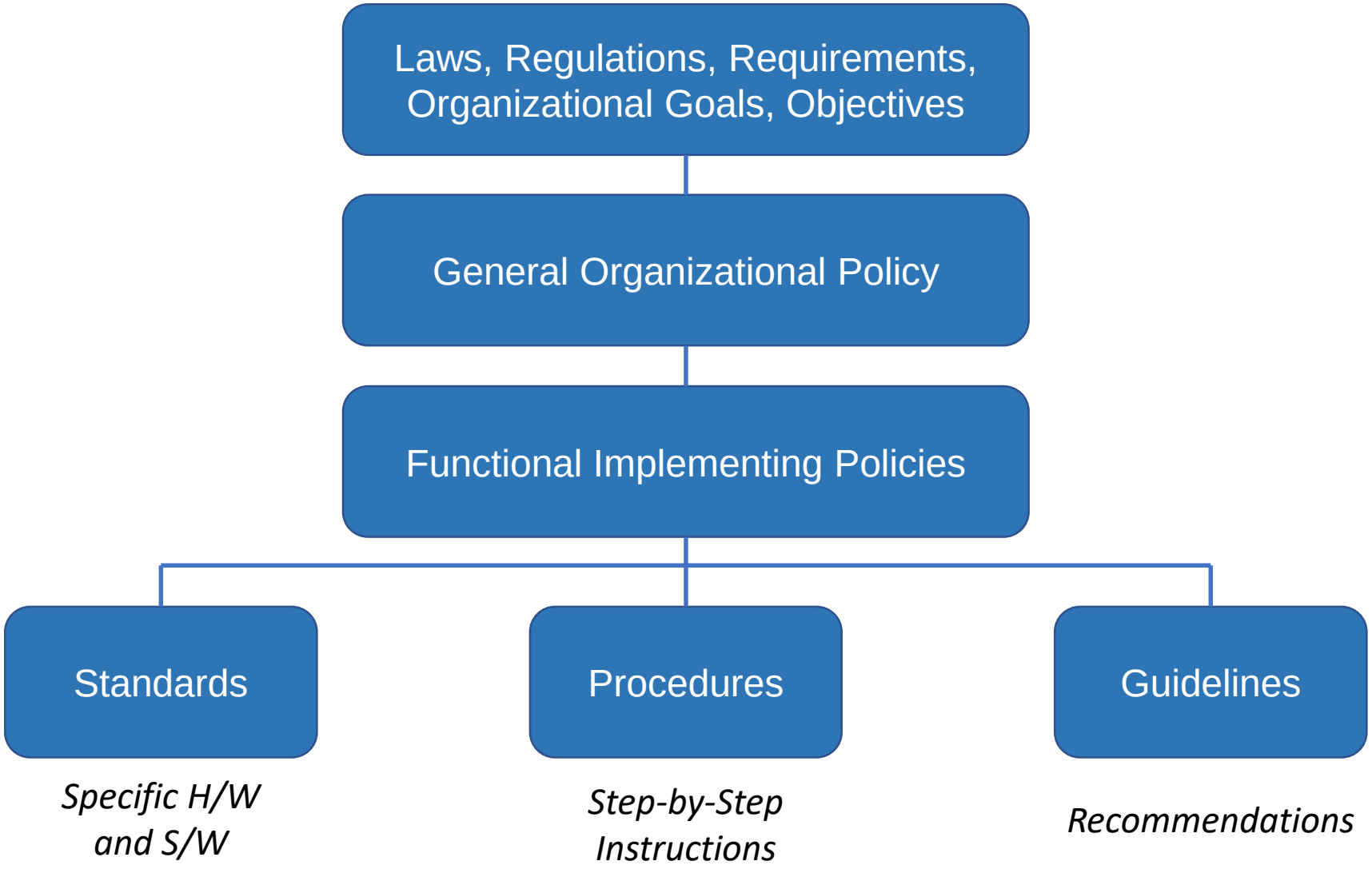
QUEEN'S UNIVERSITY BELFAST

Security is the responsibility of …

A. The Security Administrator
B. The Information systems security professional
C. Executive Management
✓ D. Everyone in the company
E. The security officer



Security policy (relationships)



QUEEN'S UNIVERSITY BELFAST

Guidelines for creating good security policies (1)

- Formally define a policy creation and policy maintenance practice
- Policies should survive for two or three years
- Do not be too specific in policy statements
- Technical implementation details do not belong in a policy
- Use forceful, directive wording
- Keep each policy as short as possible
- Provide references in policy to the supporting documents
- Thoroughly review before publishing

QUEEN'S UNIVERSITY BELFAST

Guidelines for creating good security policies (2)

- Conduct management review and sign-off
- Employees should acknowledge policies
- Do not use technical jargon in policy language
- Review incidents and adjust policies
- Periodically review policies
- Define policy exception rules
- Develop sanctions for non-compliance

QUEEN'S UNIVERSITY BELFAST

Types of security policies

Organizational or program policy

- Issued by senior mgmt., creates authority and scope for security program
- Sets out high level authority to define appropriate sanctions for failure to comply with the policy

Functional, Issue-Specific Policies

- Address areas of particular security concern (e.g. domain such as access control, segregation of duties, or technical area such as use of email)

