Network Security Administration and Management

BITS 3353

Lecture 3: Security Management

Lesson Outline
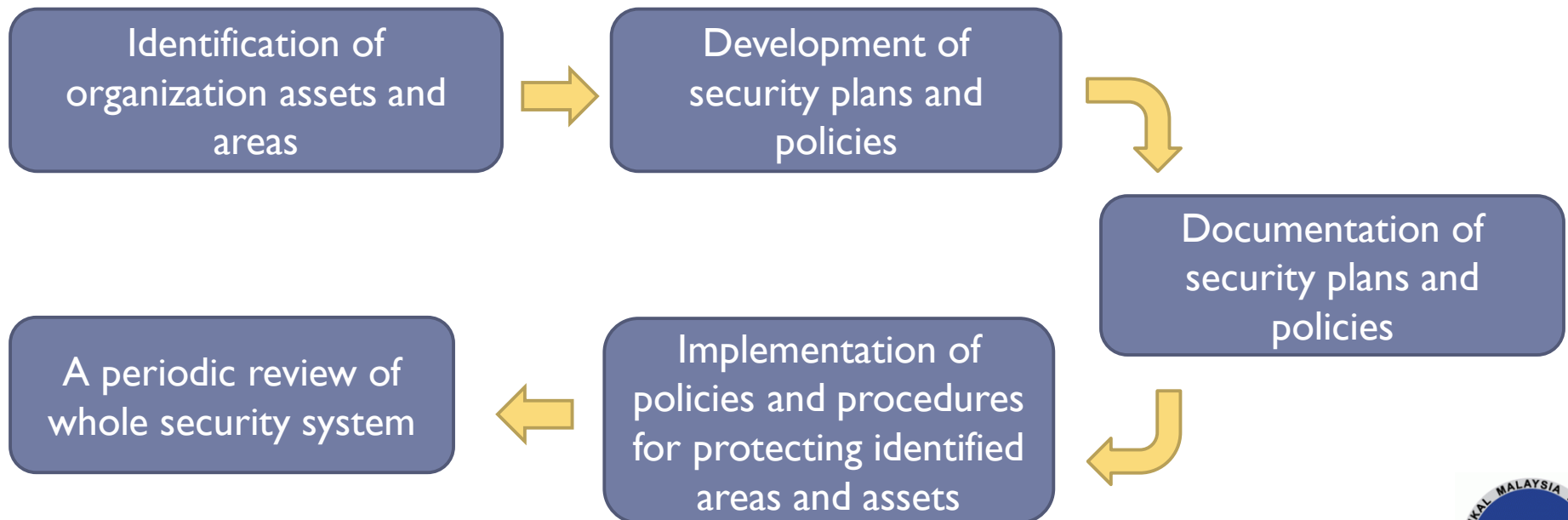
- Security Management
- Security plan
- Security Analysis
- Change Management
- Disaster recovery
- Security management Systems
- Protecting storage media
- Protection of system documentation
- Exchanges of information and software
- Security requirements of a system
- Security standards
- Security best practices

Security Management

- Security management focuses on the safety of assets (resources) in the organization, both physical safety and digital security.

- Security management is a systematic, repetitive set of interconnected activities to ensure safe operation and thus reduce the likelihood of risks.

