IS4231
Information Security Management

Lecture 5

Developing the Security Programme

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 5

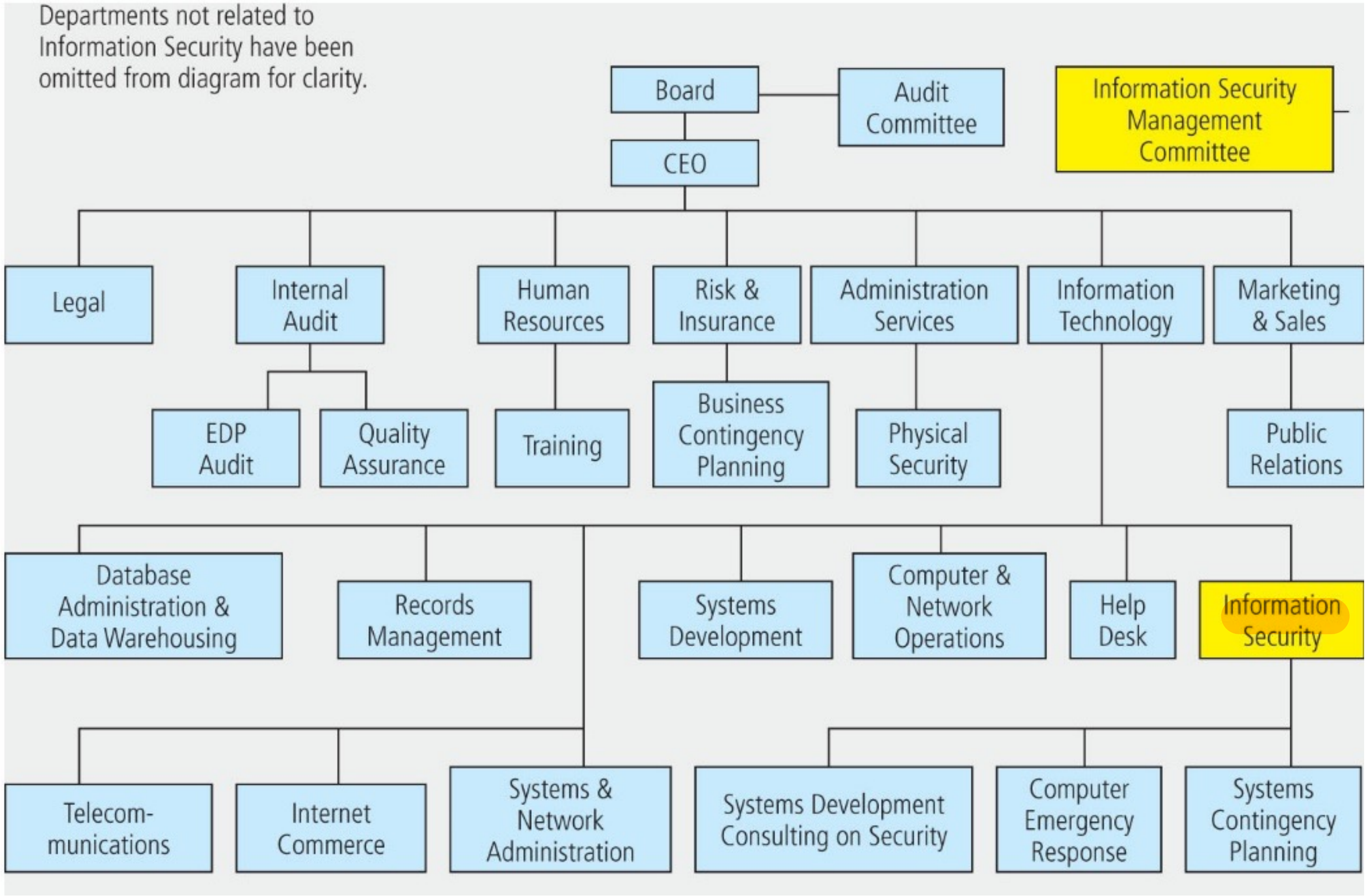
Learning Objectives

- List and describe the functional components of an information security program
  - Placing InfoSec Within an Organization
  - Components of the Security Program
    - Staffing the Security Function