System-specific Policies

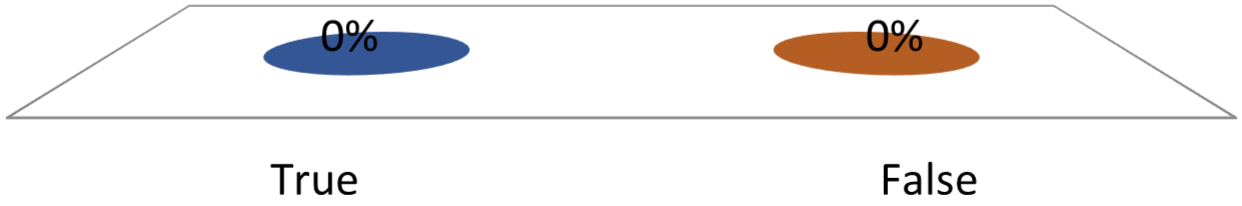
- For specific technical or operational area or specific application or platform (e.g. which departments are permitted to input or modify information in electronic payments application)

QUEEN'S UNIVERSITY BELFAST

A good security policy will be very specific and include technical implementation details.

A. True

✓B. False



Security standards

ISO-27002 (http://www.27000.org/iso-27002.htm)

"Code of Practice for Information Security Management"

NIST Special Publications 800-14 (https://csrc.nist.gov/publications/detail/sp/800-14/final)

Control Objects for Information and Related Technology (COBIT)

"Framework for IT management"

Other Examples:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Sarbanes-Oxley (SOX) - Internal controls for financial reporting
- Health Insurance Portability and Accountability Act (HIPAA)

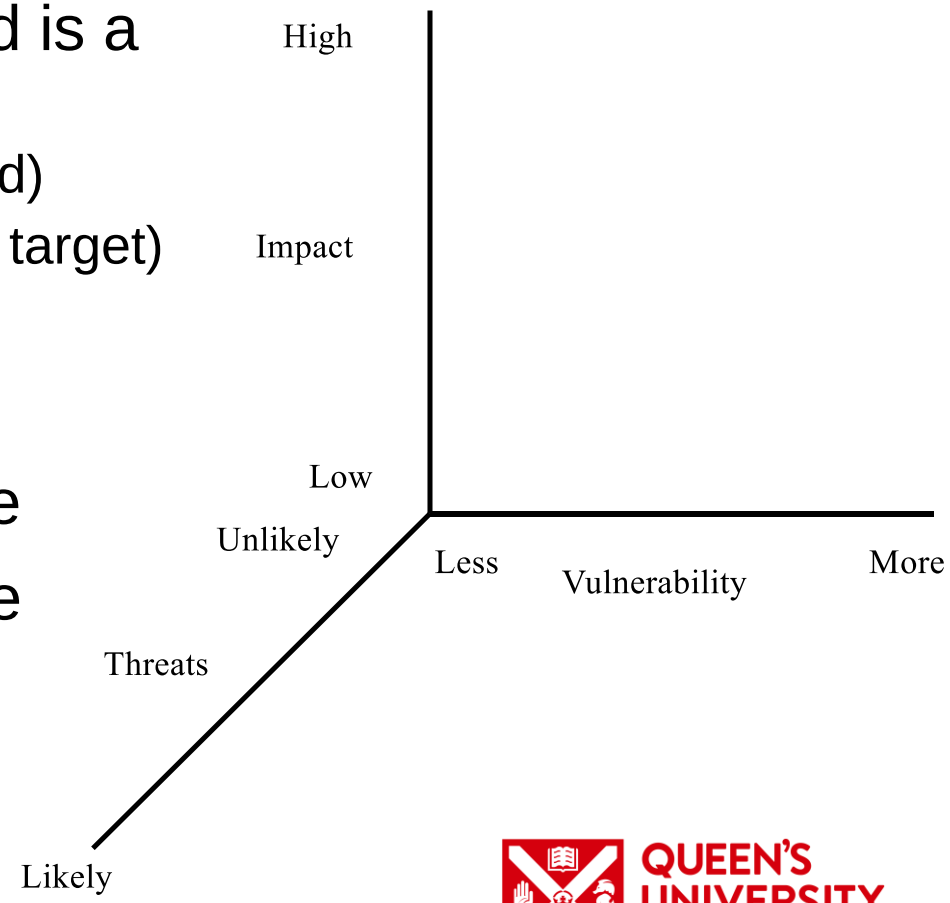
QUEEN'S UNIVERSITY BELFAST

Risk and Risk Assessment

Risk is a measure of how critical something is and is a combination of:

- **Threat** (How likely is it that the target will be attacked)
- **Vulnerability** (How likely there is a weakness in the target)
- **Impact** (What is the effect of losing the target)

Risk assessment is the process where you decide how important something is and how hard you are going to work to protect it.



