MONASH University
Information Technology

FIT2093 INTRODUCTION TO CYBER SECURITY

MONASH University
Information Technology

FIT2093 INTRODUCTION TO CYBER SECURITY

Lecture 12:
IT Risk Management

Outline

- **How IT security is managed within an organisation?**
  - Purpose
  - Function
  - Process
  - Security policy
- **IT Risk management**
  - Controls
  - Assessment for each asset
- **A case study**

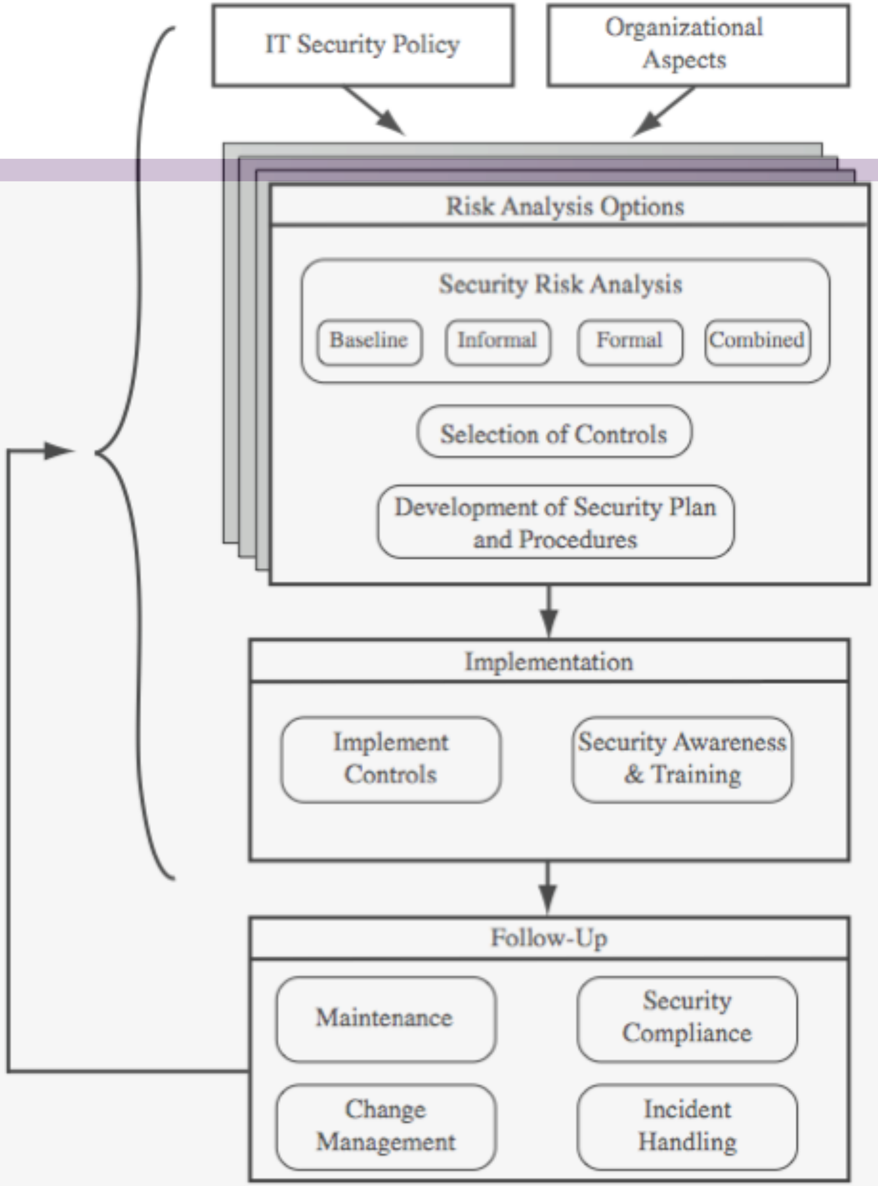
Overview

- **security requirements means asking**
  - what assets do we need to protect?
  - how are those assets threatened?
  - what can we do to counter those threats?
- **IT security management answers these**
  - 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

