IS4231
Information Security Management

Lecture 3

Governance and Planning for Security

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Email: yanglu@comp.nus.edu.sg :: **Tel**: 6516 6791 :: **Office**: COM2-02-46

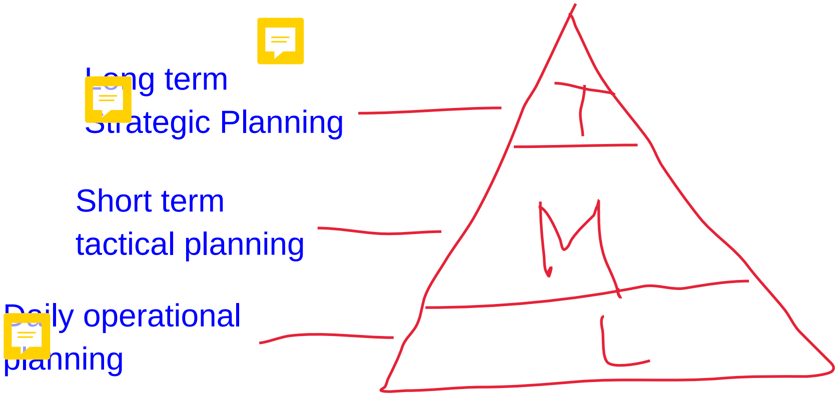
Learning Objectives

- Strategic organizational planning for information security (InfoSec)
- Information security implementation approach
- Discuss the importance of information security governance

Strategic Planning

Strategic Planning

- Strategic planning
  - Lays out the long-term direction to be taken by the organization
  - Guides organizational efforts by focusing resources on specific, clearly defined goals
  - May have to be revised or updated due to an ever-changing environment



Long term
Strategic Planning

Short term
tactical planning

Daily operational
planning

Creating a Strategic Plan

- A clearly directed strategy flows from top to bottom, and a systematic approach is required to translate it into a program that can inform and lead all members of the organization
- Organization develops a general strategy
  - Then creates specific strategic plans for major divisions
  - Each level or division translates those objectives into more specific objectives for the level below