QUEEN'S UNIVERSITY BELFAST

Risk Management

Risk management is the process of identifying, assessing, and reducing risk to an acceptable level

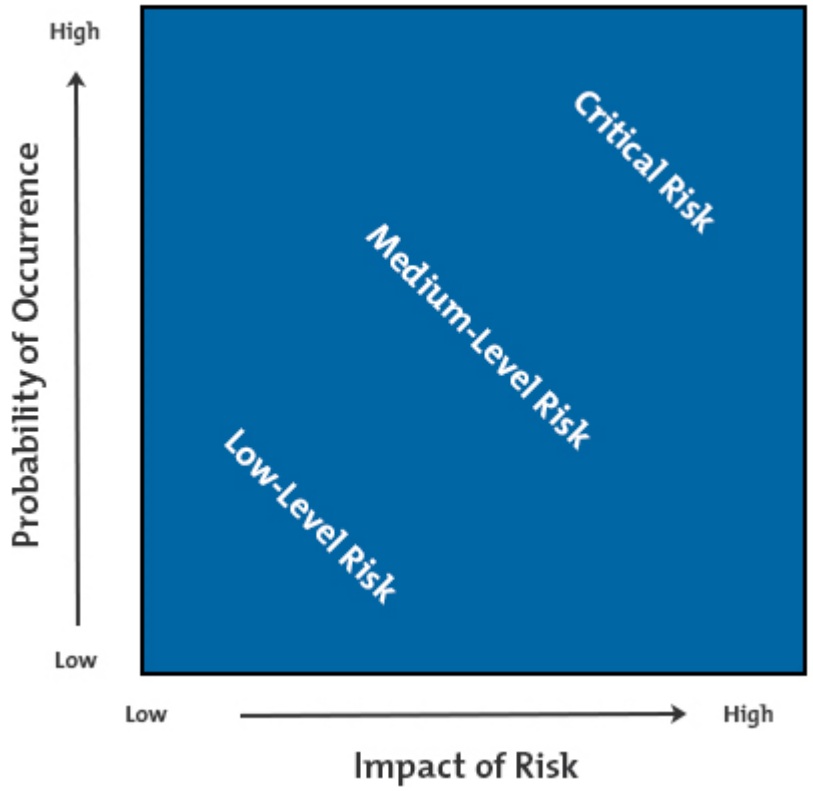
Risk analysis is a tool used to:

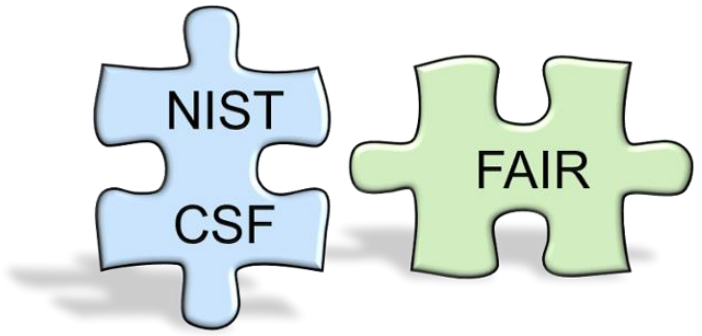
- Identify the company's assets
- Calculate asset values
- Identify vulnerabilities
- Estimate threats and associated risks
- Assess the impact the company would face if these agents took advantage of the current available vulnerabilities

QUEEN'S UNIVERSITY BELFAST

Risk Identification, Assessment, Management & Communication

- Identify
- Analyse
- Prioritize
- Mitigate





What is the maturity level of our cybersecurity activities?

How much risk do we have? Which activities matter the most and should be prioritized?

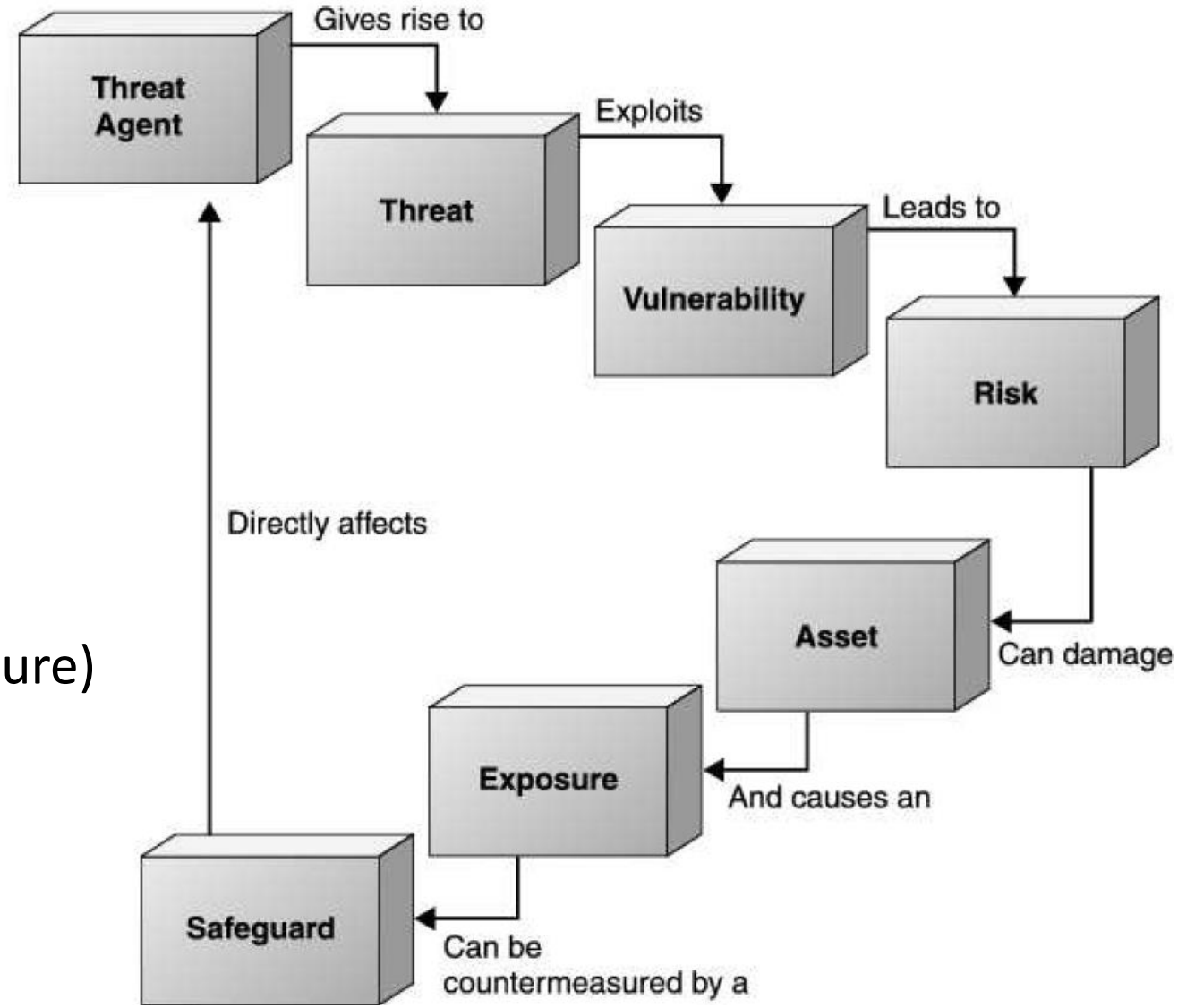
FAIR (Factor Analysis of Information Risk): http://www.fairinstitute.org/blog/press-release-two-cybersecurity-standards-come-together-to-help-organizations-quantify-and-prioritize-risk