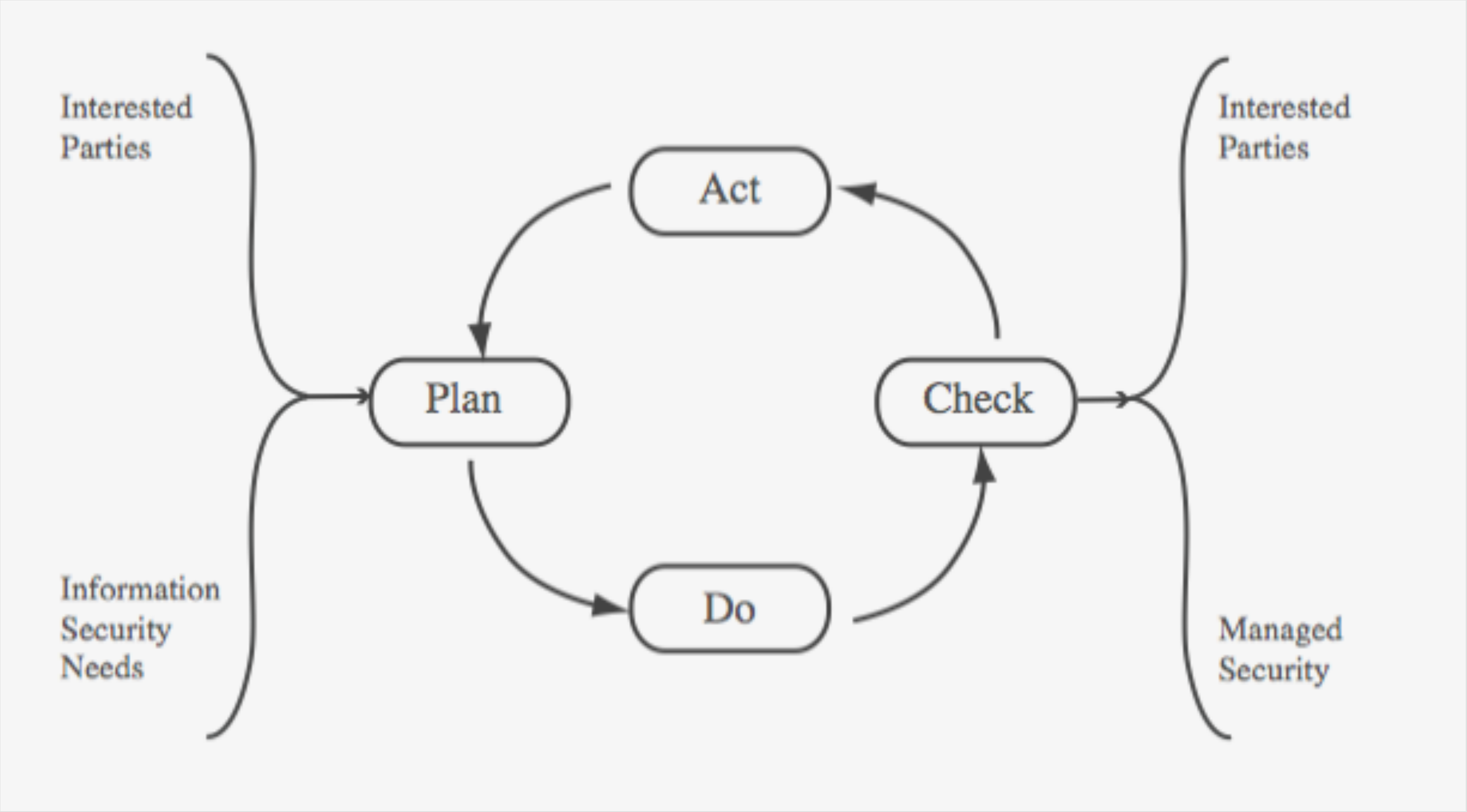
IT Security Management

- **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:**
  - organizational IT security objectives, strategies and policies
  - determining organizational IT security requirements
  - identifying and analyzing security threats to IT assets
  - identifying and analyzing risks
  - specifying appropriate safeguards
  - monitoring the implementation and operation of safeguards
  - developing and implementing a security awareness program
  - detecting and reacting to incidents