Top-down Strategic Planning

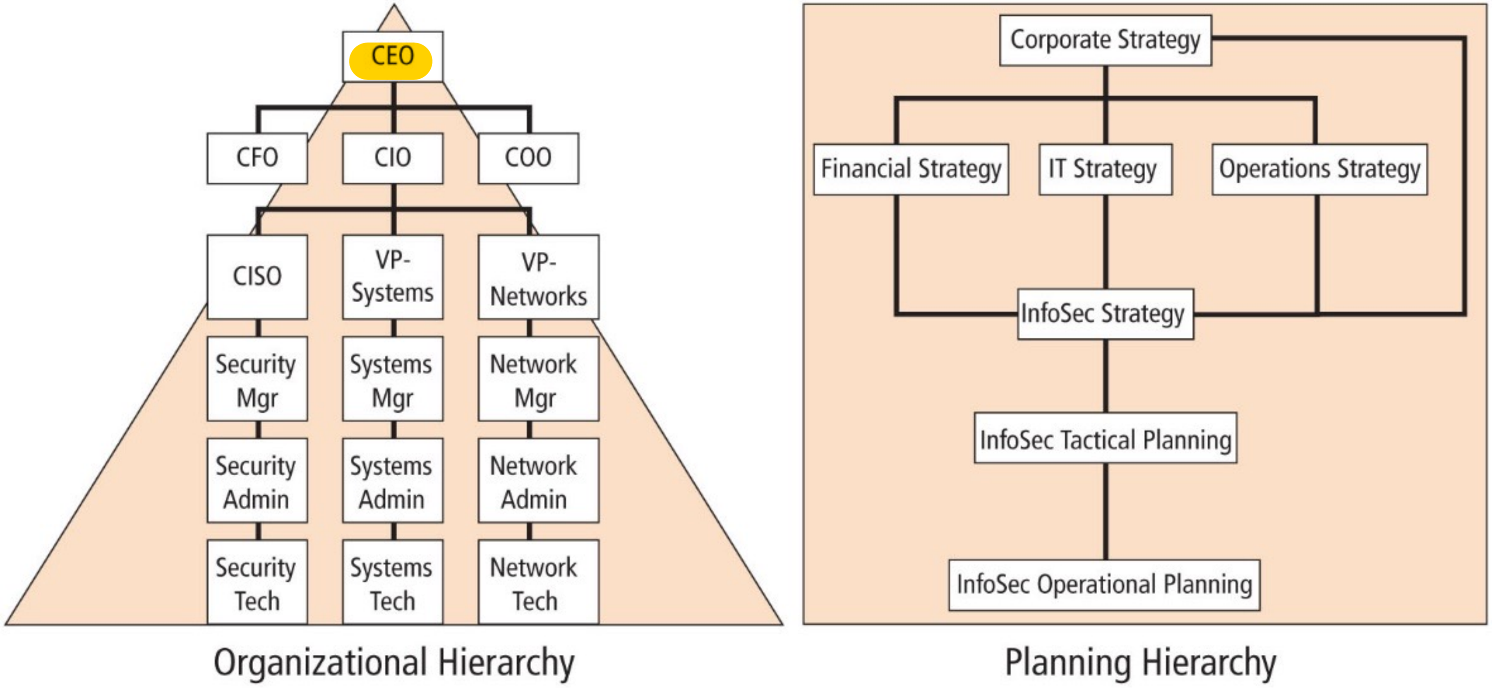
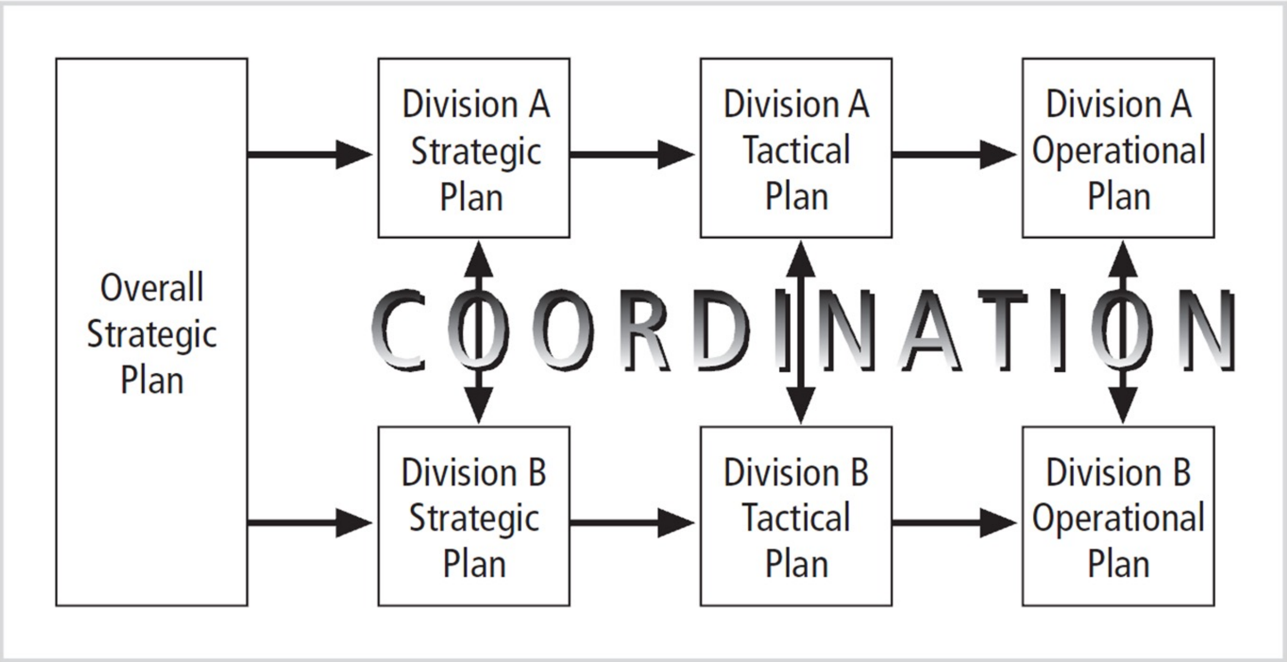


Figure 3-2 **Top-down strategic planning**

Planning Levels

- Strategic planning transforms general statement, sweeping statements towards specific and applied objectives
  - Strategic plans used to create tactical plans, which are in turn used to develop operational plans



Overall Strategic Plan

Division A Strategic Plan

Division A Tactical Plan

Division A Operational Plan

COORDINATION

Division B Strategic Plan

Division B Tactical Plan

Division B Operational Plan

Planning Levels (cont.)

- Tactical plans
  - Have a more short-term focus than strategic planning
    - Usually 1-3 years
  - Each applicable strategic goal is broken down into a serious of incremental objectives
  - Critical components
    - Budgeting
    - Resource allocation
    - Personnel
  - Often include:
    - Project plans, resource acquisition planning documents (e.g., product specifications), project budgets, project reviews, and monthly and annual reports

The CISO and the security managers use the tactical plan to organize, prioritize and acquire resources necessary for the major projects and to provide support for the overall strategic plan.

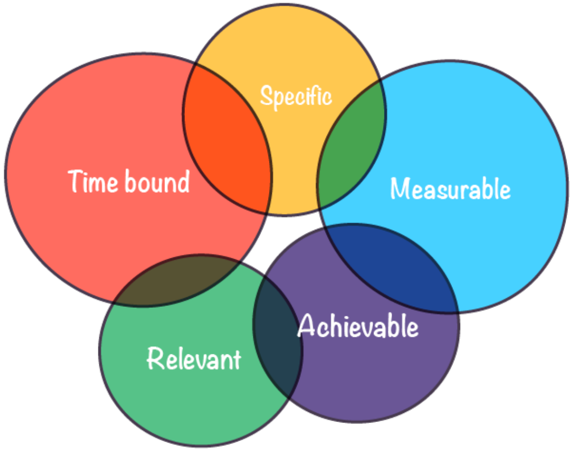
Planning Levels (cont.)