- Components of a security program

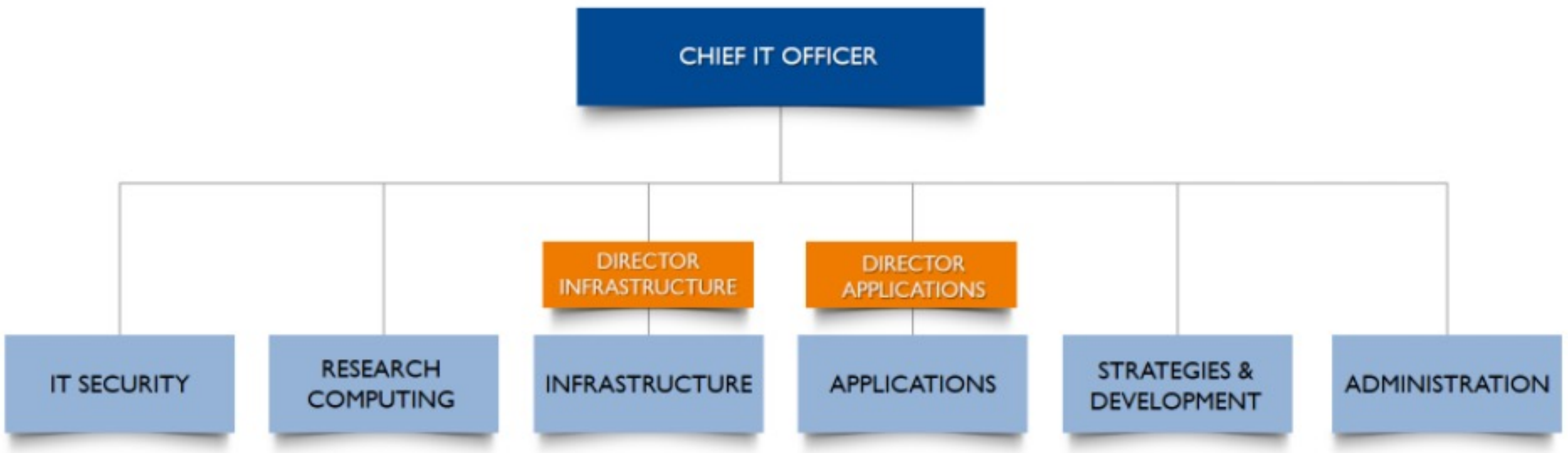
Placing InfoSec Within an Organization

Option 1: InfoSec Reports to IT Dept


Departments not related to Information Security have been omitted from diagram for clarity.
Board
Audit Committee
Information Security Management Committee
CEO
Legal
Internal Audit
Human Resources
Risk & Insurance
Administration Services
Information Technology
Marketing & Sales
EDP Audit
Quality Assurance
Training
Business Contingency Planning
Physical Security
Public Relations
Database Administration & Data Warehousing
Records Management
Systems Development
Computer & Network Operations
Help Desk
Information Security
Telecom-munications
Internet Commerce
Systems & Network Administration
Systems Development Consulting on Security
Computer Emergency Response
Systems Contingency Planning

Example: NUS

NUS IT ORGANISATION CHART



CHIEF IT OFFICER

DIRECTOR INFRASTRUCTURE

DIRECTOR APPLICATIONS

IT SECURITY

RESEARCH COMPUTING

INFRASTRUCTURE

APPLICATIONS

STRATEGIES & DEVELOPMENT

ADMINISTRATION

Source: https://nusit.nus.edu.sg/about/organisation-structure/

Option 1: InfoSec Reports to IT Dept

- Pros:
  - CIO understands IS technical issues, shared common language
  - Only CIO between InfoSec manager and CEO, efficient communication
- Cons:
  - Inherent conflict of interest when confronted with resource allocation decisions or when required to make trade-offs
    - e.g., cost minimization, enhanced user friendliness, rapid time-to-market with a new product or service

CIO VS CISO

Discussion: SingHealth Data Breach

- Organizational Structure in iHiS

"Reflecting on the structure of incident reporting at IHiS, he pointed out that its IT security team is a sub-unit of its infrastructure services, which sits within IHiS' delivery group. Reported security issues could thus be overlooked in favour of service delivery objectives."