IT Security Management Process



Plan - Do - Check - Act



Organizational Context and Security Policy

- **first examine organization's IT security:**
  - objectives - wanted IT security outcomes
  - strategies - how to meet objectives
  - policies - identify what needs to be done
- **maintained and updated regularly**
  - using periodic security reviews
  - reflect changing technical / risk environments
- **examine role of IT systems in organization**

Security Policy Topics

- **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 when policy reviewed, and controlling changes 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
  - management of IT security awareness and training programs
  - interaction with IT project security officers
  - handle incidents
- **large organizations needs IT security officers on major projects / teams**
  - manage process within their areas

IT Security Risk Management

- **IT security risks should be:**
  - Identified
  - Analysed
  - Evaluated

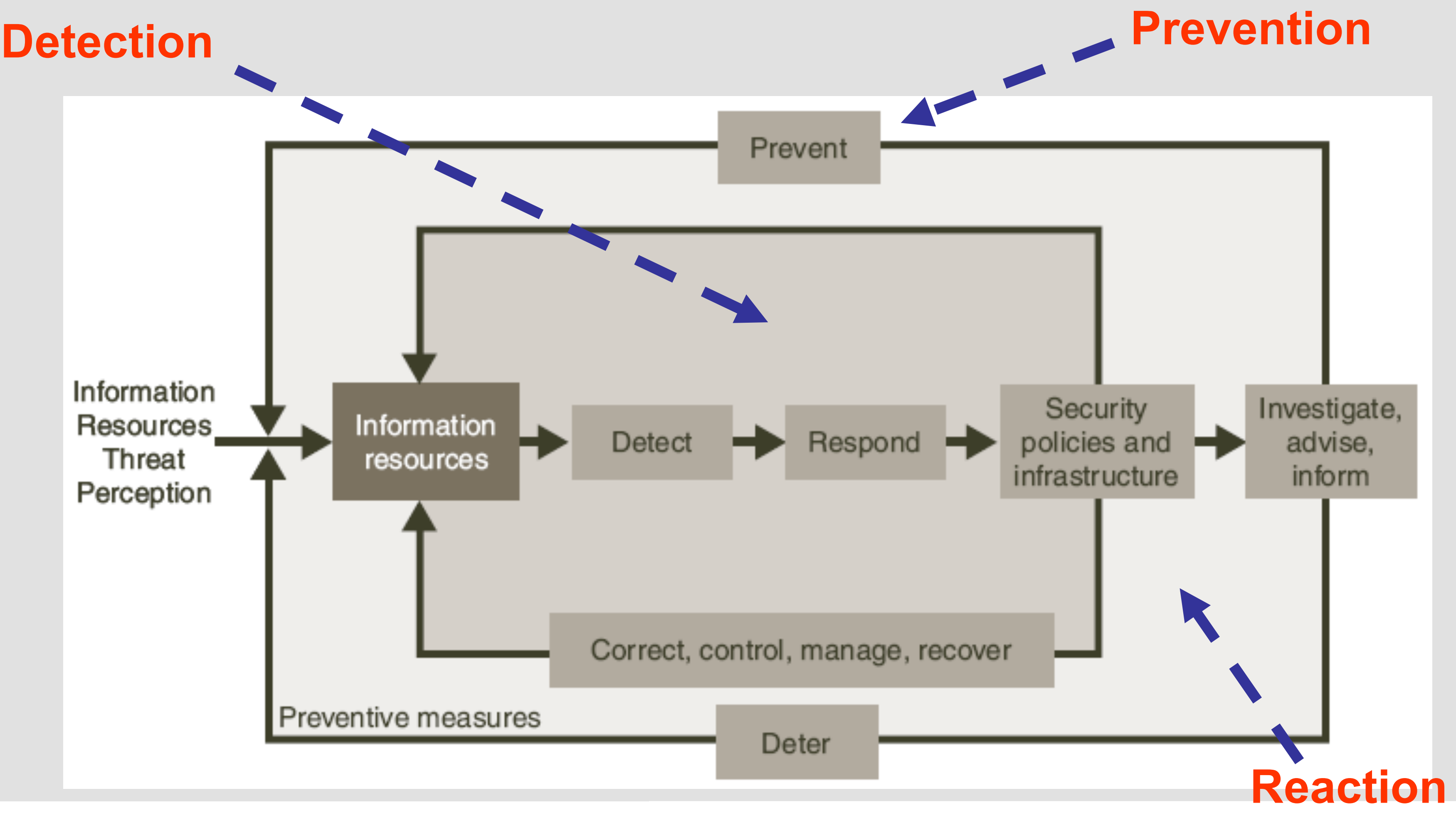
IT Security Risk Management

- **Identification**
  - – The organisation should identify risks under its control and those beyond its control
  - – Risks can also be categorised as either natural or initiated by humans
- **Analysis**
  - – This helps determine acceptable and unacceptable risks as well as how to control them

Strategic IT Security and Risk Management

- **Evaluation**
  - Risks are evaluated on the basis of the ***likelihood*** of eventuating and the ***consequences***
  - These two factors can be used to prioritise risk management

Layered Approach to IT Security


Detection
Prevention
Prevent
Information Resources Threat Perception
Information resources
Detect
Respond
Security policies and infrastructure
Investigate, advise, inform
Correct, control, manage, recover
Preventive measures
Deter
Reaction

Protecting information and information systems

- **The type of controls that can be applied to protect the information (and to provide IT security) can be classified into 3 groups:**
  - Technical controls
  - Management controls
  - Operational controls

Technical controls

- Controls used at machine or network level
- They prevent risk event and detect a security breach
- Technical controls can be supportive, preventive, as well as detection (and recovery) controls

