COS30015 IT Security

Week 10

Presented by Ms Yicun Tian

9 October 2024

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Guest Lectuer

Mr. Matt Siomos will deliver a guest lecture on "**How to land your first cyber role in industry and how to succeed**" this Wednesday.

- Bio: Matt has been in the IT/ cyber security industry for over 20 years and has managed cyber attacks for well-known companies across Australia. He has built security operations centres for multiple managed security services providers to detect and respond to cyber-attacks and managed security governance, risk, and compliance programs for many Australian businesses.

Risk

SWINBURNE UNIVERSITY OF TECHNOLOGY

Cyber Risk

Risk is a driving factor across multiple cyber viewpoints

Let’s consider two perspectives on risk

- Risk itself can be considered exposure to danger, harm, loss, negative impact
- Loss of confidentiality, integrity, or availability of information, data, or information (or control) systems
  - potential adverse impacts to organisational operations and assets, individuals, other organizations, and the Nation
- Potential Impact of Threat x Attack Likelihood = Cyber Risk
- The existence of risk requires it to be framed, assessed, respond and monitored
  - Components of Risk management
  - Multitiered Risk Management

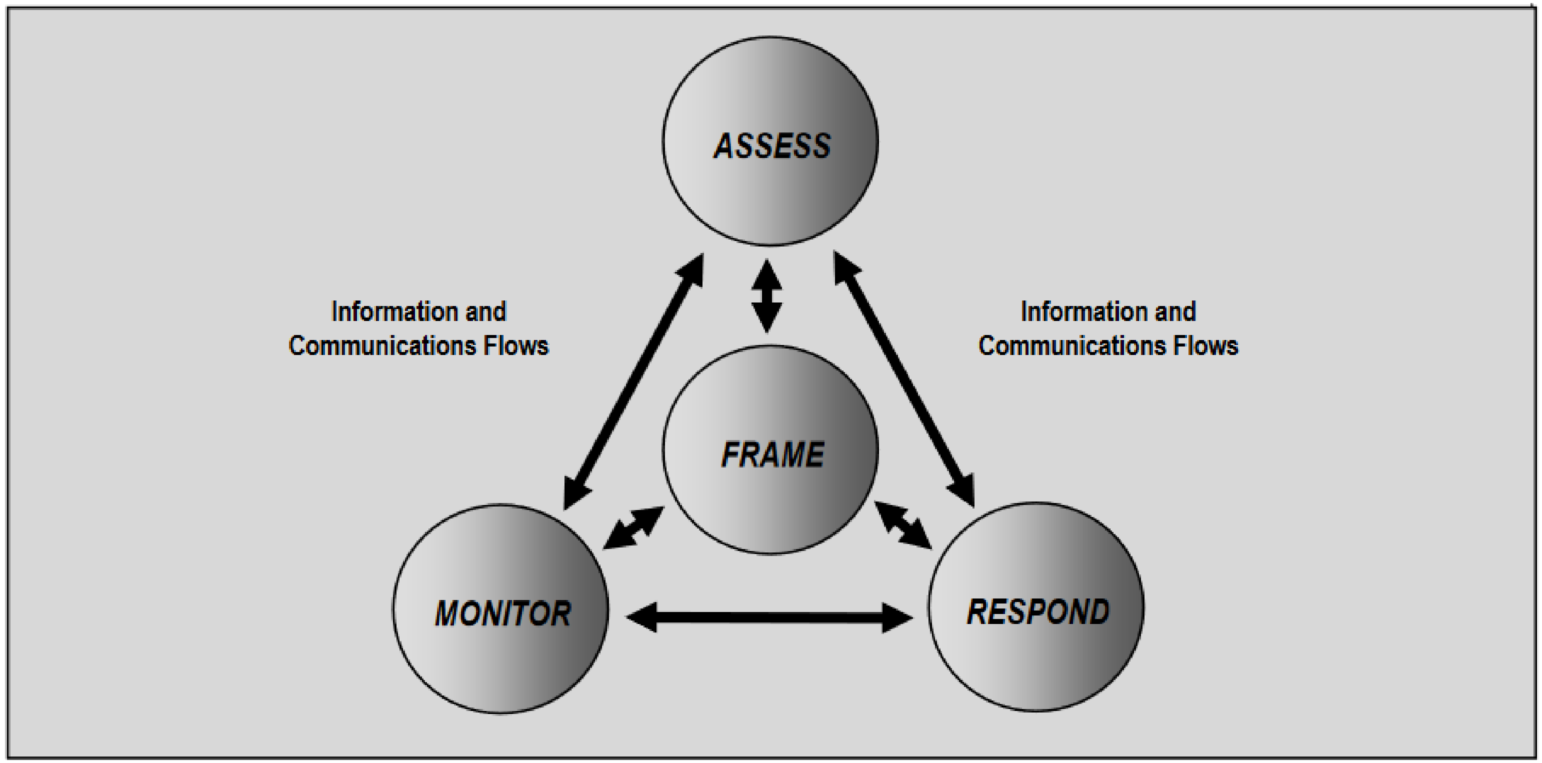
https://csrc.nist.gov/glossary/term/cybersecurity_risk

