UNIVERSITY OF WESTMINSTER

Risk management, principles, Plans and procedures

6COSC019W- Cyber Security

Dr Ayman El Hajjar

March 20, 2023

School of Computer Science and Engineering
University of Westminster

OUTLINE

1. IT Security Management and Risk Assessment

2. IT Security Controls, Plans, and Procedures

IT Security Management and Risk Assessment

IT Security Management Overview

- Is the formal process of answering the questions:
  - What assets need to be protected
  - How are those assets threatened
  - What can be done to counter those threats
- Ensures that critical assets are sufficiently protected in a cost-effective manner
- Security risk assessment is needed for each asset in the organization that requires protection
- Provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified

ISO/IEC 27000 SERIES OF STANDARDS ON IT SECURITY TECHNIQUES

27000:2016	"Information security management systems - Overview and vocabulary" provides an overview of information security management systems, and defines the vocabulary and definitions used in the 27000 family of standards.
27001:2013	"Information security management systems – Requirements" specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System.
27002:2013	"Code of practice for information security management" provides guidelines for information security management in an organization and contains a list of best-practice security controls. It was formerly known as ISO17799.
27003:2010	"Information security management system implementation guidance" details the process from inception to the production of implementation plans of an Information Security Management System specification and design.
27004:2009	"Information security management – Measurement" provides guidance to help organizations measure and report on the effectiveness of their information security management system processes and controls.
27005:2011	"Information security risk management" provides guidelines on the information security risk management process. It supersedes ISO13335-3/4.
27006:2015	"Requirements for bodies providing audit and certification of information security management systems" specifies requirements and provides guidance for these bodies.