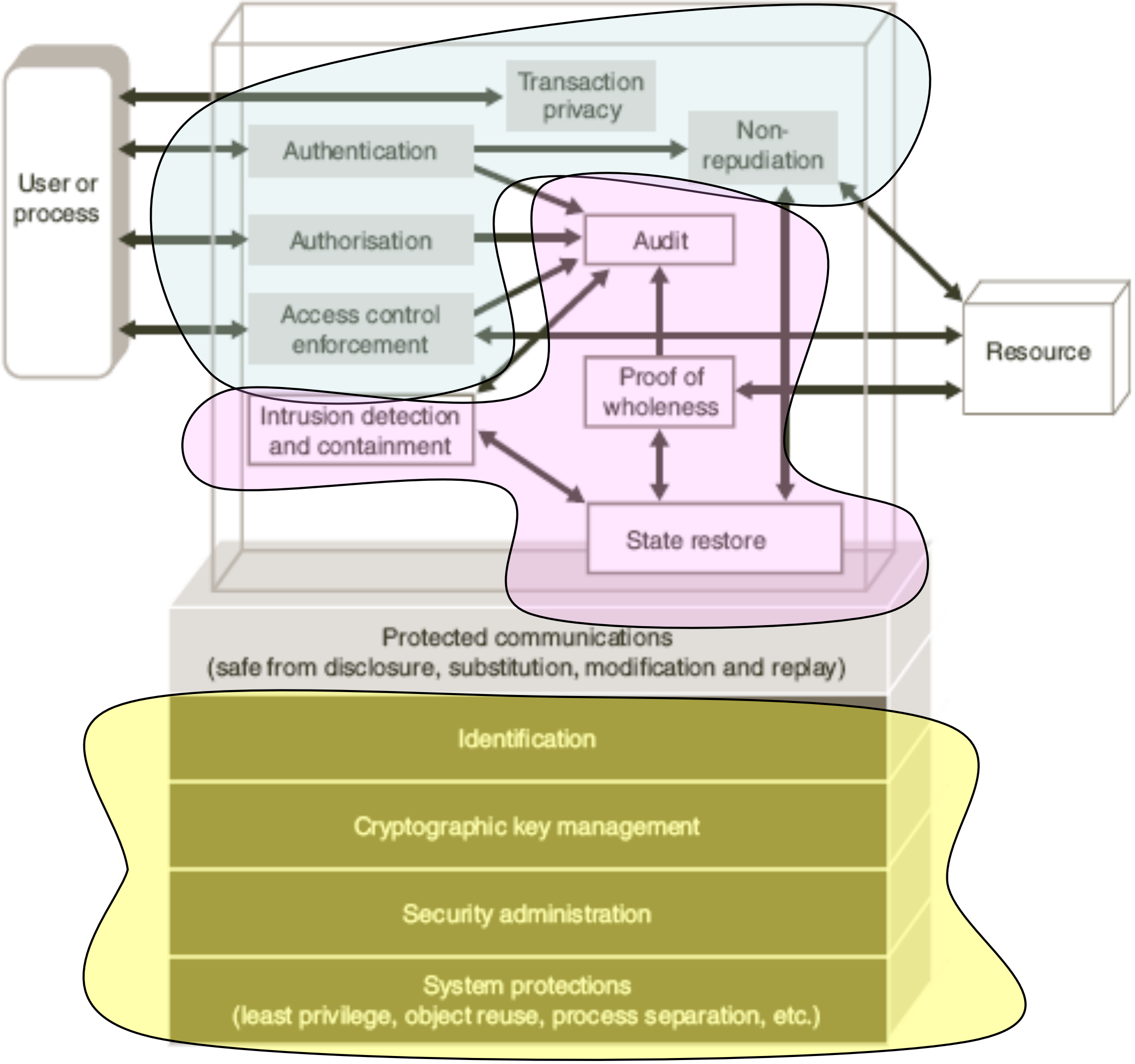
Technical Control Security Architecture

Source: National Institute of Standards and Technology (NIST) 2002, p. 33.

support

prevention

detect, recover


User or process
Transaction privacy
Authentication
Non-repudiation
Authorisation
Audit
Access control enforcement
Resource
Proof of wholeness
Intrusion detection and containment
State restore
Protected communications (safe from disclosure, substitution, modification and replay)
Identification
Cryptographic key management
Security administration
System protections (least privilege, object reuse, process separation, etc.)

Technical Controls

- **Supportive technical controls**
  - Derived from security policy, information systems policy or IT policy and define the IT resources to be used
- **Preventive technical controls**
  - Intended to limit violation of information resources security policy

Technical Controls

- **Detective and corrective technical controls**
  - Warn when violations or attempts made to breach security
  - Corrective controls attempt to enable recovery

Management Controls

- **Are in the form of policies**
- **Aimed at managing IT resources and controlling the business process**
- **Enforced by information security polices and guidelines**

Management Controls

- **Preventive**
  - include policies ensuring security guidelines are followed
- **Detective and corrective controls**
  - Focus on continuously assessing risks in the risk environment
  - Deal with the provision of finance and infrastructure for recovery

Operational Controls

- **Preventive operational controls**
  - – Include physical protection of hard drives from theft or destruction
- **Detective and corrective operational controls**
  - – Controls to detect security breaches, e.g. alarms, smoke detectors etc
  - – Corrective deals with providing financial resources and physical infrastructure for recovery.