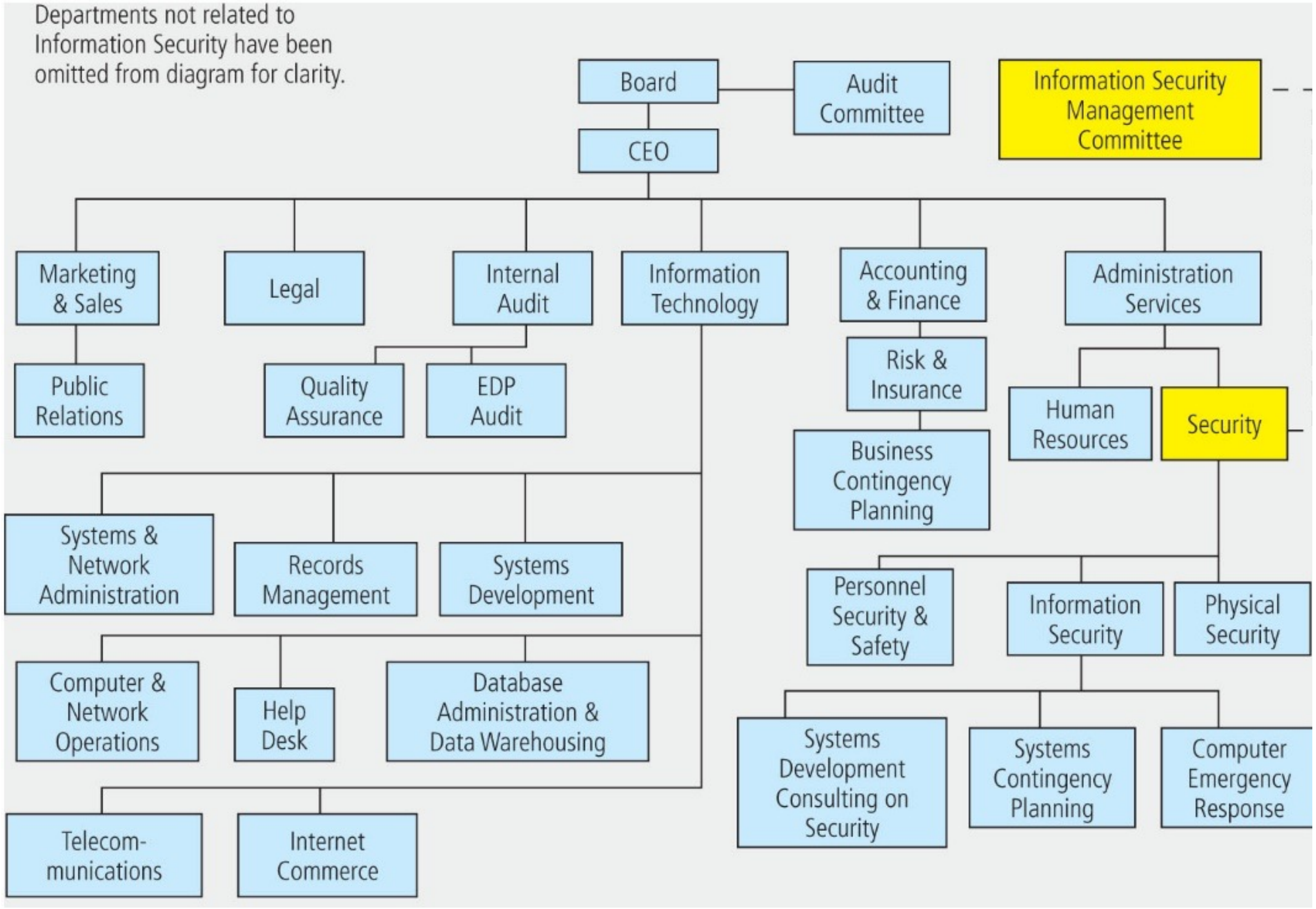
"The structure could mean the security team does not get proper access to appropriate-level managers, which makes it difficult to escalate problems. Key decision-makers might also not be fully aware of security and operational concerns."

Delivery
|
Infrastructure
|
Security

---- Mr David Koh, CSA chief

Source: https://www.straitstimes.com/singapore/senior-leaders-have-key-role-in-cyber-security-commissioner