- Security management is closely related to risk management and it is aimed at creating through various methods, procedures, guidelines and standards a permanent secure solution to such conditions, which will help prevent or reduce identified risks in particular.
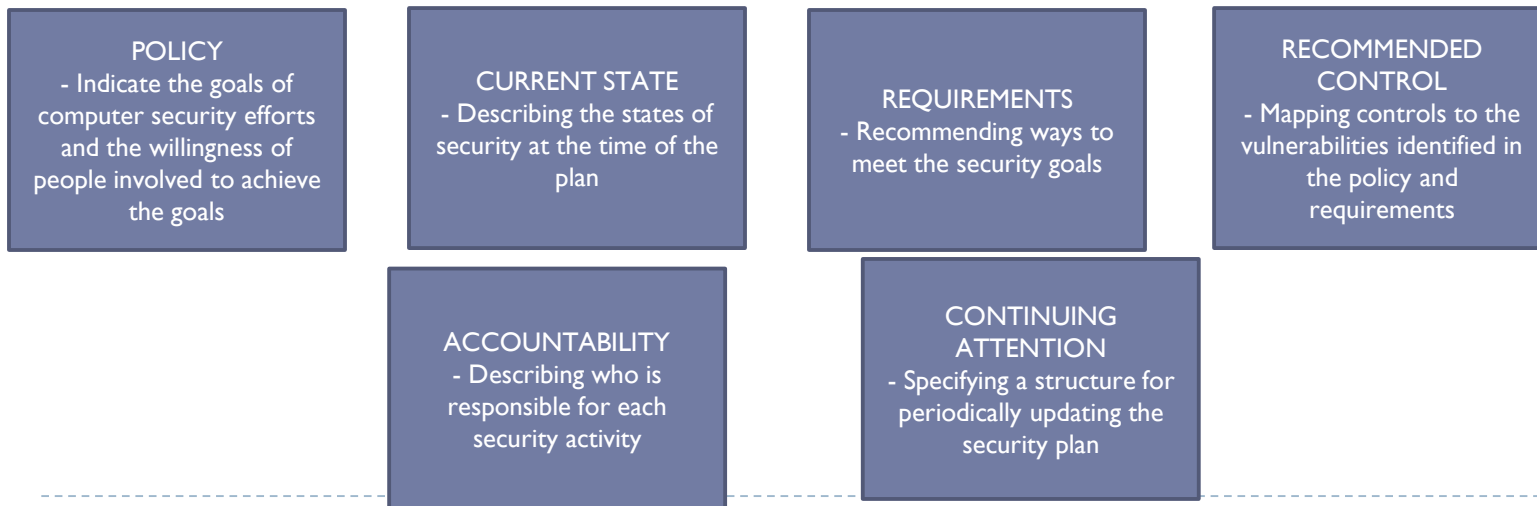
Security Management

- Security management is abroad field that encompass everything from identification of assets, persons and belongings, implement control mechanism for protection and revision of security system.

Identification of organization assets and areas	Development of security plans and policies	Documentation of security plans and policies
A periodic review of whole security system	Implementation of policies and procedures for protecting identified areas and assets	

Security Plan

- Security plan identifies and organizes the security activities for a computing system

- The plan is the description of current situation and plan for improvement

- Issues address in security plan:

POLICY
- Indicate the goals of computer security efforts and the willingness of people involved to achieve the goals

CURRENT STATE
- Describing the states of security at the time of the plan

REQUIREMENTS
- Recommending ways to meet the security goals

RECOMMENDED CONTROL
- Mapping controls to the vulnerabilities identified in the policy and requirements

ACCOUNTABILITY
- Describing who is responsible for each security activity

CONTINUING ATTENTION
- Specifying a structure for periodically updating the security plan

Security Analysis

PLAN
is written

→

Acceptance by the organizations

- Commitment to the plan

(security function will be implemented and security activities carried out)