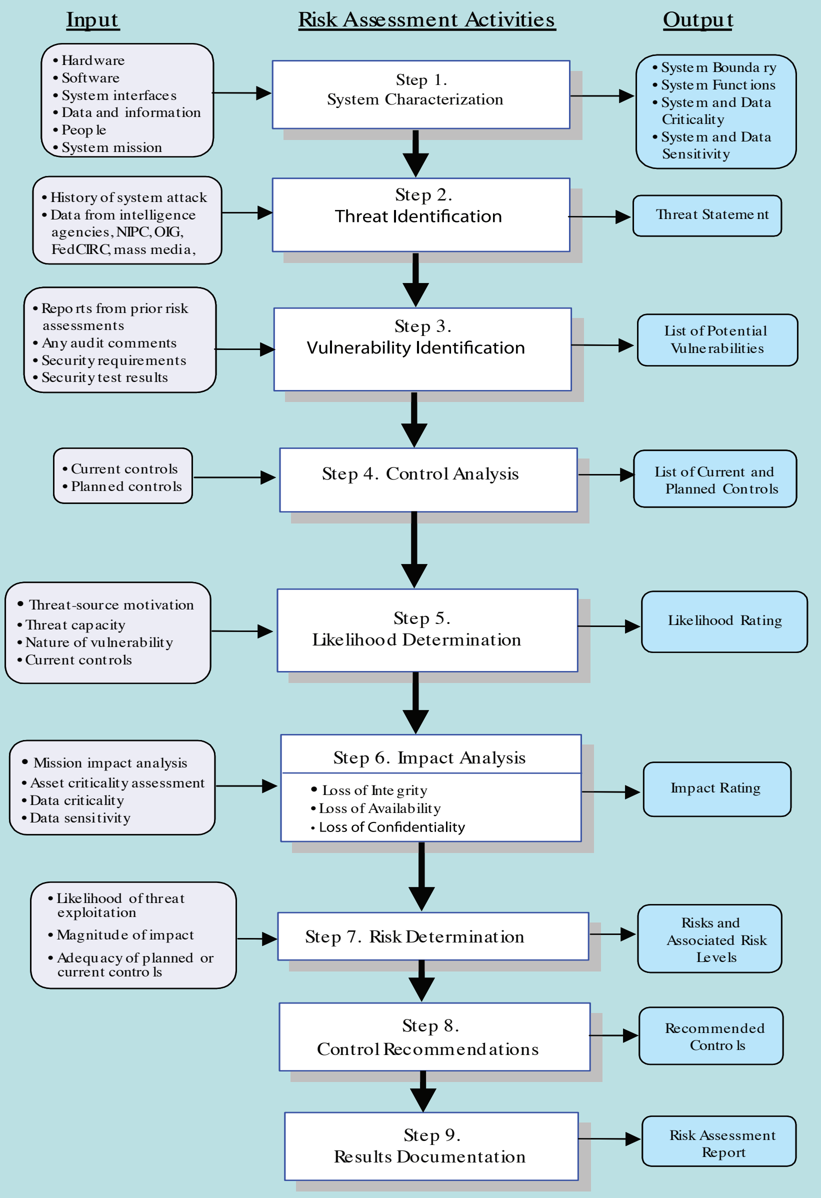
Security Risk Assessment

- **critical component of process**
  - else may have vulnerabilities or waste money
- **ideally examine every asset verses risk**
  - not feasible in practice
- **approaches to identifying and mitigating risks to an organization’s IT infrastructure:**
  - Baseline : use industry best practice
  - Informal : informal, exploits expertise of experts
  - detailed risk
  - combined

Detailed Risk Analysis

- **most comprehensive approach**
- **assess using formal structured process**
  - with a number of stages
  - identify likelihood of risk and consequences
  - hence have confidence controls appropriate
- **costly and slow, requires expert analysts**
- **may be a legal requirement to use**
- **suitable for large organizations with IT systems critical to their business objectives**

Detailed Risk Analysis Process



Input

Risk Assessment Activities

Output

- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission

Step 1.
System Characterization

- System Boundary
- System Functions
- System and Data Criticality
- System and Data Sensitivity

- History of system attack
- Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,

Step 2.
Threat Identification

Threat Statement

- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results

Step 3.
Vulnerability Identification

List of Potential Vulnerabilities

- Current controls
- Planned controls

Step 4. Control Analysis

List of Current and Planned Controls

- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Step 5.
Likelihood Determination

Likelihood Rating

- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Step 6. Impact Analysis
- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

Impact Rating

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Step 7. Risk Determination

Risks and Associated Risk Levels

Step 8.
Control Recommendations

Recommended Controls

Step 9.
Results Documentation

Risk Assessment Report

Figure 14.3 Risk Assessment Methodology

Establish Context

- **determine broad risk exposure of org**
  - related to wider political / social environment
  - and legal and regulatory constraints
  - provide baseline for organization’s risk exposure
- **specify organization’s risk appetite**
- **set boundaries of risk assessment**
  - partly on risk assessment approach used
- **decide on risk assessment criteria used**
  - identify the assets to be examined
  - knowledge and experience of those performing the analysis may determine the criteria used.