https://www.tenable.com/principles/cyber-risk-principles#chapter-2

Risk Management

Components

- Frame or “describing the environment in which risk-based decisions are made”
  - Assumptions, constraints, priorities
- Assess
  - Assess given framing context
- Respond
  - Develop to implement risk response
- Monitor
  - Verify, ongoing effectiveness, changes


ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

https://csrc.nist.gov/glossary/term/cybersecurity_risk

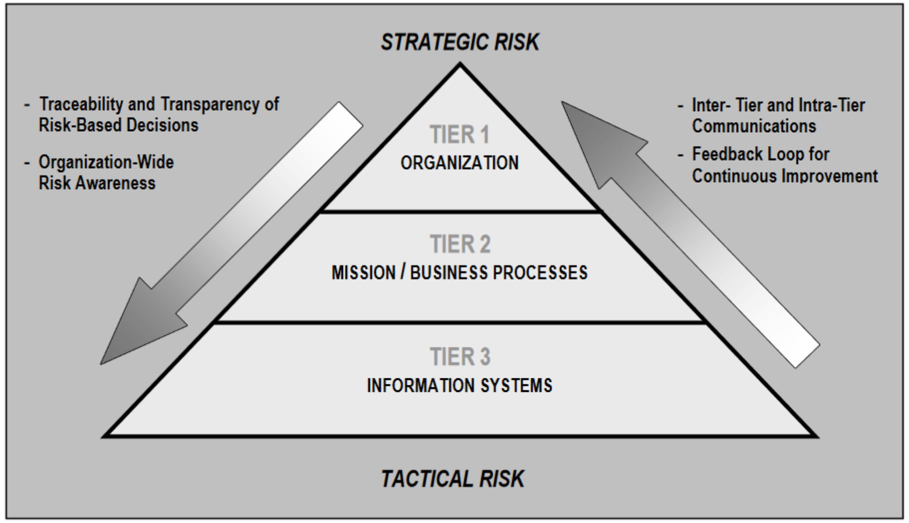
Risk Management

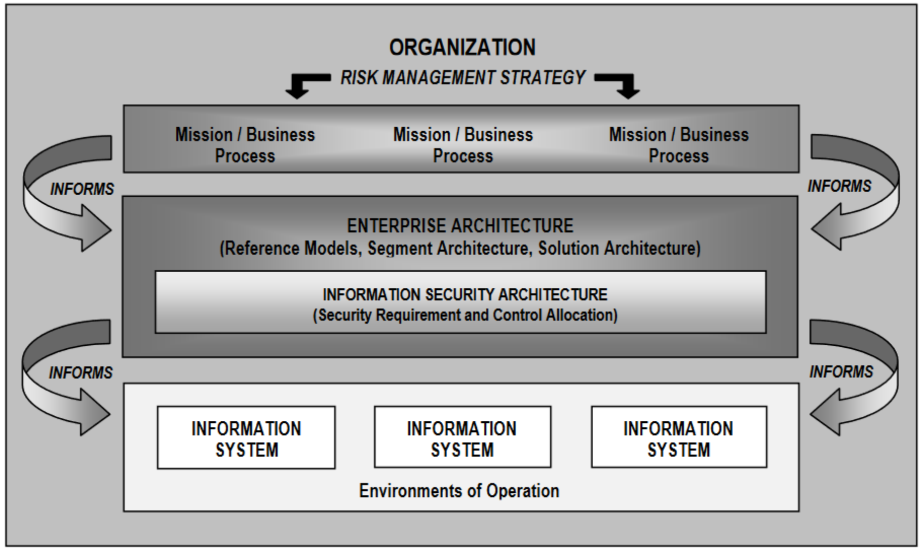
Multitiered Risk Management

Three level approach

- Tier 1
  - Organisation risk, Framing
- Tier 2
  - Risk associated with business/mission processes
  - Information/Information security of business
  - Enterprise architecture
- Tier 3
  - Risk associated for information system
  - Controls aligned to architecture
  - Managing and monitoring