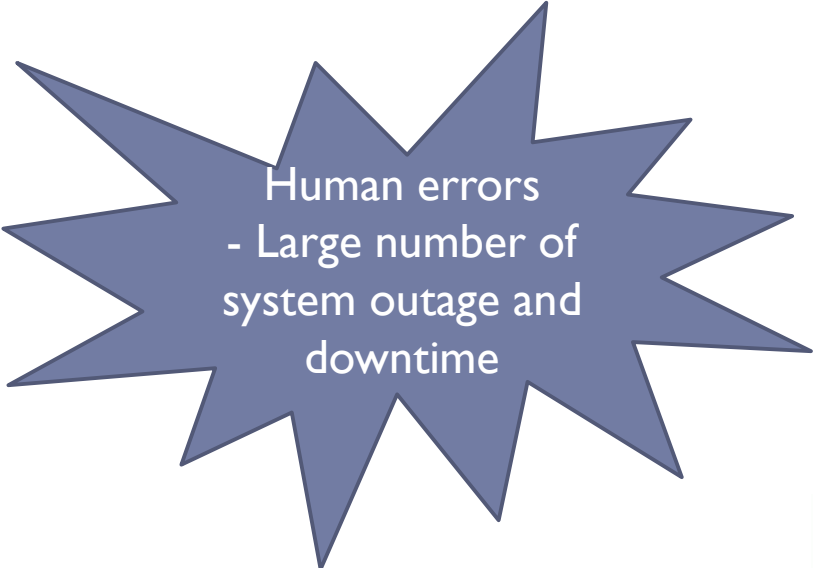TEAM involved to make the plan SUCCESS:

1) Planning team – must be sensitive to the need of each group affected by the plan

2) Affected Group – those affected by the security recommendation must understand what the plan means, way to use the system and perform their business activities

3) Management team – must be committed to using and enforcing the security aspect of the system