QUEEN'S UNIVERSITY BELFAST

Information Security

- Identify assets & values
- Identify threats
- Quantify impact of potential risks
- Mitigate the risk

  (cost of risk vs. cost of countermeasure)



QUEEN'S UNIVERSITY BELFAST

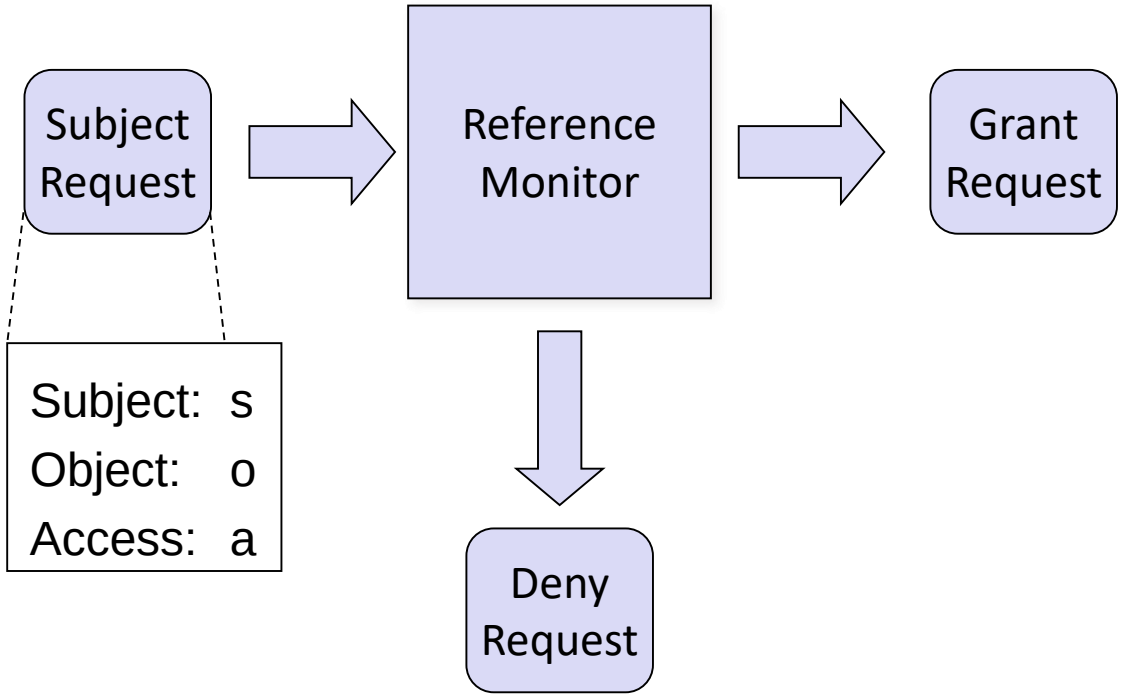
Example

Term	Definition	Example
Vulnerability	Weakness in a mechanism	Buffer overflow
Threat	Someone uncovering the vulnerability and exploiting it.	Hacker using an automated tool to exploit the buffer overflow and gain privileged access to system.
Risk	Probability of a threat agent exploiting a vulnerability. (Risk is higher if no countermeasure is in place.)	If code is written poorly, and there is no firewall to restrict access to the system with the buffer overflow, there is a high risk that a threat agent will attempt to overflow the buffer.
Countermeasure	Safeguard put into place to mitigate the risk of a threat.	Rewrite the application or replace it with a more secure application. A firewall and intrusion detection system can also work as countermeasures here.