Asset Identification

- **identify assets**
  - “anything which needs to be protected”
  - of value to organization to meet its objectives
  - tangible or intangible
  - in practice try to identify significant assets
- **draw on expertise of people in relevant areas of organization to identify key assets**
  - identify and interview such personnel
  - see checklists in various standards

Terminology

asset: anything that has value to the organization

threat: a potential cause of an unwanted incident which may result in harm to a system or organization

vulnerability: a weakness in an asset or group of assets which can be exploited by a threat

risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Threat Identification

- **to identify threats or risks to assets ask**
  - who or what could cause it harm?
  - how could this occur?
- **threats are anything that hinders or prevents an asset providing appropriate levels of the key security services:**
  - confidentiality, integrity, availability, accountability, authenticity and reliability
- **assets may have multiple threats**

Threat Sources

- **threats may be**
  - natural “acts of god”
  - man-made and either accidental or deliberate
- **should consider human attackers:**
  - motivation
  - capability
  - resources
  - probability of attack
  - deterrence
- **any previous history of attack on org**

Threat Identification

- **depends on risk assessors experience**
- **uses variety of sources**
  - natural threat chance from insurance stats
  - lists of potential threats in standards, IT security surveys, info from governments
  - tailored to organization’s environment
  - and any vulnerabilities in its IT systems

Vulnerability Identification

- identify exploitable flaws or weaknesses in organization's IT systems or processes
- hence determine applicability and significance of threat to organization
- note 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