- Operational plans
  - Derived from the tactical plans
  - Used by managers and employees to organize ongoing, day-to-day tasks
  - Often include:
    - Cleary defined coordination activities that span department boundaries
    - Communication requirements
    - Weekly meetings
    - Summaries
    - Progress reports
    - Etc.

Planning Levels (cont.)

- Tasks at the tactical and operational levels must have objectives that are – SMART
  - A well-established tool that you can use to plan and achieve your goals
- **S**pecific
- **M**easurable
- **A**chievable
- **R**elevant
- **T**ime-bound

Evaluate
Revised



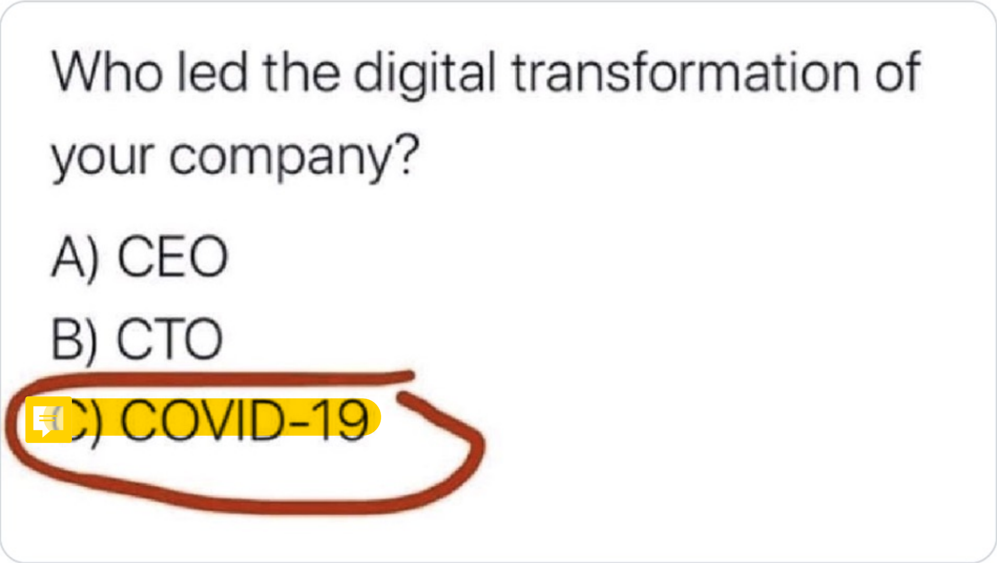
avoid using only 1 single metric to measure

Discussion: Patch Management

- Specific
- Measurable
- Achievable
- Relevant
- Time-bound

the optimal way is for the higher levels to first plan based on the the environment on high level - then adapt based on feedback given on the lower levels

Recent situations:



Who led the digital transformation of your company?

A) CEO

B) CTO

[✓ C) COVID-19]

Digital Transformation Quiz SUSANNE WOLK (TWITTER)