Option 2: InfoSec Reports to Broadly Defined Security Dept

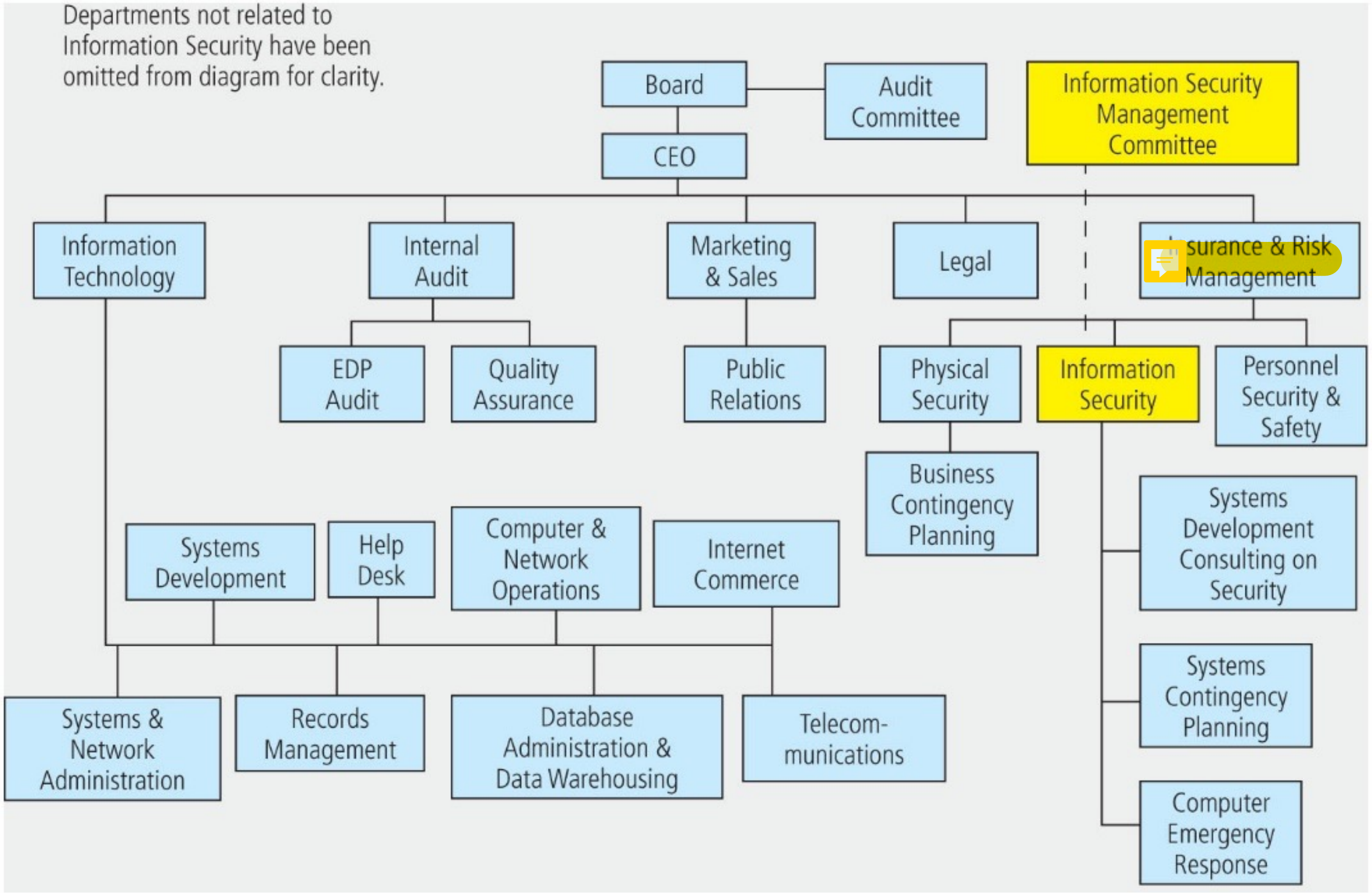

Departments not related to Information Security have been omitted from diagram for clarity.
Board
Audit Committee
Information Security Management Committee
CEO
Marketing & Sales
Legal
Internal Audit
Information Technology
Accounting & Finance
Administration Services
Public Relations
Quality Assurance
EDP Audit
Risk & Insurance
Human Resources
Security
Business Contingency Planning
Systems & Network Administration
Records Management
Systems Development
Personnel Security & Safety
Information Security
Physical Security
Computer & Network Operations
Help Desk
Database Administration & Data Warehousing
Systems Development Consulting on Security
Systems Contingency Planning
Computer Emergency Response
Telecom-munications
Internet Commerce

this method would push ITSec to a more supportive role

Option 2: InfoSec Reports to Security Dept

- Pros:
  - It facilitates communication with others who have both a security perspective and related security responsibilities.
- Cons:
  - InfoSec staff might be uncomfortable, see themselves as high-tech workers.
  - The budget for physical security has not increased much over the years, the top management may underestimate the resources InfoSec function will need.
  - Security manager often lack an appreciation of information system technology, poor communicator with top management

Option 3: InfoSec Reports to Insurance & Risk Management Dept



Departments not related to Information Security have been omitted from diagram for clarity.