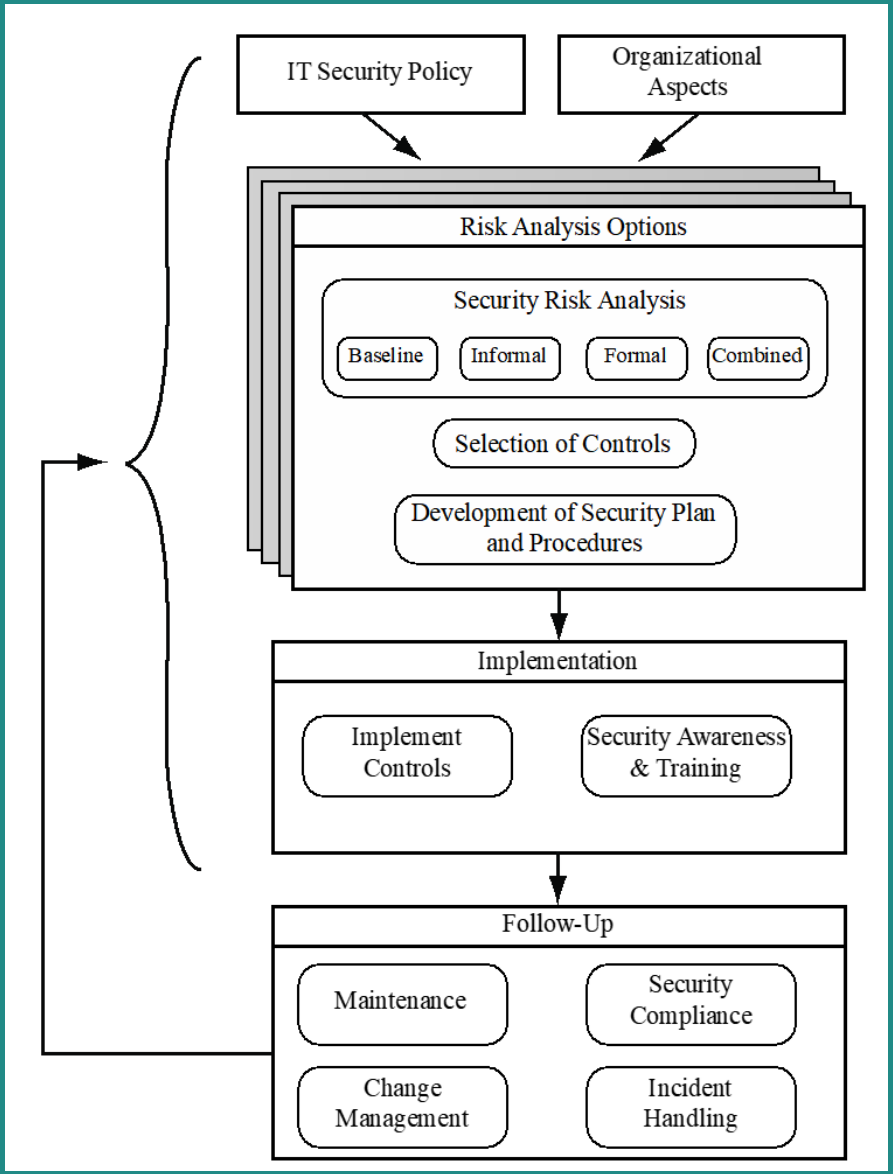
IT SECURITY MANAGEMENT

IT SECURITY MANAGEMENT

A process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability. IT security management functions include:

- Determining organizational IT security objectives, strategies, and policies
- Determining organizational IT security requirements
- Identifying and analysing security threats to IT assets within the organization
- Identifying and analysing risks
- Specifying appropriate safeguards
- Monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization
- Developing and implementing a security awareness program
- Detecting and reacting to incidents

OVERVIEW OF IT SECURITY MANAGEMENT



Organizational Context and Security Policy

- Maintained and updated regularly
  - Using periodic security reviews
  - Reflect changing technical/risk environments
- Examine role and importance of IT systems in organization

First examine organization's IT security:

- **Objectives** wanted IT security outcomes
- **Strategies** how to meet objectives
- **Policies** identify what needs to be done

Security Policy

Needs to address:

- Scope and purpose including relation of objectives to business, legal, regulatory requirements
- IT security requirements
- Assignment of responsibilities
- Risk management approach
- Security awareness and training
- General personnel issues and any legal sanctions
- Integration of security into systems development
- Information classification scheme
- Contingency and business continuity planning
- Incident detection and handling processes
- How and when policy reviewed, and change control to it

Management Support

- IT security policy must be supported by senior management
- Need IT security officer
  - To provide consistent overall supervision
  - Liaison with senior management
  - Maintenance of IT security objectives, strategies, policies
  - Handle incidents
  - Management of IT security awareness and training programs
  - Interaction with IT project security officers
- Large organizations need separate IT project security officers associated with major projects and systems
  - Manage security policies within their area

TERMINOLOGIES

- Asset:
  - ✺ : A system resource or capability of value to its owner that requires protection
- Threat:
  - ✺ : A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner
- Vulnerability:
  - ✺ : A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat
- Risk:
  - ✺ : The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner

SECURITY RISK ASSESSMENT

Critical component of process

Ideally examine every organizational asset

- Not feasible in practice

Approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline
- Informal
- Detailed risk
- Combined

Baseline Approach

- Goal is to implement agreed controls to provide protection against the most common threats
- Forms a good base for further security measures
- Use “industry best practice”
  - Easy, cheap, can be replicated
  - Gives no special consideration to variations in risk exposure
  - May give too much or too little security
- Generally recommended only for small organizations without the resources to implement more structured approaches

INFORMAL APPROACH

Involves conducting an informal, pragmatic risk analysis on organization's IT systems