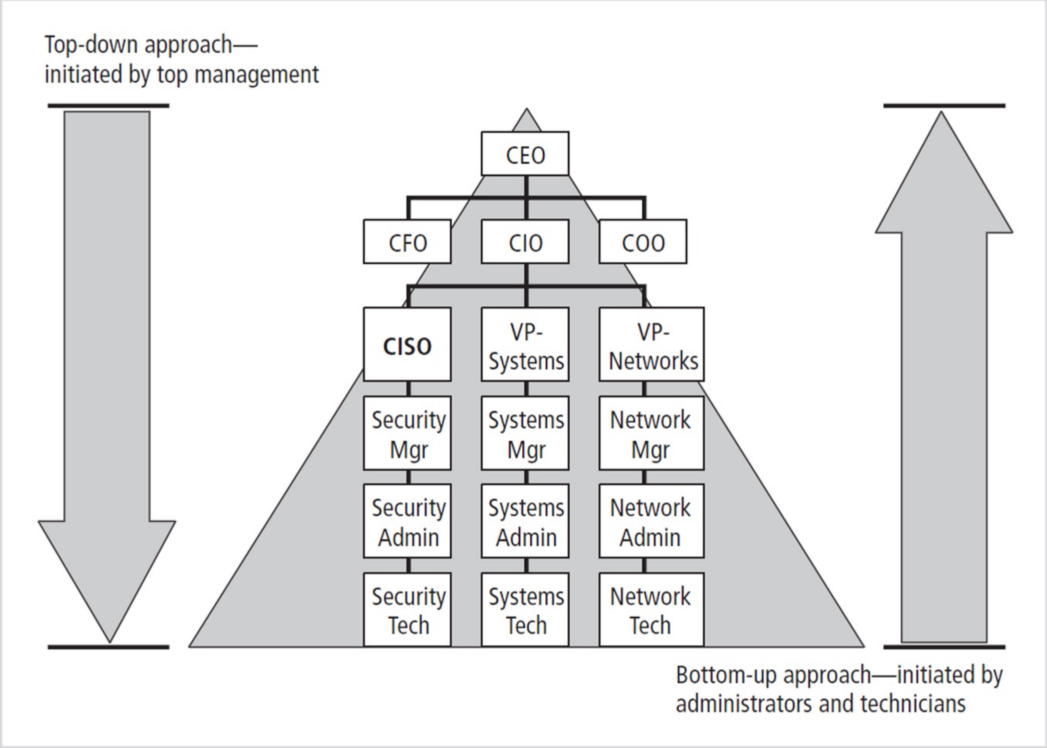
Recent situations discussions

- Strategic planning:
    - Digital transformation in every aspect
- IT planning:
    - High quality information service enabling and supporting digital transformation
- InfoSec planning:
    - Make sure the high quality information service are provided in securely and in conformance with all national information processing, information security, and privacy statutes and guidelines in facilitating digital transformation.

Planning for InfoSec Implementation

Top-down vs. Bottom-up

- InfoSec implementation can be accomplished in two ways:
  - Top-down
    - Initiated by top management
  - Bottom-up
    - Initiated by administrators and technicians



Top-down Approach

- Description
  - Information security begins as a formal program, proposed and coordinated by high-level managers with executive management support to provide resources; give direction; issue policies, procedures, and processes; dictate the goals of expected outcomes of the project; and determine who is accountable for each of the required action
- Advantage:
  - Strong upper-management support
  - Dedicated champion
  - Dedicated funding
  - A clear planning and implementation process
  - Holistic approach to support the entire organization

Top-down Approach

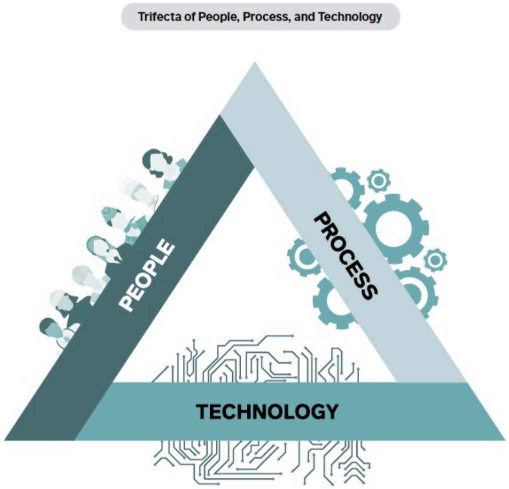
- Challenges
  - High-level management must buy into the effort and provide full support to all departments
  - Must have a **champion**
    - An executive with enough influence to move the project forward
  - Involvement and support of end users is critical

Bottom-up Approach

- Description
  - Information security begins as system and network administrators attempt to improve the security of their system
  - Advantage
    - Utilize the technical expertise of the individual administrators who work with the information systems on a daily basis
  - Disadvantage
    - Lack of coordinated planning from upper management
    - Lack of coordination between departments
    - Lack of the provision of sufficient resources
  - Seldom works in the long term