Board
Audit Committee
Information Security Management Committee
CEO
Information Technology
Internal Audit
Marketing & Sales
Legal
Insurance & Risk Management
EDP Audit
Quality Assurance
Public Relations
Physical Security
Information Security
Personnel Security & Safety
Business Contingency Planning
Systems Development Consulting on Security
Systems Development
Help Desk
Computer & Network Operations
Internet Commerce
Systems Contingency Planning
Systems & Network Administration
Records Management
Database Administration & Data Warehousing
Telecom-munications
Computer Emergency Response

Option 3: Infosec Reports to Insurance & Risk Management Dept

- Pros:
  - It fosters an integrated risk management perspective
    - A centralized perspective prioritizes and compares all risks across the organization
- Cons:
  - Chief risk managers not familiar with IT technology, lack shared language
  - Its focus is quite strategic, the operational and administrative aspects of information security may not get enough attention and support
- Adopted for information intensive organizations
  - E.g., banks, stock brokerages

Example: OCBC Org Chart

Mr Vincent Choo

Group Risk Management

Mr Vincent Choo was appointed Head of Group Risk Management on 1 August 2014.

As Chief Risk Officer, he covers the full spectrum of risk, including Credit, Technology and Information Security, Liquidity, Market and Operational Risk Management. He reports jointly to both Group CEO and the Board Risk Management Committee of OCBC Bank. Mr Choo joined OCBC Bank from Deutsche Bank AG where his last appointment was Managing Director and Chief Risk Officer for Asia Pacific. In his 20 years at Deutsche Bank AG, he served in a number of senior roles including Head of Market Risk Management for Asia Pacific, with additional responsibilities for Traded Credit Products, and Head of New Product Approval for Asia. He holds a Master of Arts in Economics from University of Akron.

Mr Praveen Raina

Group Operations and Technology

Mr Praveen Raina was appointed Head of Group Operations and Technology in June 2021.

Mr Raina joined OCBC Bank in August 2008 and has held various senior positions in Group Operations and Technology. He was responsible for the bank's innovation efforts in technology development to deliver positive customer experience and capabilities across its touchpoints.

aim is to develop IT solutions

Source: https://www.ocbc.com/group/who-we-are/leaders-management-team.html

Other approaches:

- Current movement: separate information security from the IT division
  - CISO report to CEO directly
  - E.g.,
    - Standard Chartered Korea
      - □ https://www.standardchartered.co.kr/np/en/cms/cm/bi/EnOrganizationchart.jsp?menuId=HE0501050000000&rnb=4
- Combined roles
  - E.g.,
    - Rakuten Global Structure
      - □ https://global.rakuten.com/corp/about/organization.html

Staffing the Security Function

Staffing the Security Function

- A typical organization has a number of individuals with information security responsibilities
- While the titles used may be different, most of the job functions fit into one of the following:
  - Chief information security officer (CISO)
  - Security managers
  - Security administrators and analysts
  - Security technicians
  - Security staffers and watchstanders
  - Security consultants
  - Security officers and investigators
  - Help desk personnel