QUEEN'S UNIVERSITY BELFAST

Remember access control …

Access control comprises those mechanisms that enforce mediation on subject requests for access to objects as defined in some specified ***security policy***.



In order to make access control decisions, the reference monitor needs to know the ***security policy*** of the system.

QUEEN'S UNIVERSITY BELFAST

Types of access control mechanism (1)

An *access control mechanism* is an actual realization of the reference monitor concept

There are two main types of access control mechanisms:

- ***Discretionary access control*** comprises those procedures and mechanisms that enforce the specified mediation at the discretion of individual users

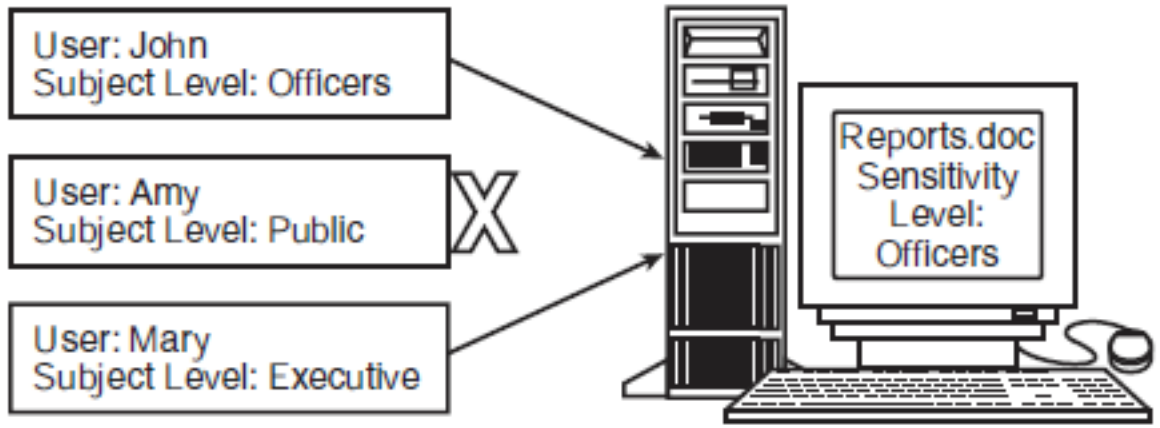
  Example: the Unix operating system allows users to give or withdraw the read/write/execute access rights for files they own

- ***Mandatory access control*** comprises those procedures and mechanisms that enforce the specified mediation at the discretion of a centralized system administration facility

QUEEN'S UNIVERSITY BELFAST

Types of access control mechanism (2)

MAC:



Both types may be combined, with the mandatory access control decisions most of the time overriding discretionary ones

Example:

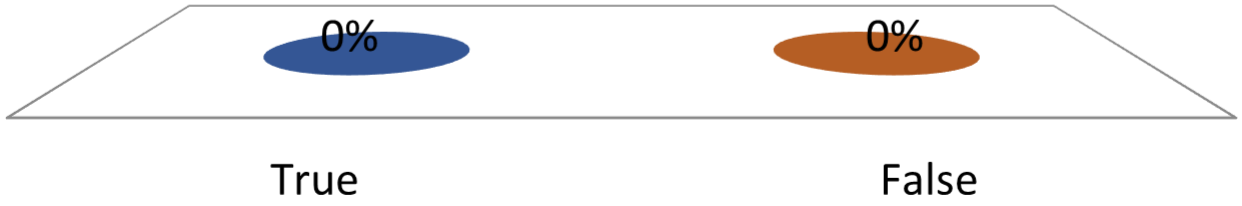
- Use of discretionary access control on personal computers combined with mandatory access control for communications (→ firewalls)

QUEEN'S UNIVERSITY BELFAST

An example of discretionary access control is a Firewall.

A. True

✓B. False



Common access control schemes (1)

Access Control Lists (ACL):

- ACLs are the basis for an access control scheme, where for each object a list of valid subjects is stored which might have access to this object (possibly together with the type of access that is allowed)
- ACLs are usually used with discretionary access control, as there are too many ACLs for maintenance by a central administration facility

	UserMary Directory	UserBob Directory	UserBruce Directory	Printer001
Mary	Full Control	Write	Write	Execute
Bob	Read	Full Control	Write	Execute
Bruce	No Access	Write	Full Control	Execute
Sally	No Access	No Access	No Access	No Access

QUEEN'S UNIVERSITY BELFAST

Security labels (1)

A *security level* is defined as a hierarchical attribute with entities of a system in order to denote their degree of sensitivity

Examples:

- Military: unclassified < confidential < secret < top secret
- Commercial: public < sensitive < proprietary < restricted

A *security category* is defined as a nonhierarchical grouping of entities to help denote their degree of sensitivity

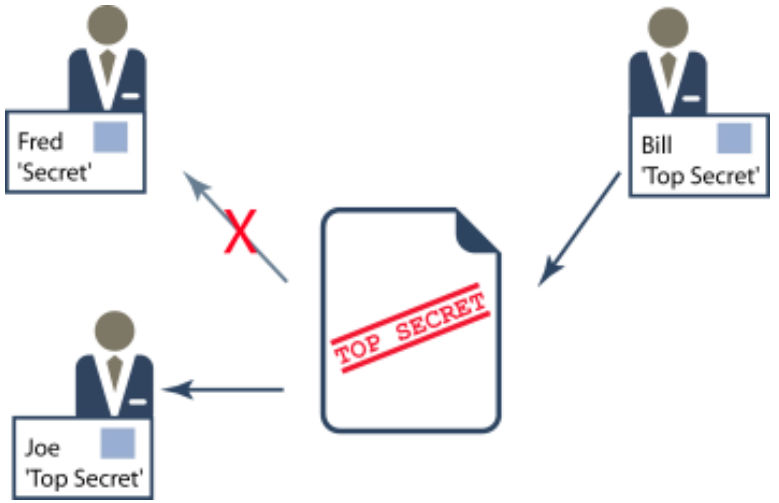
Example (commercial): department A, department B, administration, etc.