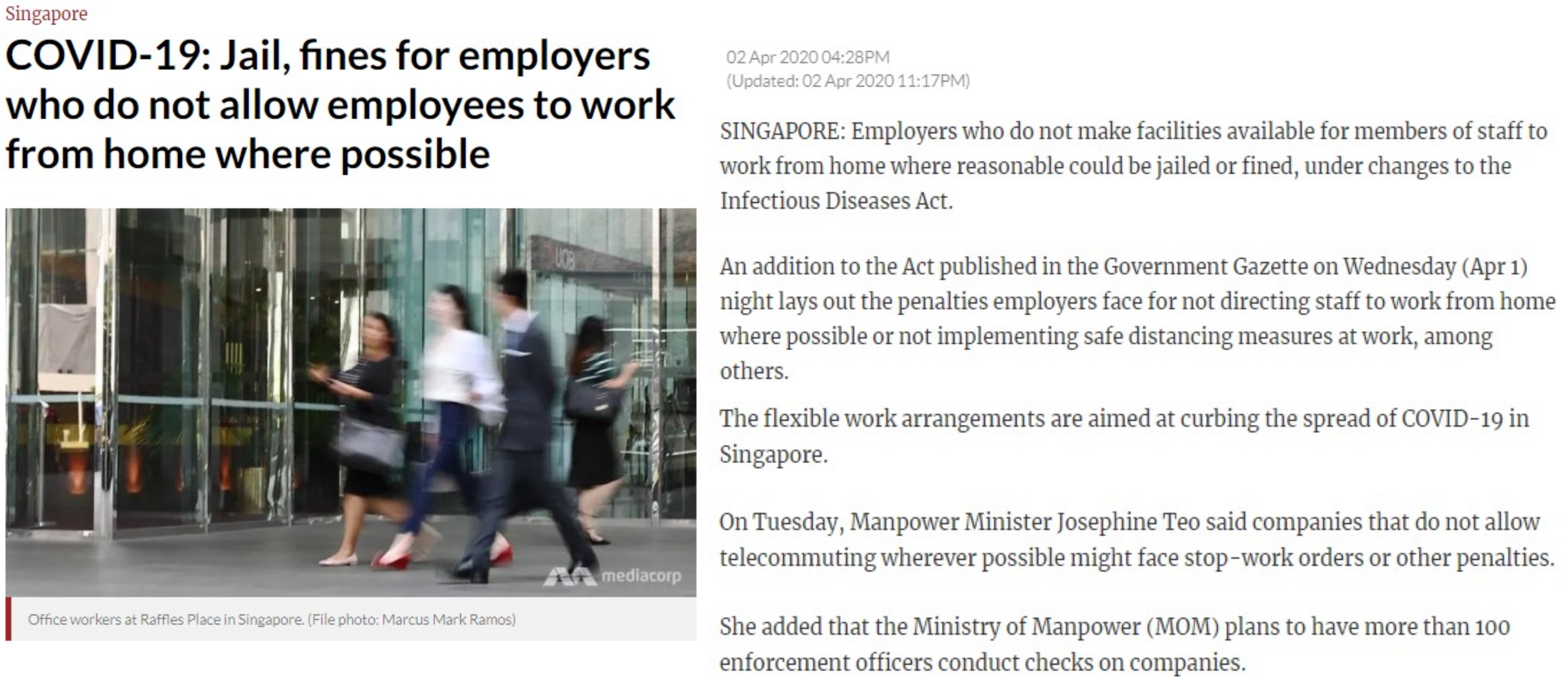
InfoSec Planning

- Includes activities necessary to support the design, creation, and implementation of InfoSec strategies
- Types of InfoSec plans:
  - Policy planning
  - Personnel planning
  - Technology rollout planning
  - Security program planning including education, training and awareness
  - Risk management planning
  - Incident response planning
  - Disaster recovery planning
  - Business continuity planning



Recent situations:

ad hoc approach since it is unexpected



Singapore

COVID-19: Jail, fines for employers who do not allow employees to work from home where possible

Office workers at Raffles Place in Singapore. (File photo: Marcus Mark Ramos)

02 Apr 2020 04:28PM
(Updated: 02 Apr 2020 11:17PM)

SINGAPORE: Employers who do not make facilities available for members of staff to work from home where reasonable could be jailed or fined, under changes to the Infectious Diseases Act.

An addition to the Act published in the Government Gazette on Wednesday (Apr 1) night lays out the penalties employers face for not directing staff to work from home where possible or not implementing safe distancing measures at work, among others.

The flexible work arrangements are aimed at curbing the spread of COVID-19 in Singapore.

On Tuesday, Manpower Minister Josephine Teo said companies that do not allow telecommuting wherever possible might face stop-work orders or other penalties.

She added that the Ministry of Manpower (MOM) plans to have more than 100 enforcement officers conduct checks on companies.

Source: https://www.channelnewsasia.com/news/singapore/covid-19-work-from-home-singapore-jail-fines-coronavirus-12602224