Change Management

- Process of modifying equipment, systems, software or procedures in a planned and authorized manner
- The methodology defines steps that ensure the system changes are required by the organization, and are properly authorized, documented, tested and approved by management.
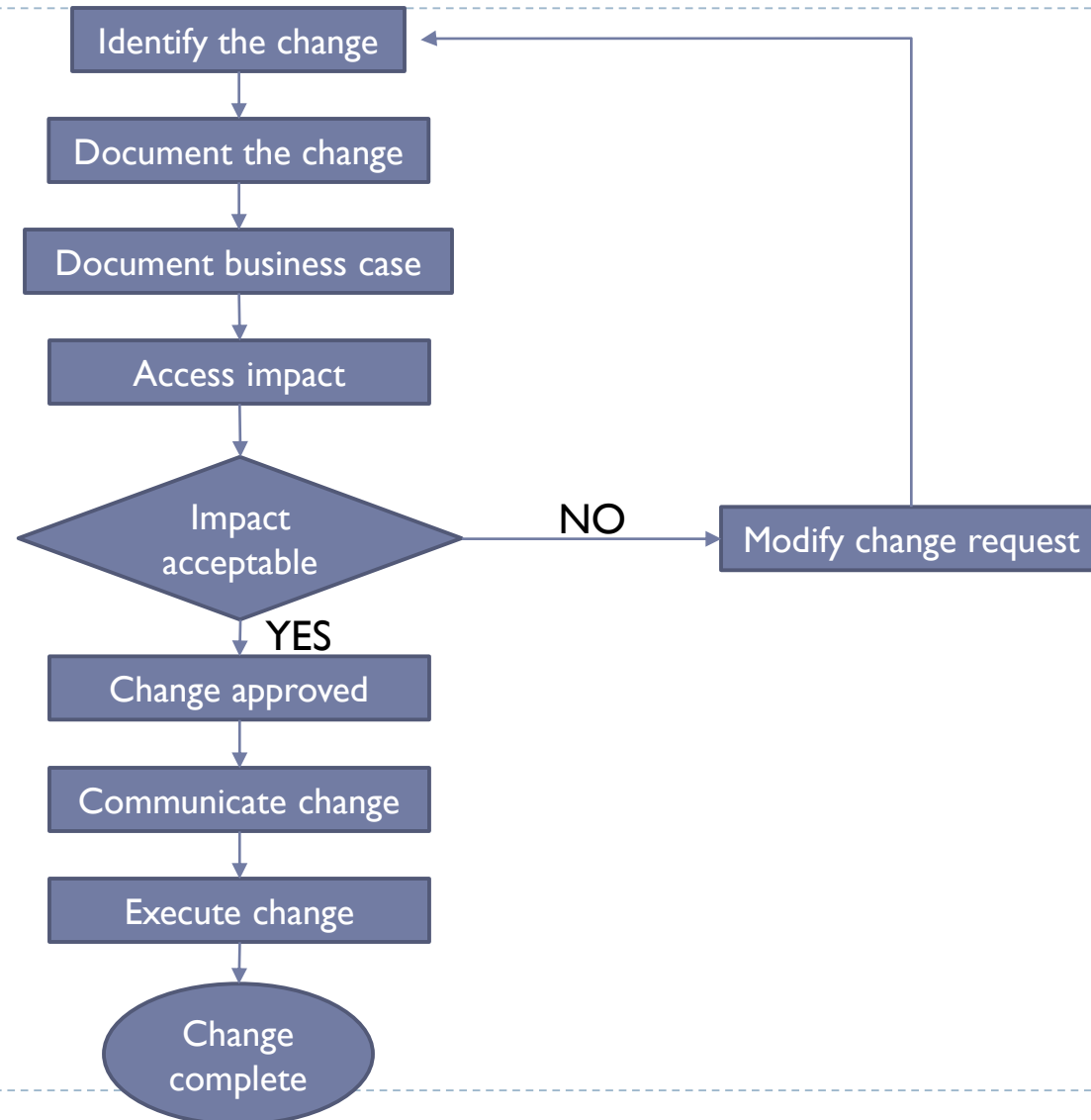- WHAT HAPPEN IF CHANGE MANAGEMENT NOT PROPERLY HANDLE?