Security labels (2)

A *security label* is defined as an attribute that is associated with system entities to denote their hierarchical sensitivity level and security categories

Security labels that denote the security sensitivity of:

- Subjects are called *clearances*
- Objects are called *classifications*

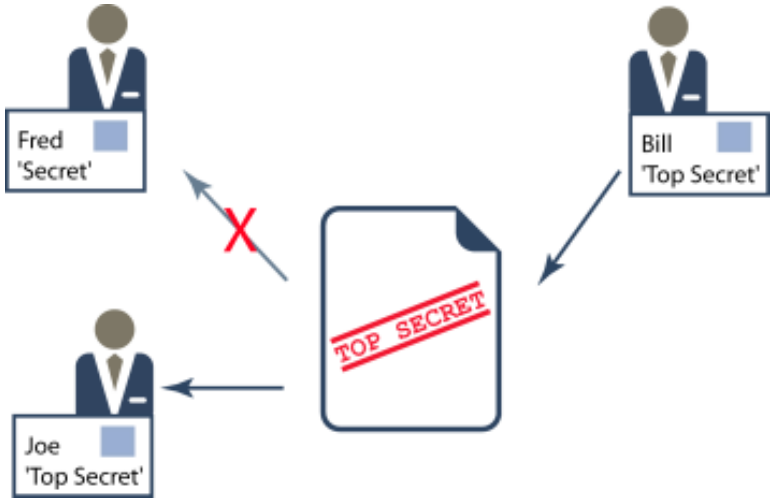


QUEEN'S UNIVERSITY BELFAST

Common access control schemes (2)

Label-based access control:

- If security labels are stored and processed with the entities of a system, they can be used to perform label-based access control
- This scheme is usually used as a mandatory access control mechanism



Data integrity of access control data structures is critical!

QUEEN'S UNIVERSITY BELFAST

Remember network access control …

- An umbrella term for managing access to a network
- Authenticates users logging into the network and determines what data they can access and actions they can perform
- Also examines the health of the user's computer or mobile device (e.g. pre-admission endpoint security policy check)

QUEEN'S UNIVERSITY BELFAST

Categories of access control

Directive:	Controls designed to specify acceptable rules of behavior within an organization
Deterrent:	Controls designed to discourage people from violating security directives
Preventive:	Controls implemented to prevent a security incident or information breach
Compensating:	Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
Detective:	Controls designed to signal a warning when a security control has been breached
Corrective:	Controls implemented to remedy circumstance, mitigate damage, or restore controls
Recovery:	Controls implemented to restore conditions to normal after a security incident

QUEEN'S UNIVERSITY BELFAST

Examples for access control categories

Control Type	*Directive*	*Deterrent*	*Preventative*	*Detective*	*Corrective*	*Recovery*	*Compensating*
Administrative	Policy	Policy	User registration procedure	Review violation reports	Termination	DR Plan	Supervision, Job Rotation, Logging
Logical	Config. Standards	Warning Banner	Password based login, IPS	Logs, IDS	Unplug, isolate, & terminate connection	Backups	CCTV, Keystroke Monitoring
Physical	Authorized personnel only signs, Traffic Lights	Beware of dog sign	Fence	Sentry, CCTV	Fire Extinguisher	Rebuild	Layered Defense

QUEEN'S UNIVERSITY BELFAST

Security Control Types

Administrative Controls

- Usually management's responsibilities, as in developing security policies, procedures and standards

Technical Controls

- Logical mechanisms that protect resources and information, as in encryption, firewall, intrusion detection system, and access control software

Physical Controls

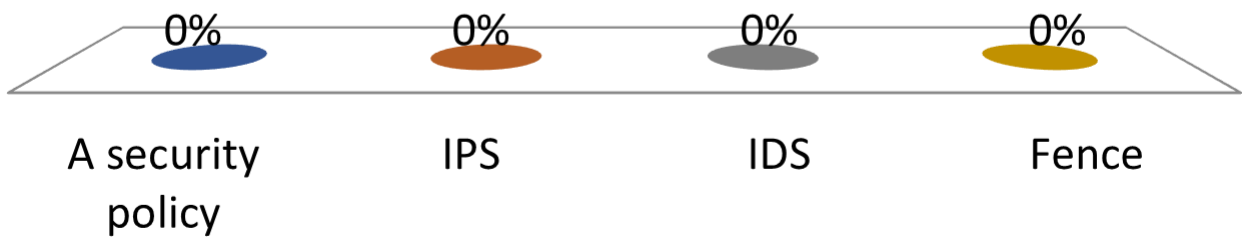
- Protect computer systems, departments, people, and the facility

=> Defense in Depth!