Recent challenges: Remote working

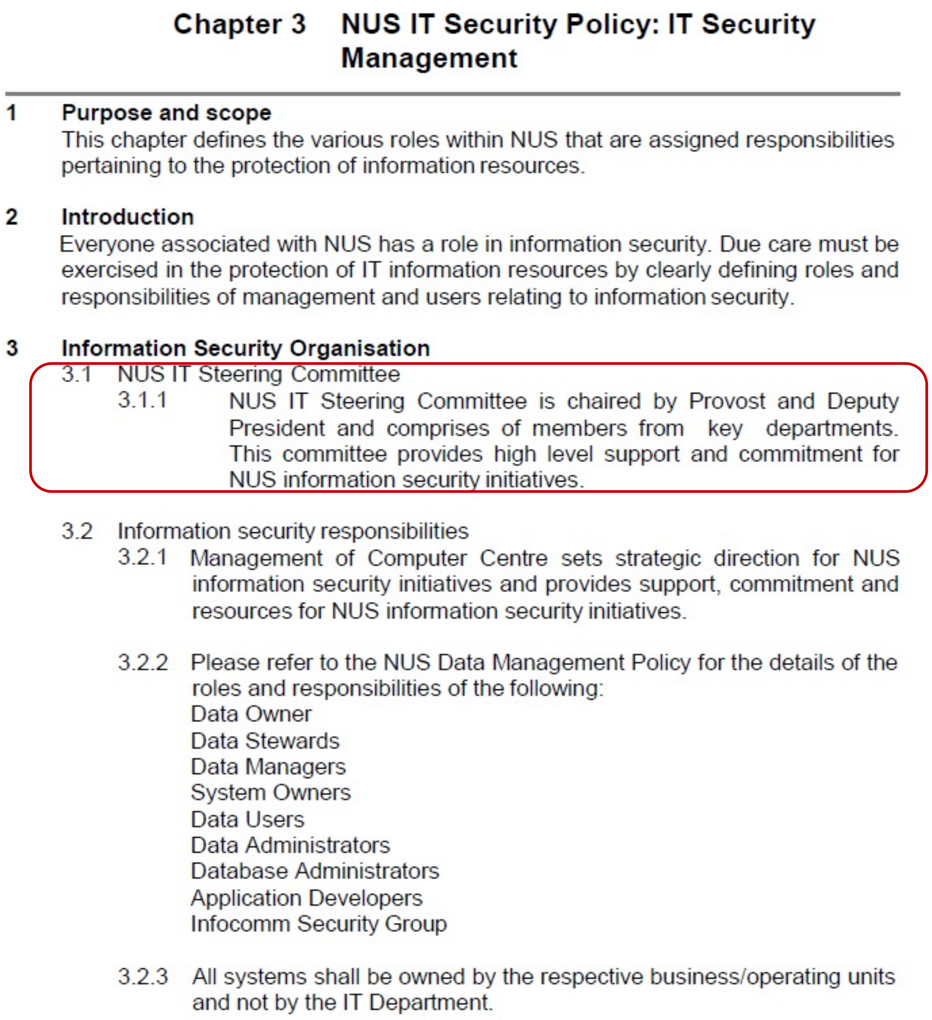
- Strategic planning:
  - Remote working would be the "New Normal"
- IT planning:
  - High quality information service supporting remote working
  - Operational plans:
    - Technology
    - Process
    - People
- InfoSec planning:
  - Make sure remote working are conducted in a secured way.
  - Operational plans
    - Technology
      - □ E.g., VPN, remote access controls, MFA, email security solutions, anti-spam solutions, endpoint protection solutions
    - Process
      - □ E.g., Telecommuting Policy, Acceptable Use Policy, device management, contingency plan
    - People
      - □ E.g., Education and training, A/B team arrangement

Information Security Governance

Information Security Governance

- Governance is
  - "The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly"
- InfoSec governance objectives must be addressed at the highest levels of an organization's management team
  - In order to be effective and offer a sustainable approach
- GRC
  - Governance, Risk Management, and Compliance

Example: NUS InfoSec Governance



Chapter 3 NUS IT Security Policy: IT Security Management

1 Purpose and scope

This chapter defines the various roles within NUS that are assigned responsibilities pertaining to the protection of information resources.

2 Introduction

Everyone associated with NUS has a role in information security. Due care must be exercised in the protection of IT information resources by clearly defining roles and responsibilities of management and users relating to information security.

3 Information Security Organisation

3.1 NUS IT Steering Committee

3.1.1 NUS IT Steering Committee is chaired by Provost and Deputy President and comprises of members from key departments. This committee provides high level support and commitment for NUS information security initiatives.

3.2 Information security responsibilities

3.2.1 Management of Computer Centre sets strategic direction for NUS information security initiatives and provides support, commitment and resources for NUS information security initiatives.

3.2.2 Please refer to the NUS Data Management Policy for the details of the roles and responsibilities of the following:
Data Owner
Data Stewards
Data Managers
System Owners
Data Users
Data Administrators
Database Administrators
Application Developers
Infocomm Security Group

3.2.3 All systems shall be owned by the respective business/operating units and not by the IT Department.

Governance

Information Security Governance (cont.)

- Why need InfoSec governance
  1. Creating and promoting a culture that recognizes the criticality of information and InfoSec to the organization
  2. Verifying that management's investment in InfoSec is properly aligned with organizational strategies and the organization's risk environment
  3. Mandating and assuring that a comprehensive InfoSec program is developed and implemented
  4. Requiring reports from the various layers of management on the InfoSec program's effectiveness and adequacy