Chaotic organization

Human errors
- Large number of system outage and downtime

Change Management Process

Disaster Recovery

- Many types of DISASTER, whether naturally or caused by people, can disrupt an organization's operation for lengthy period.
- Preparation to LESSEN the impact of the disaster → DISASTER RECOVERY PLAN (DRP)
- DRP defines the data and resources necessary and the steps to take in order to restore critical organizational process.
- Begin DRP by answering the following questions for all critical functions:

1. Who is responsible for the operation of this function?
2. What do these individuals need to perform the functions?
3. When should this function be accomplished in relation to other functions?
4. Where will this function be performed?
5. How is this function performed (What is the process)?
6. Why is this function so important or critical to the organization?

Disaster Recovery

Business Impact Assessment (BIA) or Business Impact Analysis
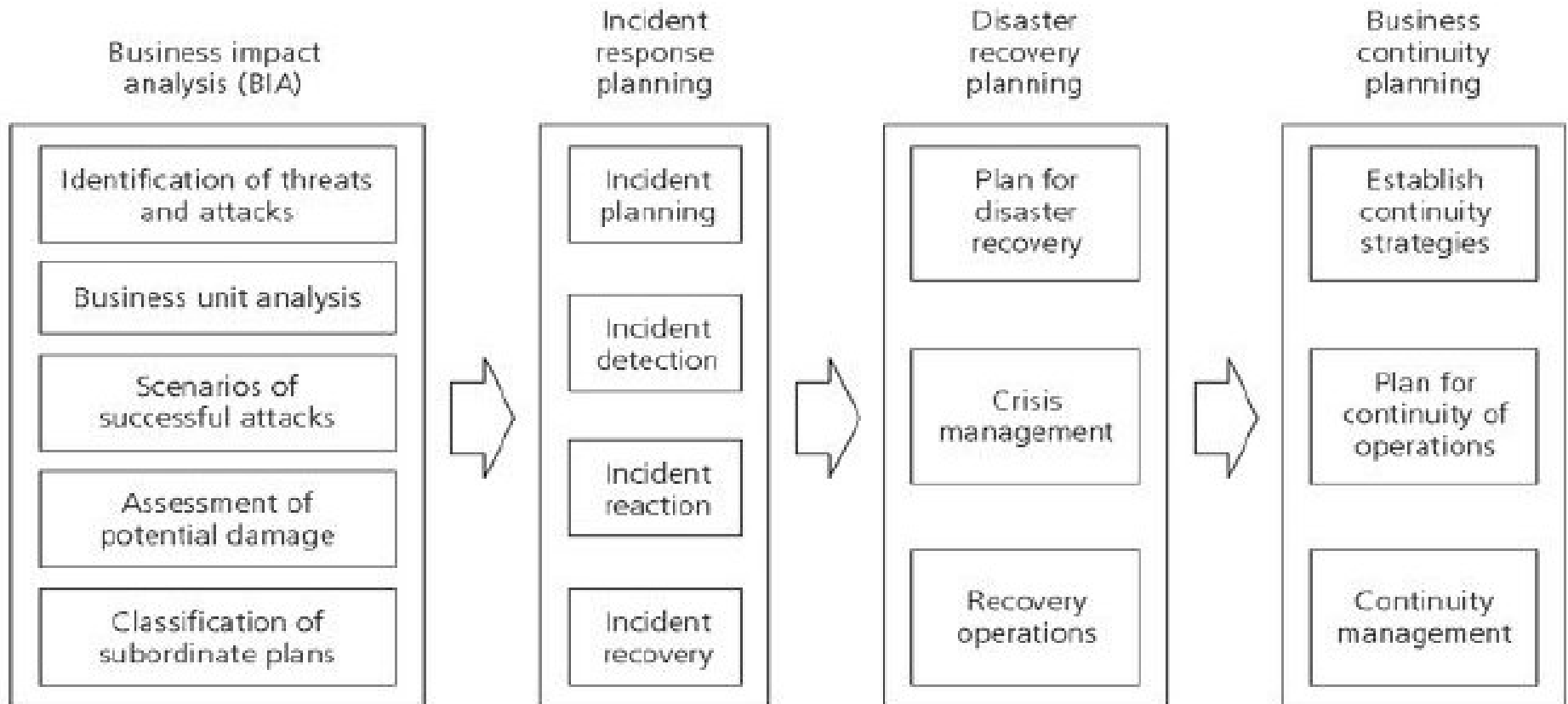
Business Impact Analysis Diagram

System Security Management

- Communications and systems security management is fundamental to the protection of the confidentiality, integrity, availability, authenticity and non-repudiation characteristics of information.
- Formal validation of system security is achieved through a process of certification and accreditation.