Exploits knowledge and expertise of analyst

Fairly quick and cheap

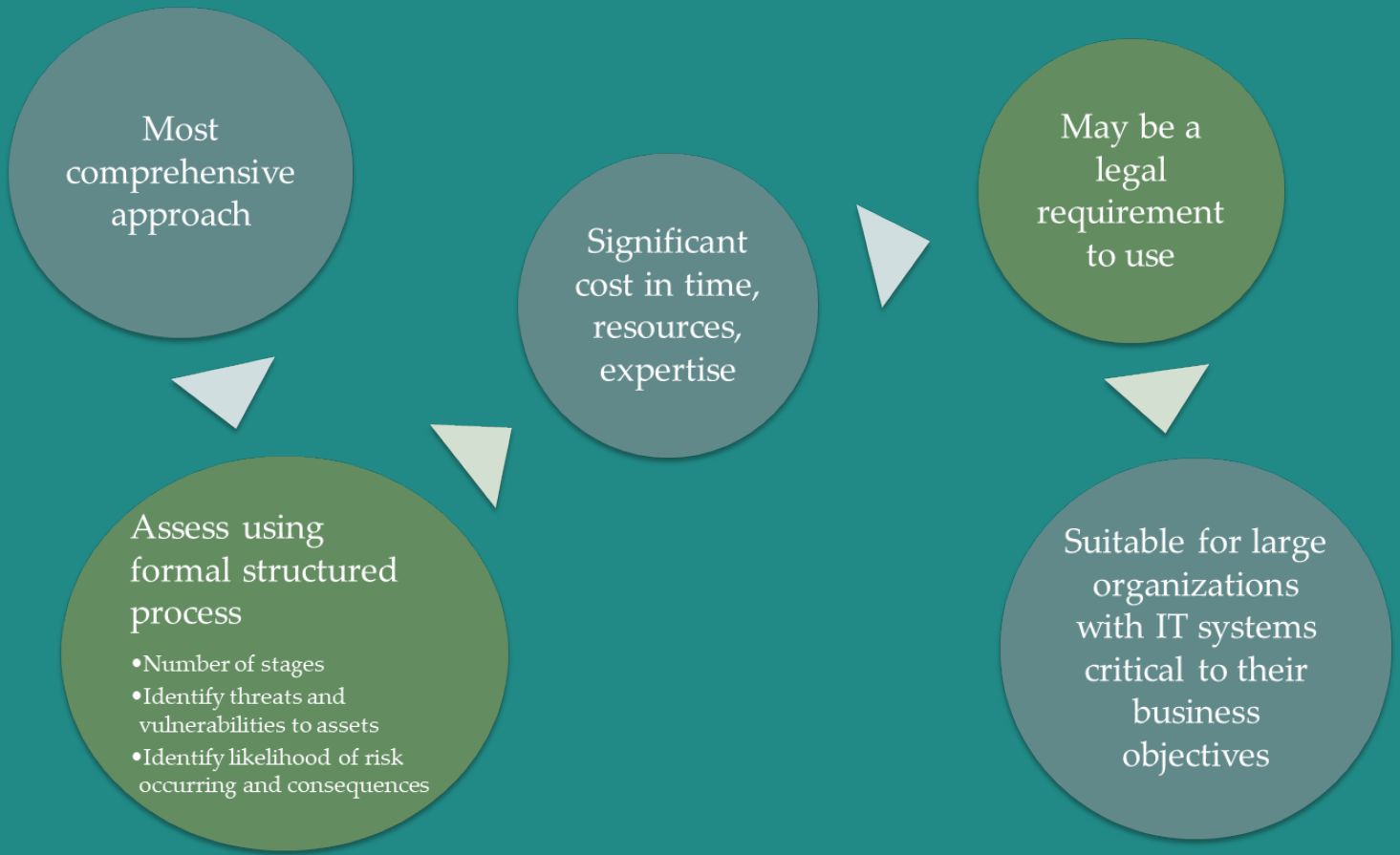
Judgments can be made about vulnerabilities and risks that baseline approach would not address

Some risks may be incorrectly assessed

Skewed by analyst's views, varies over time

Suitable for small to medium sized organizations where IT systems are not necessarily essential