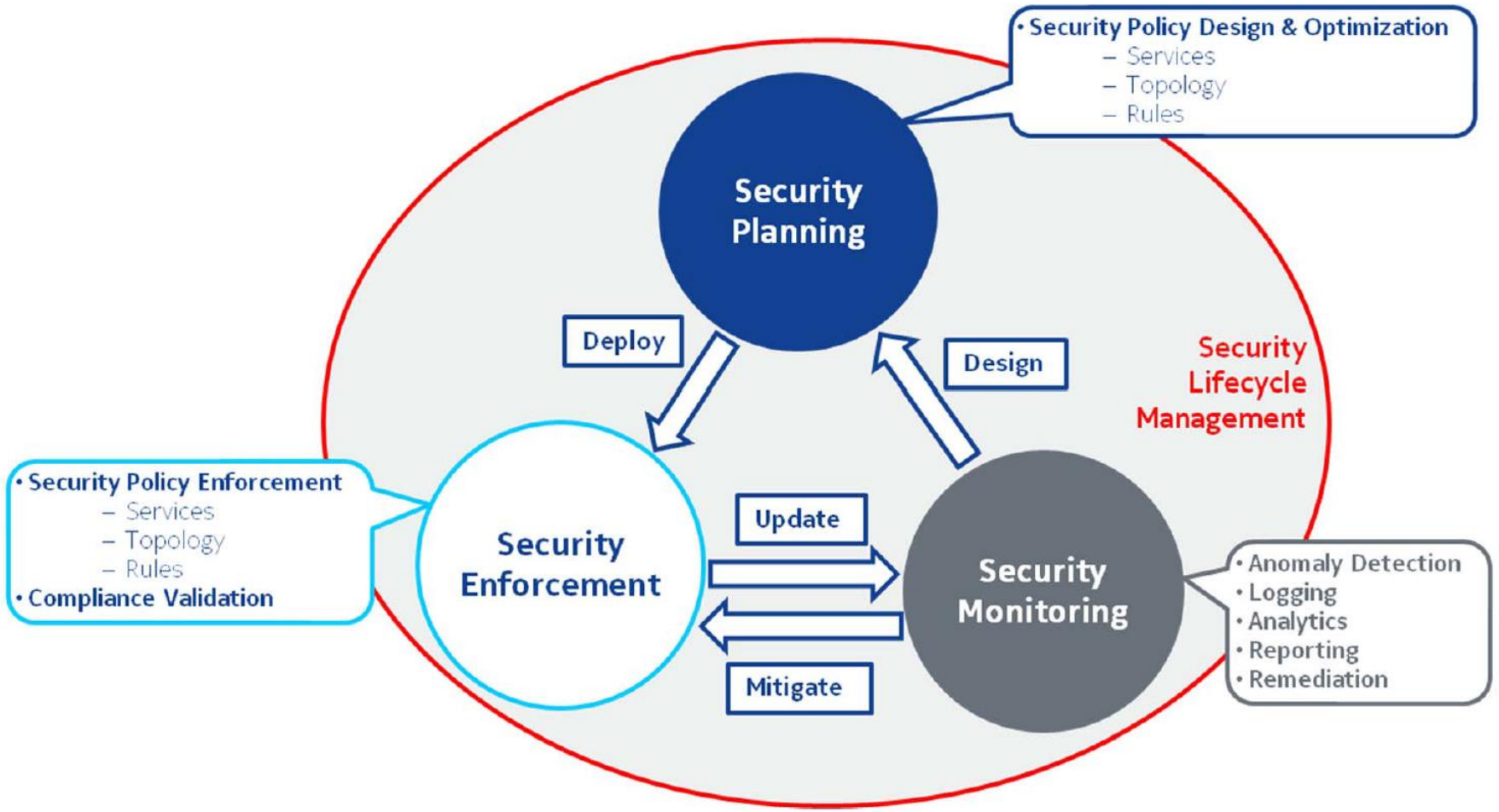
QUEEN'S UNIVERSITY BELFAST

An example of logical access control is …

A. A security policy
✓B. IPS
✓C. IDS
D. Fence



Security Lifecycle Management



"Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification, ETSI GS NFV-SEC 013 v3.1.1, February 2017

QUEEN'S UNIVERSITY BELFAST

Security Lifecycle Management

Security Planning covers:

- Manually or automatically design security policies for Infrastructure and/or network services based on security requirements, organization policies, etc.
- Manually or automatically optimize security policies for Infrastructure and/or network services based on enhancement of organization policies, analytics results of monitoring, etc.

Security Enforcement covers:

- Manage Security Policies deployment and configuration changes in the network and Security Functions.
- Automatically validate the compliance of the security policies.

Security Monitoring covers the application and implementation of the security policy and achieving trusted assurances of that implementation through secure and trusted network security monitoring telemetry.