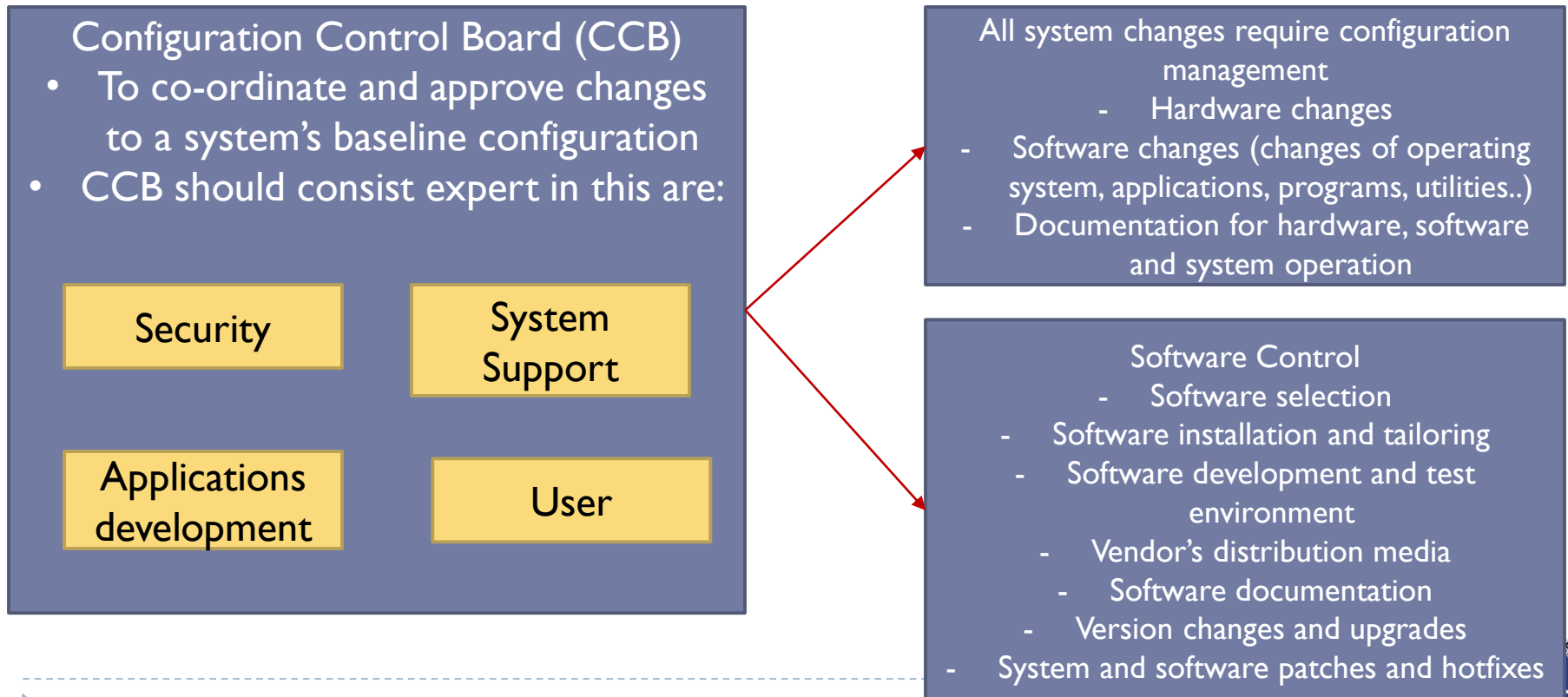| CERTIFICATION	ACCREDITATION
- development and maintenance of security documentation - Confirmation by system developer or administrators that the documentation is correct and complete - The documented security architecture, mechanism and processes have been implemented	- Follows on from certification - Process of verifying the system's security and formally authorizing the system for operation. - Involves independent review of the certification documentation to ensure security measures meet the required level of security for the information and services managed by the system - Involves site inspections to ensure that security has been implemented according to the documentation and appropriately for the environment

Once the verification process is complete, the accreditation authority will use the results to determine whether the system has approval to operate or not.

Certified and accredited systems are systems that have had their security compliance technically evaluated for optimal performance in a specific environment and configuration.

System Security Management: Configuration Management

- Set of **measures** to **keep system security, integrity and functionality from degrading** when introducing **new facilities** or **eliminating faults**.
- Configuration management is fundamental to the continued strength of system security.

Configuration Control Board (CCB)
- To co-ordinate and approve changes to a system's baseline configuration
- CCB should consist expert in this are:

| Security |
| System Support |
| Applications development |
| User |

All system changes require configuration management
- Hardware changes
- Software changes (changes of operating system, applications, programs, utilities..)
- Documentation for hardware, software and system operation

Software Control
- Software selection
- Software installation and tailoring
- Software development and test environment
- Vendor's distribution media
- Software documentation
- Version changes and upgrades
- System and software patches and hotfixes

Protecting Storage Media

- Media should protected against:
    - Damage
    - Theft
    - Loss
    - Unauthorized access
    - Virus of other software, or networks, attacks
    - Inappropriate sanitization and/or disposal

- Clearly defined procedure should be used to manage removable computer media
- All media should be marked and stored according to the most sensitive or highest-classifies information contains.
- It must be labelled clearly and distinctively with the security classification (Sensitive, Restrictive)

- All movement of media in and out should be recorded
- On arrival for classification, damage and malicious software such as viruses
- On departure for classified information and viruses
- Adequate back-up facilities should be used so that all essential business data and software can be accessed and recovered after an incident.
- Back-up for each system should meet the requirements of the organization business continuity plan.