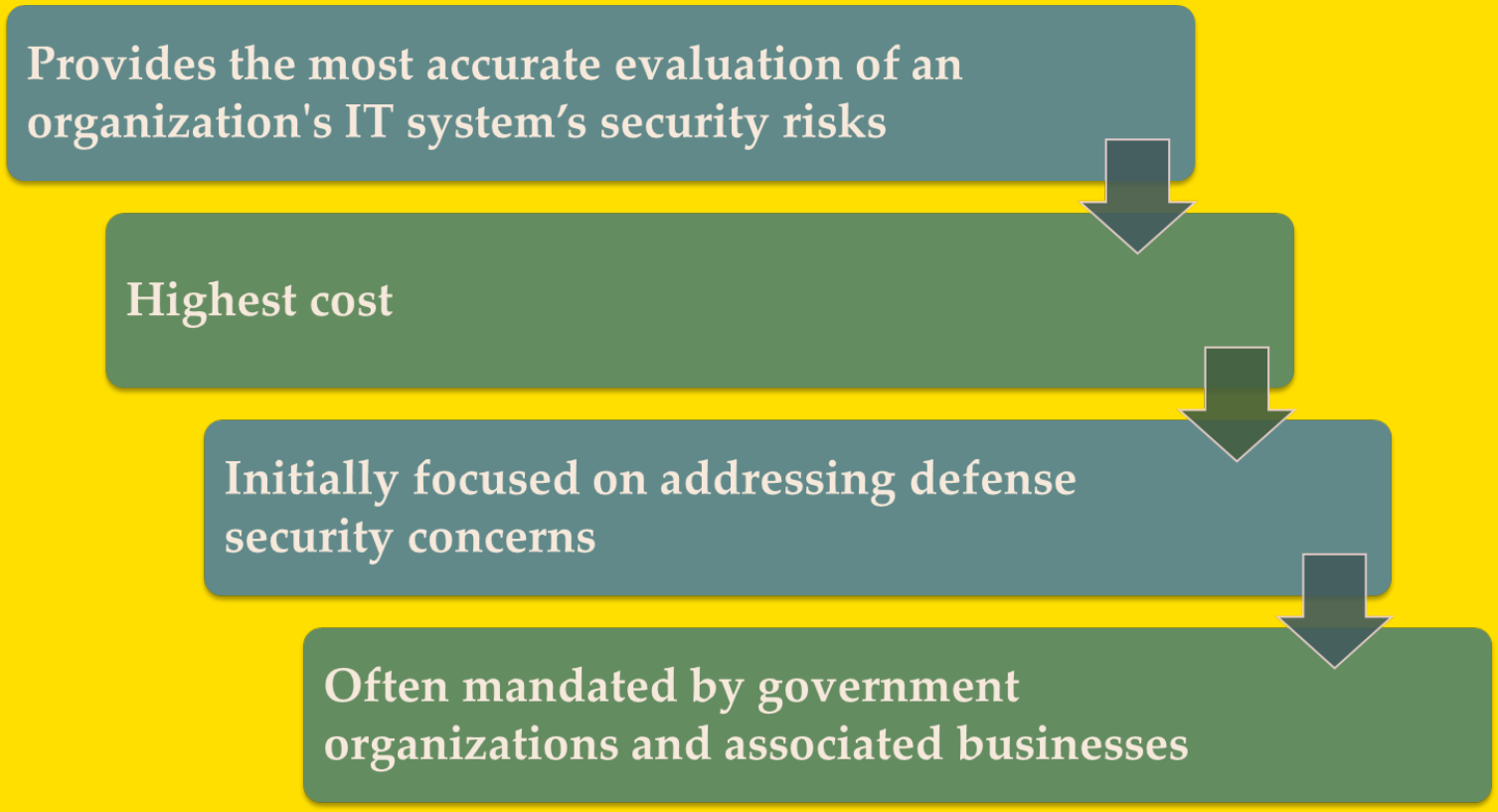
DETAILED RISK ANALYSIS



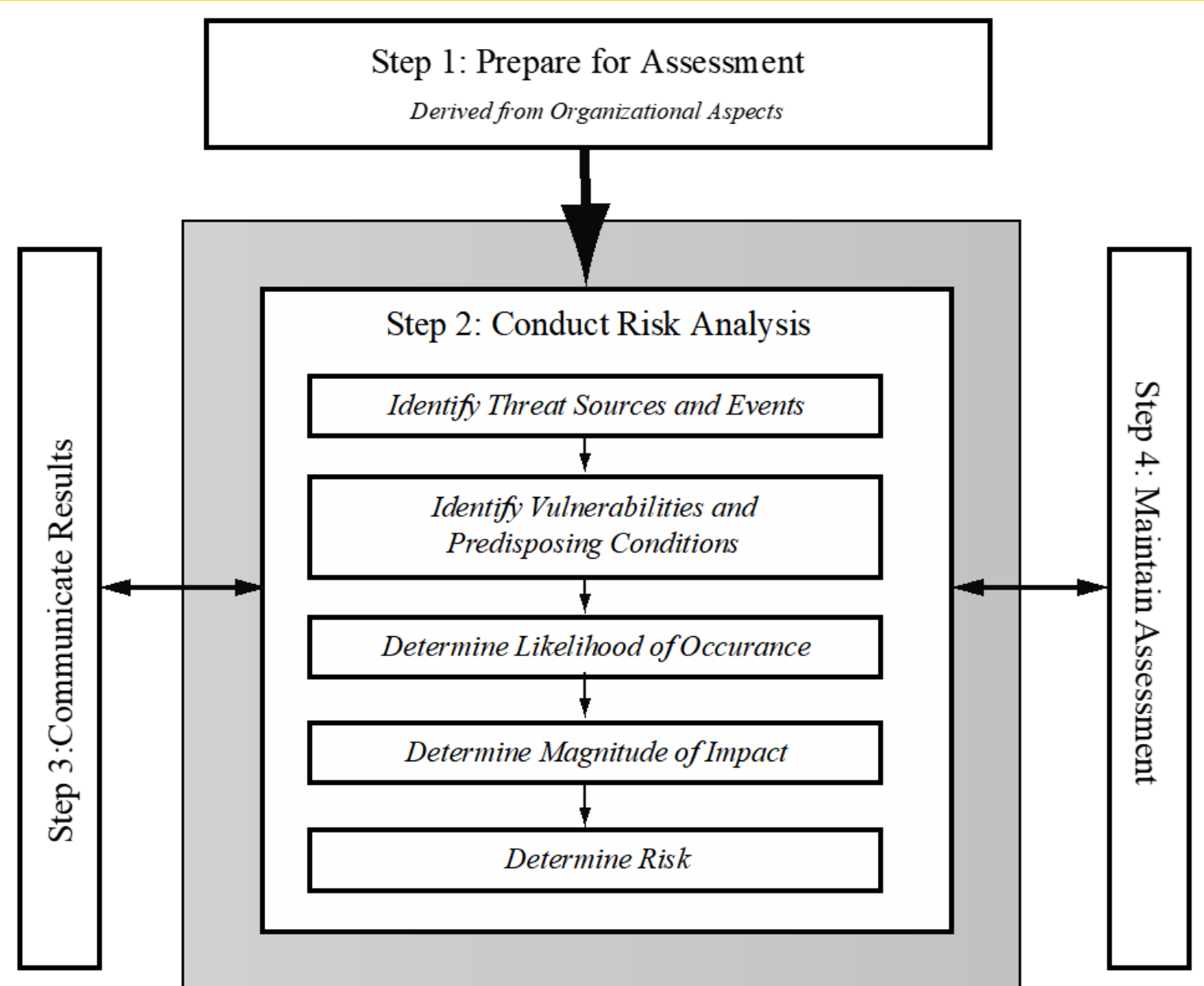
Combined Approach

- Combines elements of the baseline, informal, and detailed risk analysis approaches
- Aim is to provide reasonable levels of protection as quickly as possible then to examine and adjust the protection controls deployed on key systems over time
- Approach starts with the implementation of suitable baseline security recommendations on all systems
- Next, systems either exposed to high risk levels or critical to the organization's business objectives are identified in the high-level risk assessment
- A decision can then be made to possibly conduct an immediate informal risk assessment on key systems, with the aim of relatively quickly tailoring controls to more accurately reflect their requirements
- Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted

DETAILED SECURITY RISK ANALYSIS



RISK ASSESSMENT PROCESS



Establishing the Context

- Initial step
  - Determine the basic parameters of the risk assessment
  - Identify the assets to be examined
- Explores political and social environment in which the organization operates3
  - Legal and regulatory constraints
  - Provide baseline for organization's risk exposure
- Risk appetite
  - The level of risk the organization views as acceptable

Asset Identification

- Last component is to identify assets to examine
- Draw on expertise of people in relevant areas of organization to identify key assets
  - Identify and interview such personnel

Asset

"anything that needs to be protected" because it has value to the organization and contributes to the successful attainment of the organization's objectives

THREAT IDENTIFICATION

- A threat is:

Threat Sources

- Threats may be
  - Natural “acts of God”
  - Man-made
  - Accidental or deliberate

Evaluation of human threat sources should consider:

- Motivation
- Capability
- Resources
- Probability of attack
- Deterrence

- Any previous experience of attacks seen by the organization also needs to be considered

Vulnerability Identification

- Identify exploitable flaws or weaknesses in organization's IT systems or processes
  - Determines applicability and significance of threat to organization
- Need combination of threat and vulnerability to create a risk to an asset
- Outcome should be a list of threats and vulnerabilities with brief descriptions of how and why they might occur

Analyse Risks

- Specify likelihood of occurrence of each identified threat to asset given existing controls
- Specify consequence should threat occur
- Derive overall risk rating for each threat
  - Risk probability threat occurs x cost to organization
- Hard to determine accurate probabilities and realistic cost consequences
- Use qualitative, not quantitative, ratings

Analyse Existing Controls

- Existing controls used to attempt to minimize threats need to be identified
- Security controls include:
  - Management
  - Operational
  - Technical processes and procedures
- Use checklists of existing controls and interview key organizational staff to solicit information

RISK LIKELIHOOD

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may be deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

RISK CONSEQUENCES

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event.
4	**Major**	Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior

RISK LEVEL DETERMINATION AND MEANING

	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Risk Register

Risk Register

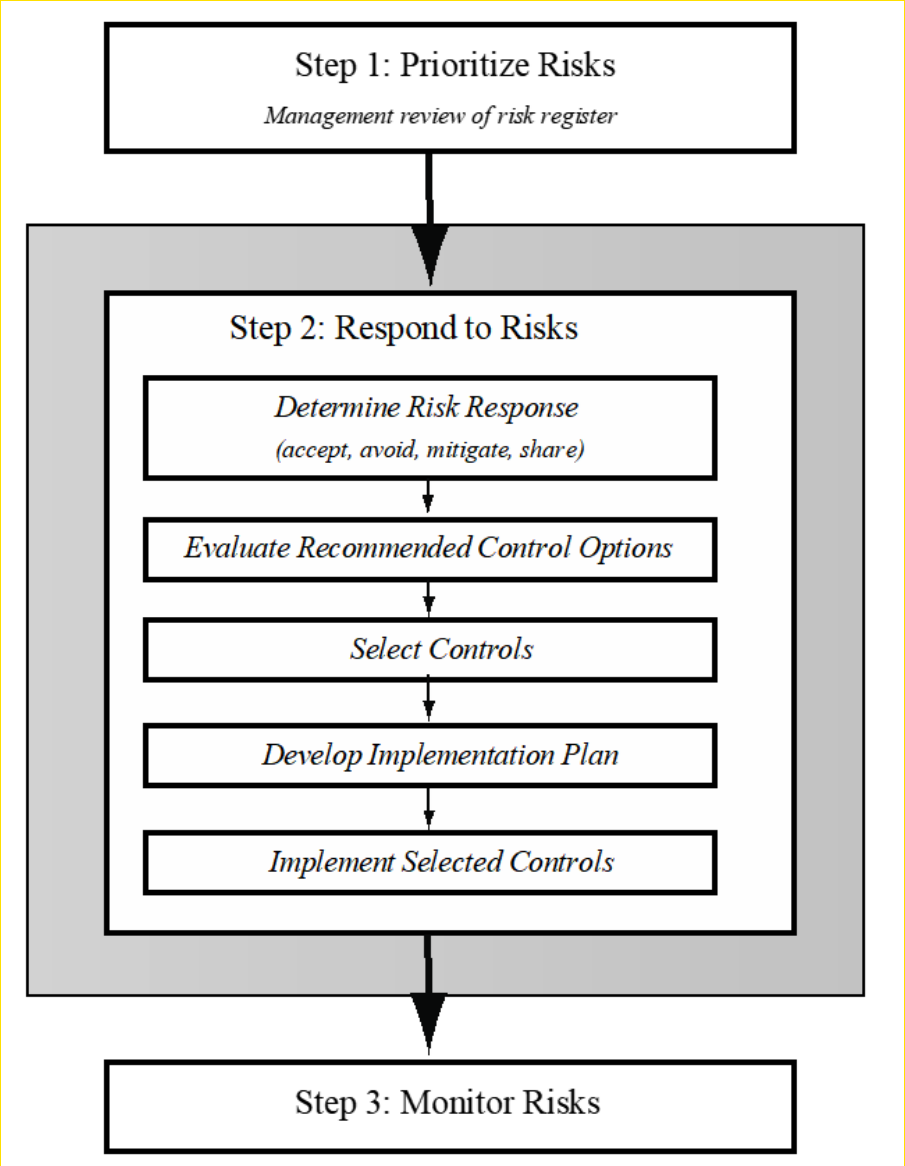
Put all of this together: The results of the risk analysis process should be documented in a risk register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet router	Outside hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of data center	Accidental fire or flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Risk Treatment Alternatives