https://csrc.nist.gov/glossary/term/cybersecurity_risk


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TACTICAL RISK

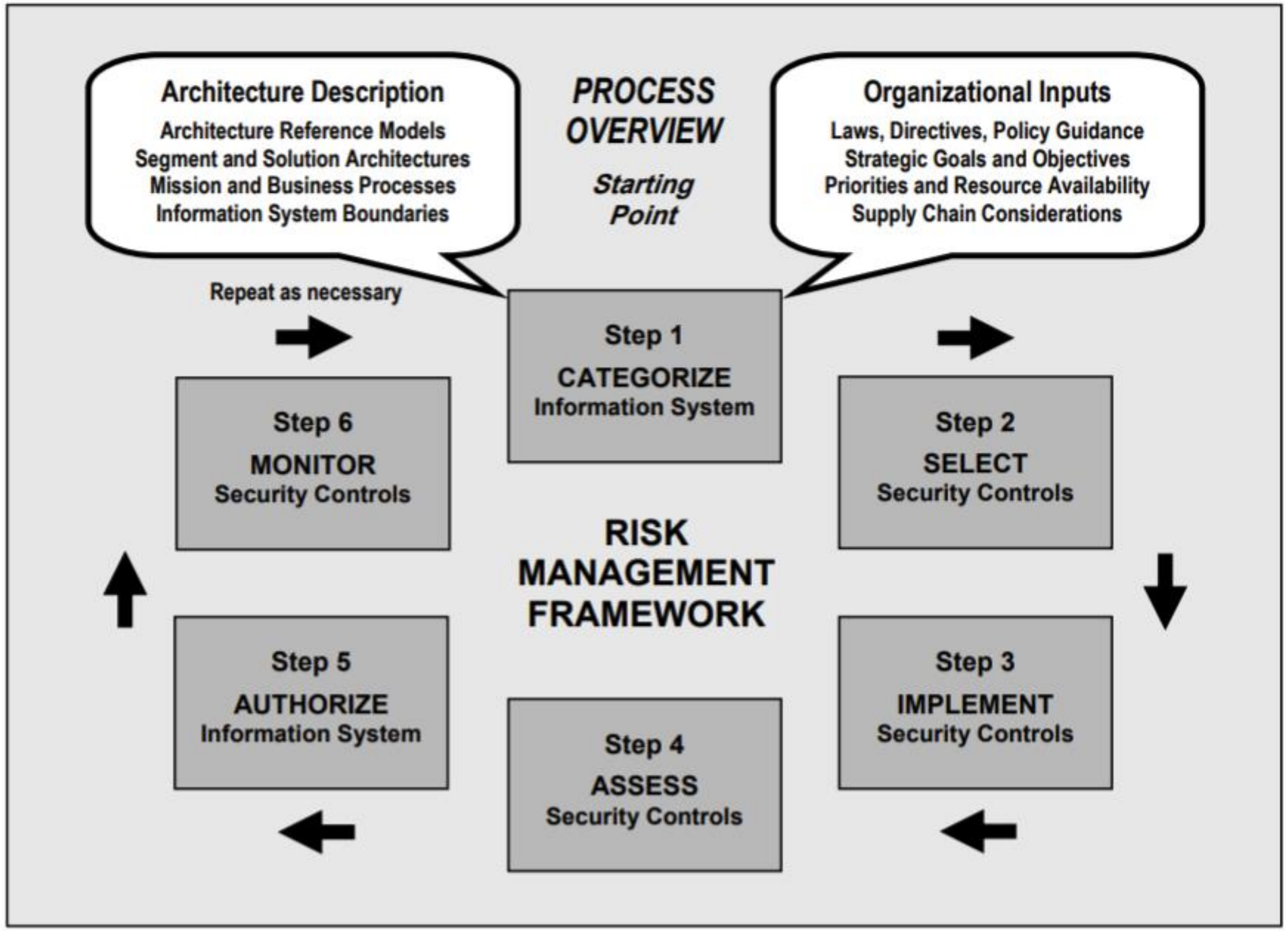

ORGANIZATION
RISK MANAGEMENT STRATEGY
Mission / Business Process
Mission / Business Process
Mission / Business Process
INFORMS
INFORMS
ENTERPRISE ARCHITECTURE
(Reference Models, Segment Architecture, Solution Architecture)
INFORMATION SECURITY ARCHITECTURE
(Security Requirement and Control Allocation)
INFORMS
INFORMS
INFORMATION SYSTEM
INFORMATION SYSTEM
INFORMATION SYSTEM
Environments of Operation

Risk Management Framework

NIST

Cyclical Approach

- Categorise
- Select
- Implement
- Assess
- Authorise
- Monitor


Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

https://csrc.nist.gov/glossary/term/cybersecurity_risk

Risk Management

Categorising issues

Consequence Rating	Sample Interpretation
Insignificant	Little disruption Managed through standard business operations, broad stakeholders Minor effort required for technology in use
Minor	Minor disruption Availability of service is restricted Receiving key stakeholder, management attention
Moderate	Some inconvenience Availability of service is compromised severely Moderate effort required for alternative solution implementation Activities or service receiving public criticism from key stakeholders