- Waste material that contain official information must be disposed of securely.

Protection of System Documentation
- System documentation may contain a range of sensitive information and should be protected from unauthorized access by:
    - Physically securing it
    - Minimizing its distribution
    - Disposing securely when is outdated

Security in Software Applications
- Should have validation checks to detect any such corruption.

Operating System and Package Maintenance
- All changes to operating system software must ne managed through strong configuration management process
- Changes to original copies and standard commercial software should be discourage
- If necessary, change should made only to a clearly identified copy, the original software should be retained

Protection of Development Suite and Test data
- Development and operational system should be separated to reduce risk of accidental changes or unauthorized access to operational software, processes and data.
- Development and operational software should be run from in different operating environments.
- Source code and configuration files should be protected from unauthorized viewing and changing
- Testing data should be completed before implementation. Test data should be protected and controlled.
- The use of live database containing personal information should be avoided.

Exchanges of Information and Software

- Exchange of information and software should be based on formal agreements, in line with any relevant legislation and licensing agreements

- Procedures and standards should be set to protect information in transit, especially electronic data interchanges.

- Security concern in using leased line or public network that used to communicate between information system that process classified information must be consider :
  - Data interception
  - Data modification
  - User impersonation

REMEMBER

Conversation classified CONFIDENTIAL or above must not be held over telephone circuit unless it has end-to-end cryptographic protection

The use of STRONG device PASSWORD should be mandated, as the password may be the only mechanism that prevents an attacker into personal electronic devices

System that process information classified CONFIDENTIAL or above must not be connected to internet unless security measure are used such as encryption product

Video-conferencing system should be protected by encryption system
- The auto-answer features should be disables
- The internet should not be used as a vehicle for sensitive video-conferencing

Security Requirements of System

- System must consider:
  - Infrastructure
  - Applications, including user-developed applications

- Before developing information systems, organizations should identify and agree on security need.
- At the requirement phase of information system projects, as part of the overall business case, all security needs should be:
  - Identified
  - Justified
  - Agreed
  - Documented

Security Standards

- STANDARD : Collection of system-specific requirements that must be met

- The computer network model also suffers from the standardization problem.

- Security protocols, solutions, and best practices that can secure the computer network model come in many different types and use different technologies resulting in incompatibility of interfaces , less interoperability, and uniformity among the many system resources with differing technologies within the system and between systems.

- System managers, security chiefs, and experts, choose or prefer standards, that are based on service, industry, size, or mission.

Security Standards

- Bodies and organizations behind the formulation, development, and maintenance of these standards. These bodies fall into the following categories:

- International organizations such as the Internet Engineering Task Force (IETF), the Institute of Electronic and Electric Engineers (IEEE), the International Standards Organization (ISO), and the International Telecommunications Union (ITU)
- Multinational organizations like the European Committee for Standardization (CEN), the Commission of European Union (CEU), and the European
- Telecommunications Standards Institute (ETSI)
- National governmental organizations like the National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI), and the Canadian Standards Council (CSC)
- Sector-specific organizations such as the European Committee for Banking Standards (ECBS), the European Computer Manufacturers Association (ECMA), and the Institute of Electronic and Electric Engineers (IEEE)
- Industry standards such as the RSA, the Open Group (OSF+X/Open), the Object Management Group (OMG), the World Wide Web Consortium (W3C)), and the Organization for the Advancement of Structured Information Standards (OASIS)
- Other sources of standards in security and cryptography