QUEEN'S UNIVERSITY BELFAST

Network security assessment

Vulnerability Assessment

Internal Assessment

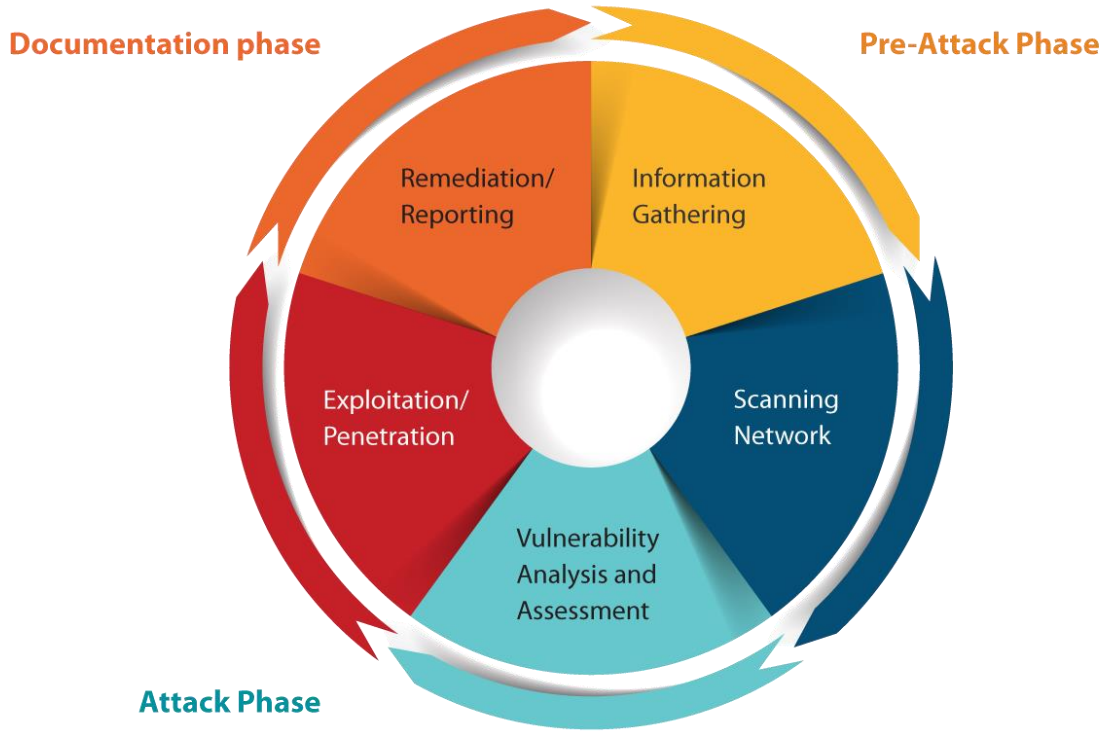
- Internal, trusted network

External Assessment

- Internet-connected systems

Wireless Assessment

- Wireless infrastructure



Assessment analysis and documentation

QUEEN'S UNIVERSITY BELFAST

Network security testing

Objectives of the security test and evaluation:

- Uncover design, implementation, and operational flaws that could allow the violation of the security policy
- Determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy
- Assess the degree of consistency between the system documentation and its implementation

Network security testing

Results can be used:

- As a reference point for corrective action
- To define mitigation activities to address identified vulnerabilities
- As a benchmark to trace the progress of an organization in meeting security requirements
- To assess the implementation status of system security requirements
- To conduct cost and benefit analysis for improvements to system security
- To enhance other lifecycle activities, such as risk assessments, certification and authorization (C&A), and performance-improvement efforts

QUEEN'S UNIVERSITY BELFAST

Network security testing

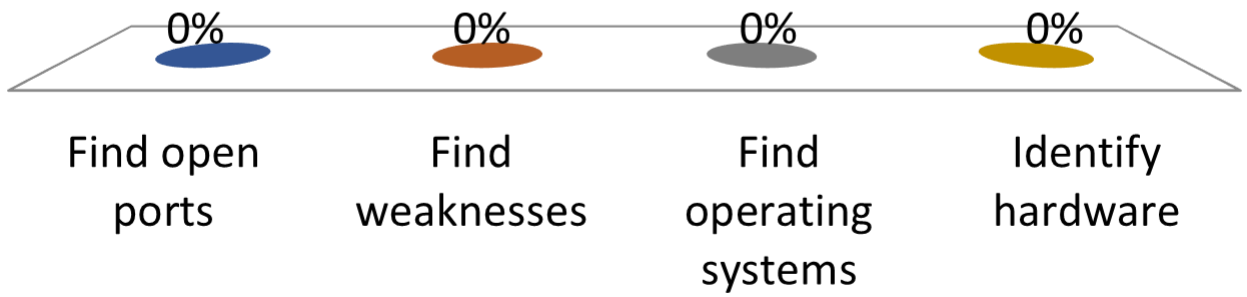
Testing techniques include:

- Network scanning
- Vulnerability scanning
- Password cracking
- Log review
- Integrity checkers
- Virus detection
- War driving (802.11 or wireless LAN testing)
- Penetration testing

QUEEN'S UNIVERSITY BELFAST

A vulnerability scan is a good way to …

A. Find open ports
✓ B. Find weaknesses
C. Find operating systems
D. Identify hardware



Summary

- Security Governance – Management, Roles & Responsibilities
- Security Policy – Types and Guidelines
- Security Standards
- Risk Management
- Access Control and Security Policy
- Security Lifecycle Management
- Network Security Testing

QUEEN'S UNIVERSITY BELFAST

Questions?

Next Session: Thursday, 14 March 2019

Incident Response/Management

QUEEN'S UNIVERSITY BELFAST