Major	Noticeable user impact Some core services unavailable Potential for serious distress or minor injury Sustainability of current operations receives sustained criticism from majority portion of key stakeholders
Catastrophic	Community unable to function without significant support Key technologies no longer available and no viable alternative exists Potential for major injury or fatalities Irreparable damage to relationships with key stakeholders and potential for organisation to cease operating in current form

Risk Management

Likelihood

Recall impact and likelihood?

Likelihood Rating	Example Interpretation
Almost certain	The event is expected to occur. (e.g., 1 incident every month)
Likely	The event will probably occur. (e.g., 1 incident every 6 months)
Possible	The event should occur at some time. (e.g., 1 incident every year)
Unlikely	The event could occur at some time. (e.g., 1 incident every 2 years)
Rare	The event may occur only in exceptional circumstances. (e.g., 1 incident every 5 or more years)

Cyber Risk Matrix

Potential Impact of Threat x Attack Likelihood = Cyber Risk

	Rare	Unlikely	Possible	Likely	Almost Certain
Insignificant	Very Low	Very Low	Very Low	Low	Low
Minor	Very Low	Low	Low	Low	Low
Moderate	Low	Medium	Medium	Medium	Medium
Major	Medium	Medium	High	High	High
Catastrophic	High	High	Extreme	Extreme	Extreme

Thank You

SWINBURNE
UNIVERSITY OF
TECHNOLOGY