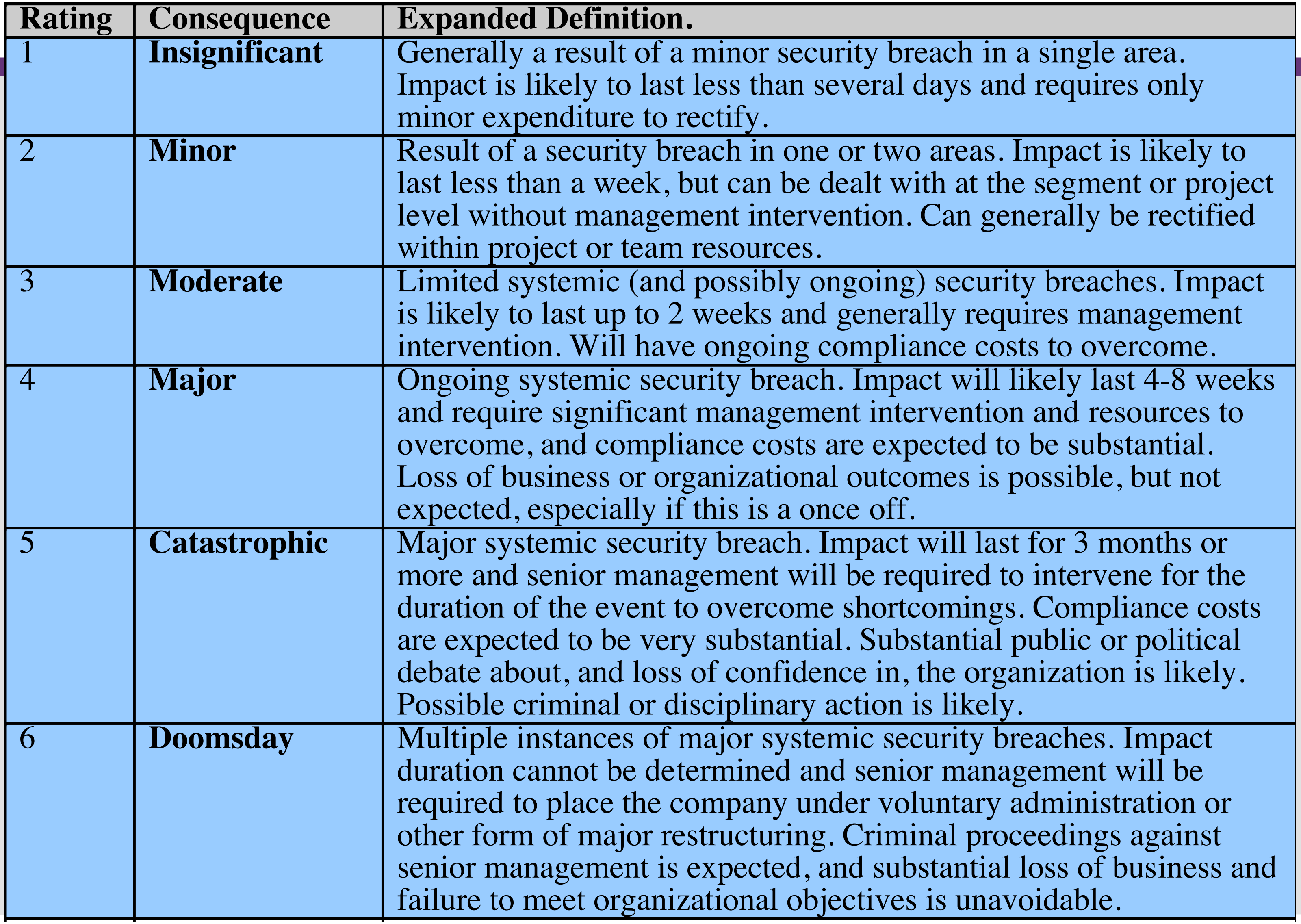
Analyse Risks

- **specify likelihood of occurrence of each identified threat to asset given existing controls**
  - management, operational, technical processes and procedures to reduce exposure of org to some risks
- **specify consequence should threat occur**
- **hence derive overall risk rating for each threat**
  - risk = probability threat occurs x cost to organization
- **in practice very hard to determine exactly**
- **use qualitative not quantitative, ratings for each**
- **aim to order resulting risks in order to treat them**

Determine Likelihood

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may 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.

Determine Consequence



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.
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.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and generally requires management intervention. Will have ongoing compliance costs to overcome.
4	**Major**	Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome, and compliance costs are expected to be substantial. 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. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable.

Determine Resultant Risk

	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.

Document in Risk Register and Evaluate Risks

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

- **risk acceptance**
  - Management must then accept responsibility for the consequences to the organization should the risk eventuate.
- **risk avoidance**
  - not proceeding with the activity or system which creates this risk
- **risk transferal**
  - sharing responsibility for the risk with a third-party
- **reduce consequence**
  - by modifying the structure or use of the assets at risk to reduce the impact should the risk occur
- **reduce likelihood**
  - by implementing suitable controls to lower the chance of the vulnerability being exploited

Case Study: Silver Star Mines

- **fictional operation of global mining company**
- **large IT infrastructure**
  - both common and specific software
  - some directly relates to health & safety
  - formerly isolated systems now networked