IT Security Controls, Plans, and Procedures

IT SECURITY MANAGEMENT CONTROLS AND IMPLEMENTATION



SECURITY CONTROL

Control is defined as:

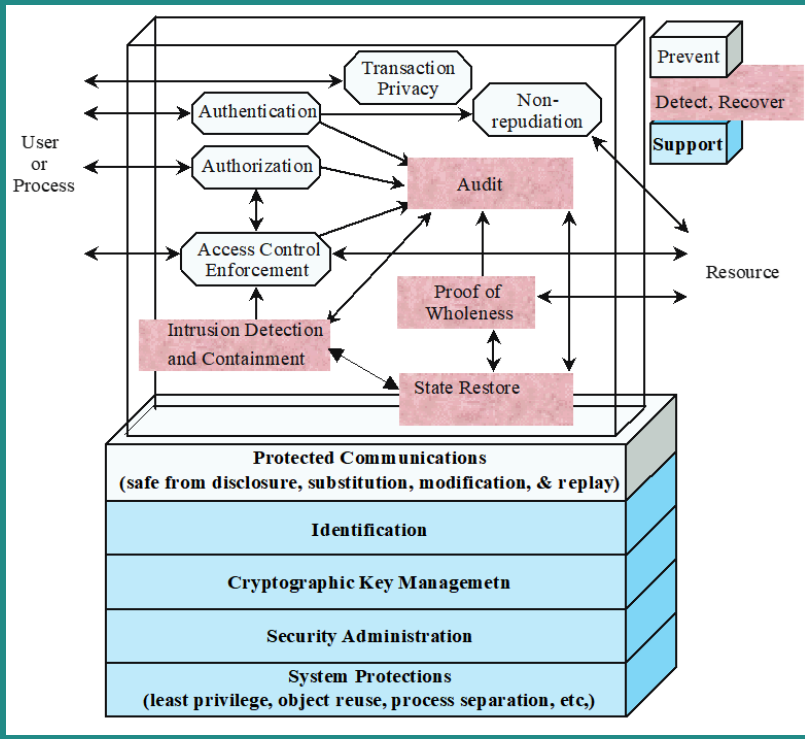
"An action, device, procedure, or other measure that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action."