Information Security Positions

- InfoSec Roles

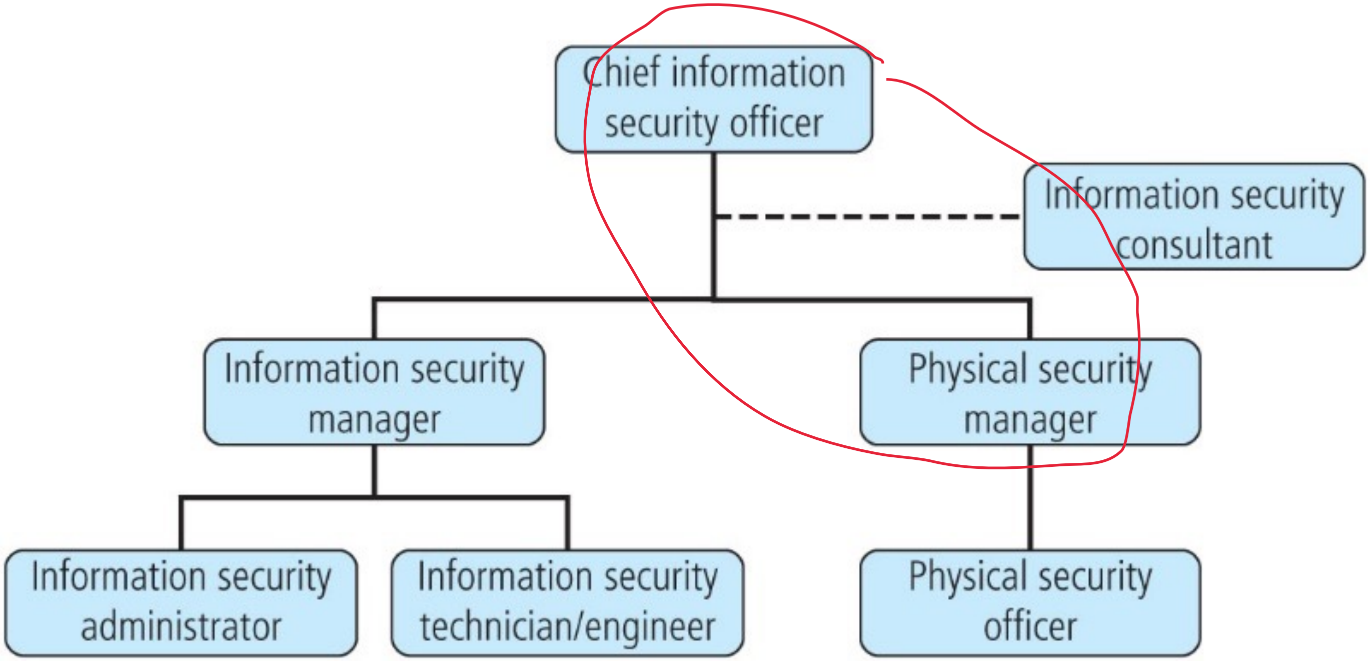

Chief information security officer
Information security consultant
Information security manager
Physical security manager
Information security administrator
Information security technician/engineer
Physical security officer

Figure 5-10 **InfoSec roles**

Information Security Positions

- The CISO, or in some cases, the CSO
  - is usually the top InfoSec officer in the organization and is the spokesperson for the security team and responsible for the overall InfoSec program
- Security Managers
  - accountable for the day-to-day operations of the InfoSec program
- Security Administrators and Analysts
  - The security administrator is a hybrid of a security technician and a security manager, with both technical knowledge and managerial skill

Information Security Positions

- Security Technician
  - A technically qualified individual who may configure firewalls and IDPSs, implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure that security technical controls are properly implemented
- Security Staffers and Watchstanders
  - Who perform routine watchstanding or administrative activities
- Security Consultants
  - An independent expert in some aspect of InfoSec
  - Usually brought in when the organization makes the decision to outsource one or more aspects of its security program
  - While it is usually preferable to involve a formal managed security services (MSS) company, qualified individual consultants are available for hire to organizations that do not choose to hire an MSS company

Information Security Positions

- Security Officers and Investigators
  - Occasionally, the physical security and InfoSec programs are blended into a single, converged functional unit
  - When that occurs, several roles are added to the pure IT security program, including physical security officers and investigators
- Help desk
  - Which enhances the security team's ability to identify potential problems

Some Staffing Model and Ratio…

- For every 500 to 750 IT users, you need one security operations full-time equivalent (FTE).
- For every 1,500 to 2,000 IT users, you need one security architecture FTE.
- For organizations with more than 4,000 IT users, you need to have a named security manager.
- For every 5,000 IT users, you need an IT risk FTE (this number varies significantly if you use a tool or are heavily regulated).
- Organizations with more than 7,500 IT users should have a dedicated security team with formal direct-line and dotted-line relationships.

currently NUS has 50000 IT users (but ITSec has around 12)

Components of A Security Program

Information Security Program

- The structure and organization of the efforts to manage risks to an organization’s information assets.
  - Variables determining how a given organization chooses to structure its InfoSec program:
    - Organizational culture
    - Size
    - Security budget
    - etc