- **decided on formal risk assessment by security analyst**
- **mining industry less risky end of spectrum**
- **subject to legal / regulatory requirements**
- **management accepts moderate or low risk**

Assets

- **reliability and integrity of SCADA nodes and net**
- **integrity of stored file and database information**
- **availability, integrity of financial system**
- **availability, integrity of procurement system**
- **availability, integrity of maintenance/production system**
- **availability, integrity and confidentiality of mail services**

MONASH University
Information Technology

Threats & Vulnerabilities

- **unauthorized modification of control system**
- **corruption, theft, loss of DB info**
- **attacks/errors affecting financial system**
- **attacks/errors affecting procurement system**
- **attacks/errors affecting maintenance/production system**
- **attacks/errors affecting e-mail system**

Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	layered firewalls & servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	firewall, policies	Possible	Major	Extreme	2
Availability and integrity of Financial System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	3
Availability and integrity of Procurement System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	4
Availability and integrity of Maintenance/ Production System	Attacks/errors affecting system	firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	firewall, ext mail gateway	Almost Certain	Minor	High	6

Summary

- **detailed need to perform risk assessment as part of IT security management process**
- **presented risk assessment**
- **detailed risk assessment process involves**
  - context including asset identification
  - identify threats, vulnerabilities, risks
  - analyse and evaluate risks
- **Silver Star Mines case study**

Further Reading

- **Chapter 14 of the textbook: *Computer Security: Principles and Practice" by William Stallings & Lawrie Brown,* Prentice Hall, 2015**

- **Acknowledgement: part of the materials presented in the slides was developed with the help of Instructor' s Manual and other resources made available by the author of the textbook.**