CONTROL CLASSIFICATIONS

- Management controls
  - Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission
  - These controls refer to issues that management needs to address
- Operational controls
  - Address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies
  - These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems
  - They are used to improve the security of a system or group of systems

CONTROL CLASSIFICATIONS

- Technical controls
  - Involve the correct use of hardware and software security capabilities in systems
  - These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions



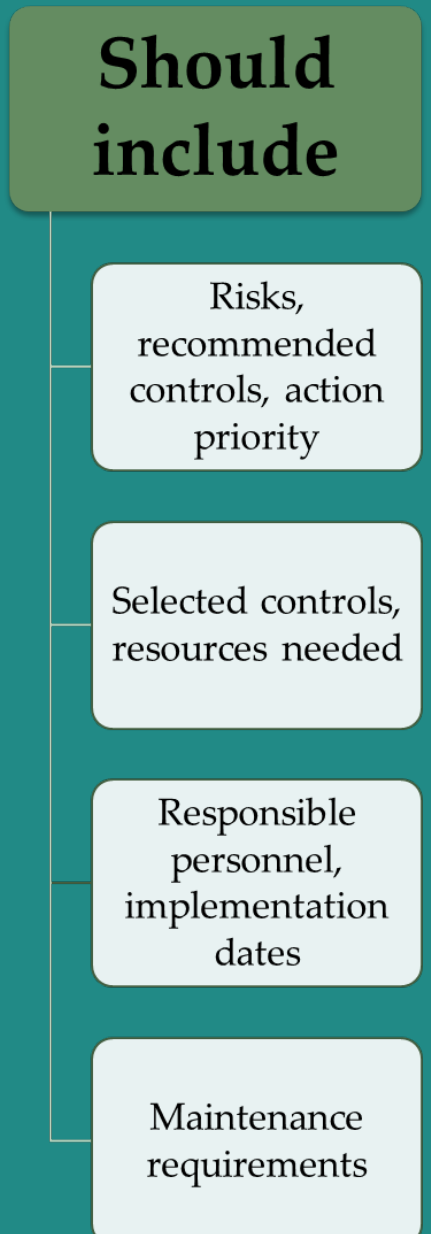
CONTROL CLASSES

Each of the control classes may include the following:

- Supportive controls
  - Pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls
- Preventative controls
  - Focus on preventing security breaches from occurring, by inhibiting attempts to violate security policies or exploit a vulnerability
- Detection and recovery controls
  - Focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources

IT Security Plan

- Provides details of:
  - What will be done
  - What resources are needed
  - Who is responsible
- Goal is to detail the actions needed to improve the identified deficiencies in the risk profile



IMPLEMENTATION PLAN

Risk (Asset/Threat)	Hacker attack on Internet router
Level of Risk	High
Recommended Controls	•Disable external telnet access •Use detailed auditing of privileged command use •Set policy for strong admin passwords •Set backup strategy for router configuration file •Set change control policy for the router configuration
Priority	High
Selected Controls	•Implement all recommended controls •Update related procedures with training for affected staff
Required Resources	•3 days IT net admin time to change & verify router configuration, write policies; •1 day of training for network administration staff
Responsible Persons	John Doe, Lead Network System Administrator, Corporate IT Support Team
Start – End Date	February 6, 2017 to February 9, 2017
Other Comments	•Need periodic test and review of configuration and policy use

SECURITY

- IT security plan documents:
  - What needs to be done for each selected control
  - Personnel responsible
  - Resources and time frame
- Identified personnel:
  - Implement new or enhanced controls
  - May need system configuration changes, upgrades or new system installation
  - May also involve development of new or extended procedures
  - Need to be encouraged and monitored by management
- When implementation is completed management authorizes the system for operational use

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **Recommended Readings note:** Focus on what was covered in the class. Other parts will come later in other lectures.
  - Chapters 14,15- Computer Security: Principles and Practice, , William Stallings and Lawrie Brown
  - Chapter 2- CyBOK, The Cyber Security Body of Knowledge