Elements of InfoSec Program

- NIST model

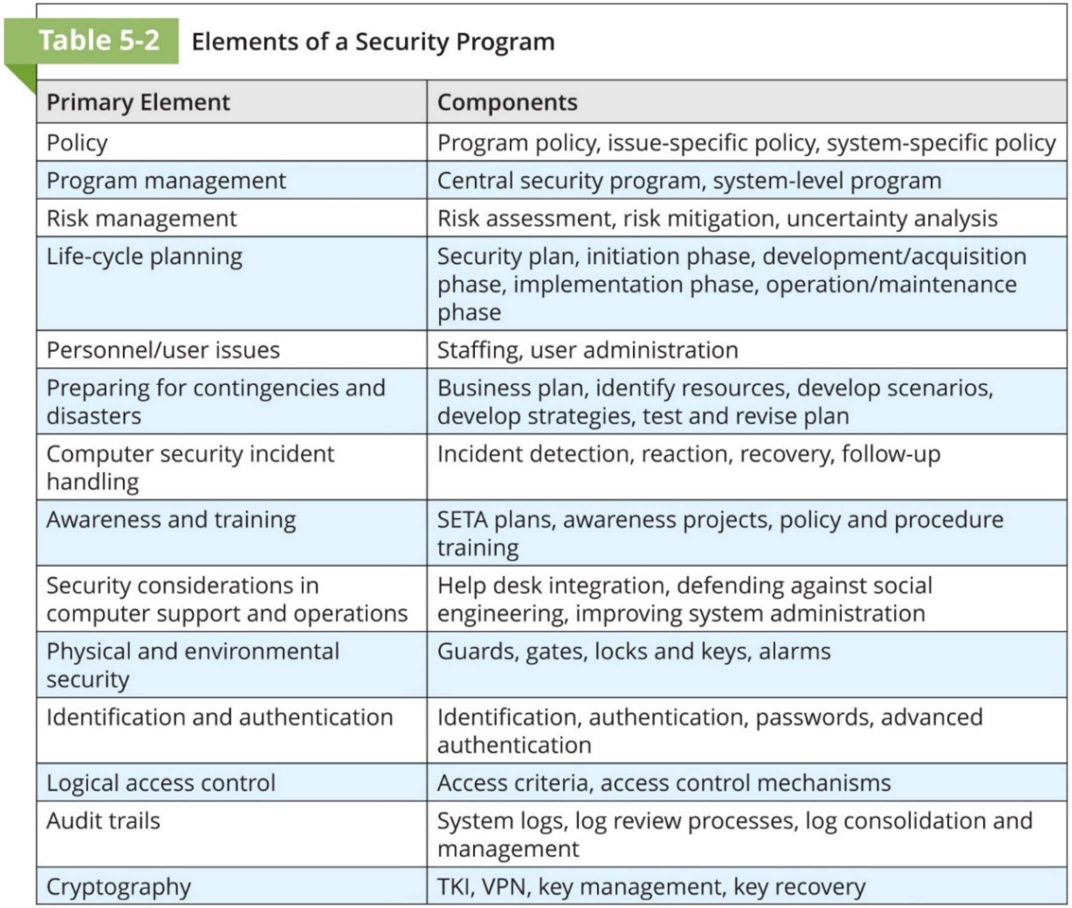


Table 5-2 Elements of a Security Program

Primary Element	Components
Policy	Program policy, issue-specific policy, system-specific policy
Program management	Central security program, system-level program
Risk management	Risk assessment, risk mitigation, uncertainty analysis
Life-cycle planning	Security plan, initiation phase, development/acquisition phase, implementation phase, operation/maintenance phase
Personnel/user issues	Staffing, user administration
Preparing for contingencies and disasters	Business plan, identify resources, develop scenarios, develop strategies, test and revise plan
Computer security incident handling	Incident detection, reaction, recovery, follow-up
Awareness and training	SETA plans, awareness projects, policy and procedure training
Security considerations in computer support and operations	Help desk integration, defending against social engineering, improving system administration
Physical and environmental security	Guards, gates, locks and keys, alarms
Identification and authentication	Identification, authentication, passwords, advanced authentication
Logical access control	Access criteria, access control mechanisms
Audit trails	System logs, log review processes, log consolidation and management
Cryptography	TKI, VPN, key management, key recovery

Source: NIST.

Elements of InfoSec Program

- ISO/IEC 27002: 2013 ISMS guideline
  - 0. Introduction
  - 1. Scope
  - 2. Normative references
  - 3. Terms and definitions
  - 4. Structure of this standard
  - 5. Information security policies
  - 6. Organization of information security
  - 7. Human resource security
  - 8. Asset management
  - 9. Access Control
  - 10. Cryptography
  - 11. Physical and environmental security
  - 12. Operations security
  - 13. Communication security
  - 14. System acquisition, development, and maintenance
  - 15. Supplier relationships
  - 16. Information security incident management
  - 17. Information security aspects of business continuity management
  - 18. Compliance

Elements of InfoSec Program

- ISO 27K ISMS Guideline

1. Information security policies

    - Management direction for information security
        - □ Review the organization's policies for information risk, security and related areas (e.g., governance, risk management, privacy, business continuity, compliance, HR, physical site security, change management, logging, classification, assets management, system development and acquisition…)
        - □ E.g., is there clear evidence of a sensibly designed and managed overall framework/structure/hierarchy?
        - □ E.g., Are the policies reasonably comprehensive, covering all relevant information risks and control areas?
        - □ E.g., How are the policies authorized, communicated, understood, and accepted?
        - □ Etc.

Elements of InfoSec Program

- ISO 27K ISMS Guideline

  2. Organizations of information security

     - Internal organization
       - Information security roles and responsibilities
         - E.g., Is information risk and security given sufficient emphasis and management support?
         - E.g., Is there a senior management involved governance on InfoSec related issues?
         - E.g., Are roles and responsibilities clearly defined and assigned to suitable skilled individuals?
         - E.g., Are the information flow operating effectively in practice?
         - E.g., Is there adequate awareness of and support for the information risk and security structure and governance arrangement?