InfoSec Governance Responsibilities

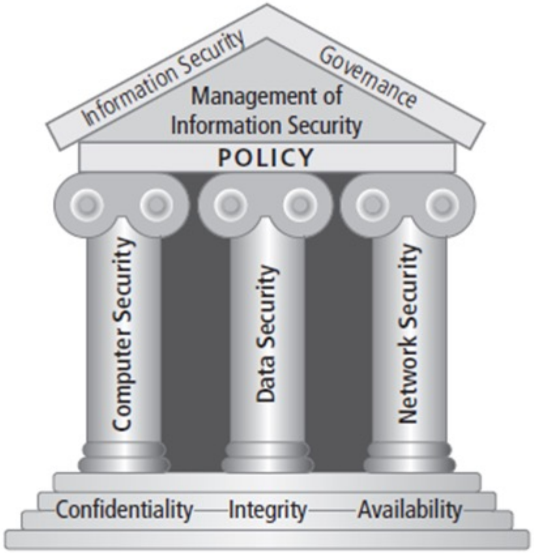
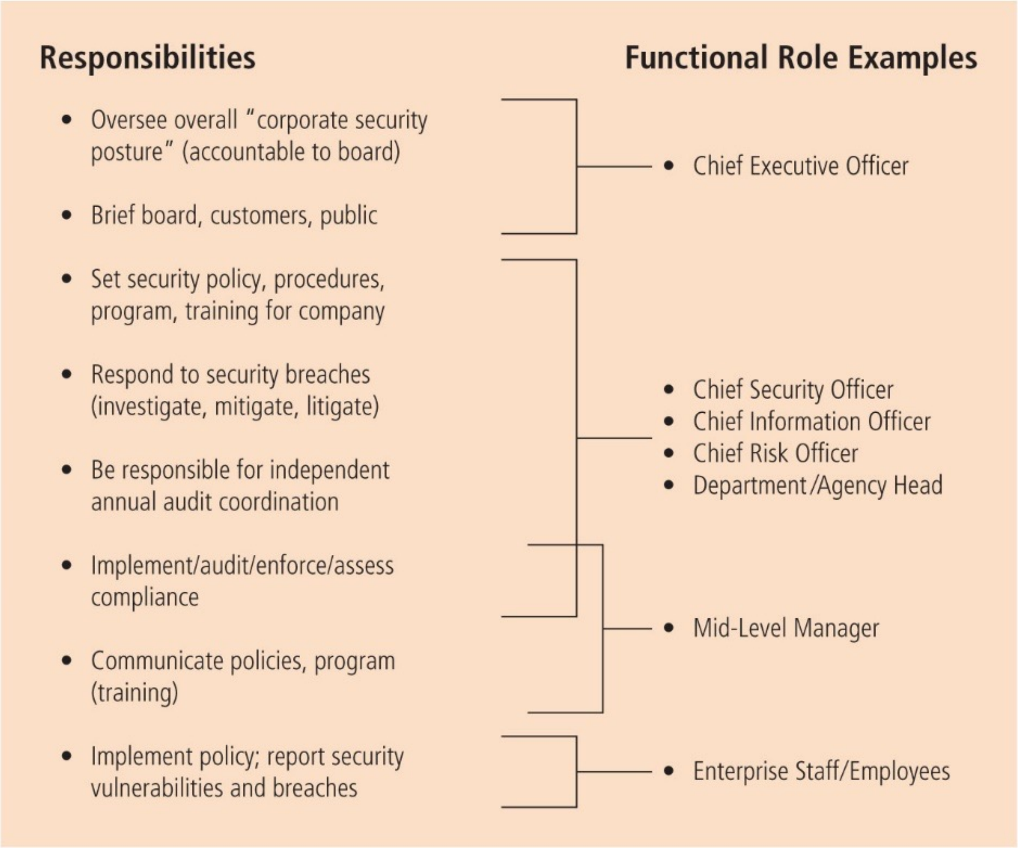


Figure 1-1 **Components of information security**



Responsibilities

- Oversee overall "corporate security posture" (accountable to board)
- Brief board, customers, public
- Set security policy, procedures, program, training for company
- Respond to security breaches (investigate, mitigate, litigate)
- Be responsible for independent annual audit coordination
- Implement/audit/enforce/assess compliance
- Communicate policies, program (training)
- Implement policy; report security vulnerabilities and breaches

Functional Role Examples

- Chief Executive Officer
- Chief Security Officer
- Chief Information Officer
- Chief Risk Officer
- Department /Agency Head
- Mid-Level Manager
- Enterprise Staff/Employees

Figure 3-5 Information security governance responsibilities[10]

Source: IT Governance Institute.

Information Security Governance (cont.)

- Benefits of InfoSec governance:
  - *An increase in share value for organizations*
  - *Increased predictability and reduced uncertainty of business operations by lowering information-security-related risks to definable and acceptable levels*
  - *Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care*
  - *Optimization of the allocation of limited security resources*
  - *Assurance of effective InfoSec policy and policy compliance*
  - *A firm foundation for efficient and effective risk management, process improvement, and rapid incident response*
  - *A level of assurance that critical decisions are not based on faulty information*
  - *Accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response*

this planning will encompass a full/whole cycle

Information Security Governance Program

- When developing an InfoSec governance program, the designers should ensure that the program includes:
  - An effective security *organizational structure*
  - A *comprehensive security strategy* explicitly linked with business and IT objectives
  - An *InfoSec risk management methodology*
  - A security strategy that talks about *the value of information* being protected and delivered
  - *Security policies* that address each aspect of strategy, control, and regulation
  - A complete set of *security standards for each policy* to ensure that procedures and guidelines comply with policy
  - *Institutionalized monitoring processes* to ensure compliance and provide feedback on effectiveness and mitigation of risk
  - A process to *ensure continued evaluation and updating of security policies, standards, procedures, and risks*

ISO/IEC 27014: Governance of Information Security

- ISO 27014:2013 is the ISO 27000 series standard for Governance of Information Security
- The standard specifies six high-level "action-oriented" information security governance principles:

1. Establish organization-wide information security
2. Adopt a risk-based approach
3. Set the direction of investment decisions
4. Ensure conformance with internal and external requirements
5. Foster a security-positive environment
6. Review performance in relation to business outcomes

ISO/IEC 27014: Governance of Information Security

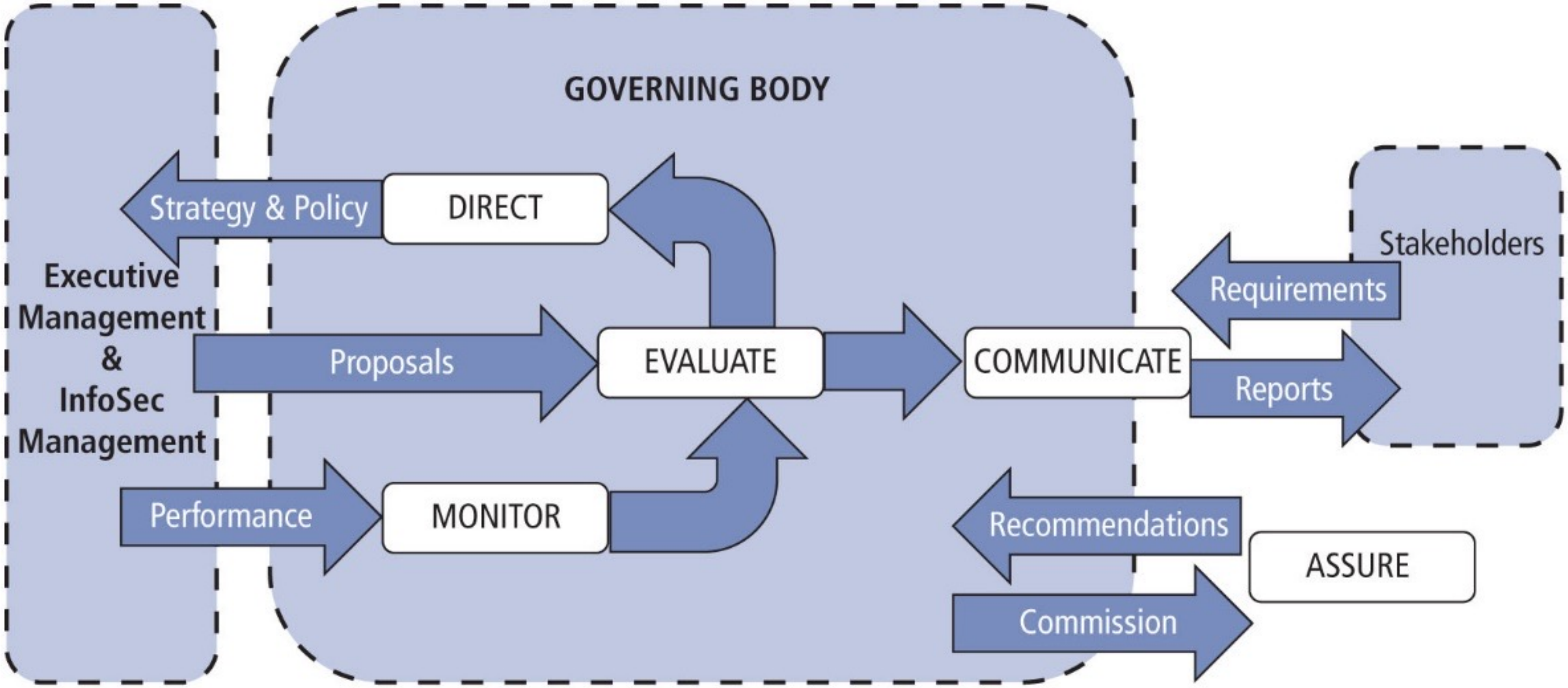


Figure 3-7 ISO/IEC 27014:2013 governance processes[19]

Source: R. Mahncke, Australian eHealth Informatics and Security Conference, December 2013.

Case: SingHealth Data Breach

- Enhancements to Governance and Organisational Structures
  - "At the Ministry, the MOH Chief Information Security Officer (CISO) is currently also the Director of Cyber Security Governance at IHiS. We will separate these roles. The MOH CISO will be supported by a dedicated office in MOH and report to the Permanent Secretary. The MOH CISO office will be the cybersecurity sector lead for the healthcare sector. It will coordinate efforts to protect Critical Information Infrastructure in the healthcare sector, and ensure that the sector fulfils its regulatory obligations under the Cybersecurity Act. For its part, IHiS will have its own separate Director of Cyber Security Governance. "

Source: https://www.moh.gov.sg/news-highlights/details/ministerial-statement-on-the-committee-of-inquiry-into-the-cyber-attack-on-singhealth-s-it-system

difference policy/structure level vs implementation level

Next Week

- Information Security Policy
  - Chapter 4