Elements of InfoSec Program

- ISO 27K ISMS Guideline

3. Human resources security

  - Prior to employment
    - □ Screening
    - □ Terms and Conditions of employment
  - During employment
    - □ Information security awareness, education and training
  - Termination and change of employment

Elements of InfoSec Program

- ISO 27K ISMS Guideline
  4. Asset management
     - Assets inventory
       - □ Inventory List
         - □ E.g., digital data, hardcopy information, software, infrastructure, information service and service provider, physical security and safety, business relationship, people
       - □ Ownership list
     - Information classification
       - □ Classification of information
       - □ Labelling of information
     - Media handling
       - □ Management of removable data
       - □ Disposal of media
       - □ Physical media transfer

Risk based approach - label via criticality of data

Elements of InfoSec Program

- ISO 27K ISMS Guideline

5. Access control

- Business requirements of access control
  - Access control policy
- User access management
  - User registration and de-registration
  - User access provisioning
  - Management of privileged access rights
  - Management of secret authentication information of users
  - Review of user access rights
  - Removal or adjustment of access rights
- User responsibilities
- System and application access control
  - Secure log-on procedures
  - Password management system
  - User of privileged utility programs
  - Access control to program source code

Elements of InfoSec Program

- ISO 27K ISMS Guideline

6. Cryptography
   - Cryptographic controls
     - □ Principles
     - □ Standards
     - □ A risk-based process
   - Key management
     - □ Equipment protection
     - □ Rules
     - □ Back up
     - □ Logging and auditing

Elements of InfoSec Program

- ISO 27K ISMS Guideline

  7. Physical and environment security

  - Secure areas
    - Physical security perimeter
    - Physical entry controls
    - Securing offices, rooms, and facilities
    - Protecting against external and external threats
    - Working in secure areas
    - Delivery and loading areas
  - Equipment
    - Equipment siting and protection
    - Supporting utilities
    - Cabling security
    - Equipment maintenance
    - Removal of assets
    - Security of equipment and assets off-premises
    - Secure disposal or re-use of equipment
    - Unattended user equipment
    - Clear desk and clear screen policy

Elements of InfoSec Program

- ISO 27K ISMS Guideline

8. Operational security
   - □ Operational procedures and responsibilities
     - □ Documented operating procedures
     - □ Change management
     - □ Capacity management
     - □ Separation of development, testing and operational environment
   - □ Protection from malware
   - □ Backup
   - □ Logging and monitoring
   - □ Control of operational software
   - □ Technical vulnerability management
     - □ E.g., Are patches assessed for applicability and risks before being implemented?
     - □ E.g., Are the process for implementing urgent patches sufficiently slick and comprehensive?
     - □ E.g., To what extent does the organization depend on automated patch management, in effect accepting the associated risks of implementing rogue patches?
   - □ Audit considerations

Elements of InfoSec Program

- ISO 27K ISMS Guideline

9. Communication security
   - Network security management
     - Network controls
     - Security of network services
     - Segregation in network services
   - Information transfer
     - Information transfer policies and procedures
     - Agreements on information transfer
     - Electronic messaging
     - Confidentiality or non-disclosure agreements

Elements of InfoSec Program

- ISO 27K ISMS Guideline

  10. System acquisition, development and maintenance
      - □ Security requirements of information systems
      - □ Security in development and support processes
        - □ Secure development policy
        - □ System change control procedures
        - □ Technical review of applications after operating platform changes
        - □ Restrictions on changes to software packages
        - □ Secure system engineering principles
          - E.g., DevSecOps
        - □ Secure development environments
        - □ Outsourced development
        - □ System security testing
        - □ System acceptance testing
      - □ Test data

Elements of InfoSec Program

- ISO 27K ISMS Guideline

11. Supplier relationships

    - Information security in supplier relationships
        - □ Information security policy for supplier relationships
        - □ Addressing security within supplier agreement
    - Supplier service delivery management
        - □ Monitoring and review supplier services
        - □ Managing changes to supplier services

Elements of InfoSec Program

- ISO 27K ISMS Guideline

12. Information security incident management
    - □ Responsibilities and procedures

13. Business continuity management
    - □ Business continuity
    - □ Redundancies

14. Compliance
    - □ Compliance with legal and contractual requirements
    - □ Information security review
        - □ Independent review of information security
        - □ Compliance with security policies and standards
        - □ Technical compliance review

Next Week

- Security Management Practices
  - Chapter 9