Organization	Standards
IETF	IPSec, XML Signature XPath Filter2, X.509, Kerberos, S/MIME
ISO	ISO 7498–2:1989 Information processing systems – Open Systems Interconnection, ISO/IEC 979x, ISO/IEC 997, ISO/IEC 1011x, ISO/IEC 11xx, ISO/IEC DTR 13xxx, ISO/IEC DTR 14xxx
ITU	X.2xx, X.5xx, X.7xx, X.80x,
ECBS	TR-40x
ECMA	ECMA-13x, ECMA-20x
NIST	X3 Information Processing, X9.xx Financial, X12.xx Electronic Data Exchange
IEEE	P1363 Standard Specifications, For Public-Key Cryptography, IEEE 802.xx, IEEE P802.11 g, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
RSA	PKCS #x – Public-Key Cryptographic Standard
W3C	XML Encryption, XML Signature, exXensible Key Management Specification (XKMS)

Table 1: Organizations and their standards

Security Standards based on type of service/industry

Area of application	Service	Security standard
Internet security	Network authentication	Kerberos
	Secure TCP/IP communications over the Internet	IPSec
	Privacy-enhanced electronic mail	S/MIME, PGP
	Public-key cryptography standards	3-DES, DSA, RSA, MD-5, SHA-1, PKCS
	Secure hypertext transfer protocol	S-HTTP
	Authentication of directory users	X.509/ISO/IEC 9594–8:2000:
	Security protocol for privacy on Internet/transport security	SSL, TLS, SET
Digital signature and encryption	Advanced encryption standard/PKI/ digital certificates, XML digital signatures	X509, RSA BSAFE SecurXML-C, DES, AES, DSS/DSA, EESSI, ISO 9xxx, ISO, SHA/ SHS, XML Digital Signatures (XMLD- SIG), XML Encryption (XMLENC), XML Key Management Specification (XKMS)
Login and authentication	Authentication of user's right to use system or network resources	SAML, Liberty Alliance, FIPS 112
Firewall and system security	Security of local, wide, and metropolitan area networks	Secure Data Exchange (SDE) protocol for IEEE 802, ISO/IEC 10164

Table 2: Security standards based on services

Security Standards based on size/implementation

- If the network is small or it is a small organization security standards can be spelled out as either the organization's security policy or its best practices on the security of the system, including the physical security of equipment, system software, and application software.

Physical Security

This emphasizes the need for security of computers running the Web servers and how these machines should be kept physically secured in a locked area. Standards are also needed for backup storage media like tapes and removable disks.

Operating systems

The emphasis here is on privileges and number of accounts, and security standards are set based on these.

For example, the number of users with most privileged access like root in UNIX or Administrator in NT should be kept to a minimum. Set standards for privileged users. Keep to a minimum the number of user accounts on the system. State the number of services offered to clients computers by the server, keeping them to a minimum. Set a standard for authentication such as user passwords and for applying security patches.

System logs

Logs always contain sensitive information such as dates and times of user access. Logs containing sensitive information should be accessible only to authorized staff and should not be publicly accessible. Set a standard on who and when logs should be viewed and analyzed.

Data security

Set a standard for dealing with files that contain sensitive data.

For example, files containing sensitive data should be encrypted wherever possible using strong encryption or should be transferred as soon as possible and practical to a secured system not providing public services.

Security Standards based on interests

- Institutions and government agencies choose to pick a security standard based solely on the interest of the institution or the country.

Area of application	Service	Security standard
Banking	Security within banking IT systems	ISO 8730, ISO 8732, ISO/TR 17944
Financial	Security of financial services	ANSI X9.x, ANSI X9.xx

Table 3: Interest-based security standards

Security best practices

- Best Practices : A human **practice**; that is, a repeated or. customary method used by people to perform

- There is a rich collection of standards security tools on the system and information security landscape because as technology evolves, the security situation becomes more complex, and it grows more so every day.

- Security experts and security managers must know how and what to protect and what controls to put in place and at what time. It takes security management, planning, policy development, and the design of security procedures.

Security best practices / guidelines

Best Practices provided by CyberSecurity Malaysia

Security best practices / guidelines
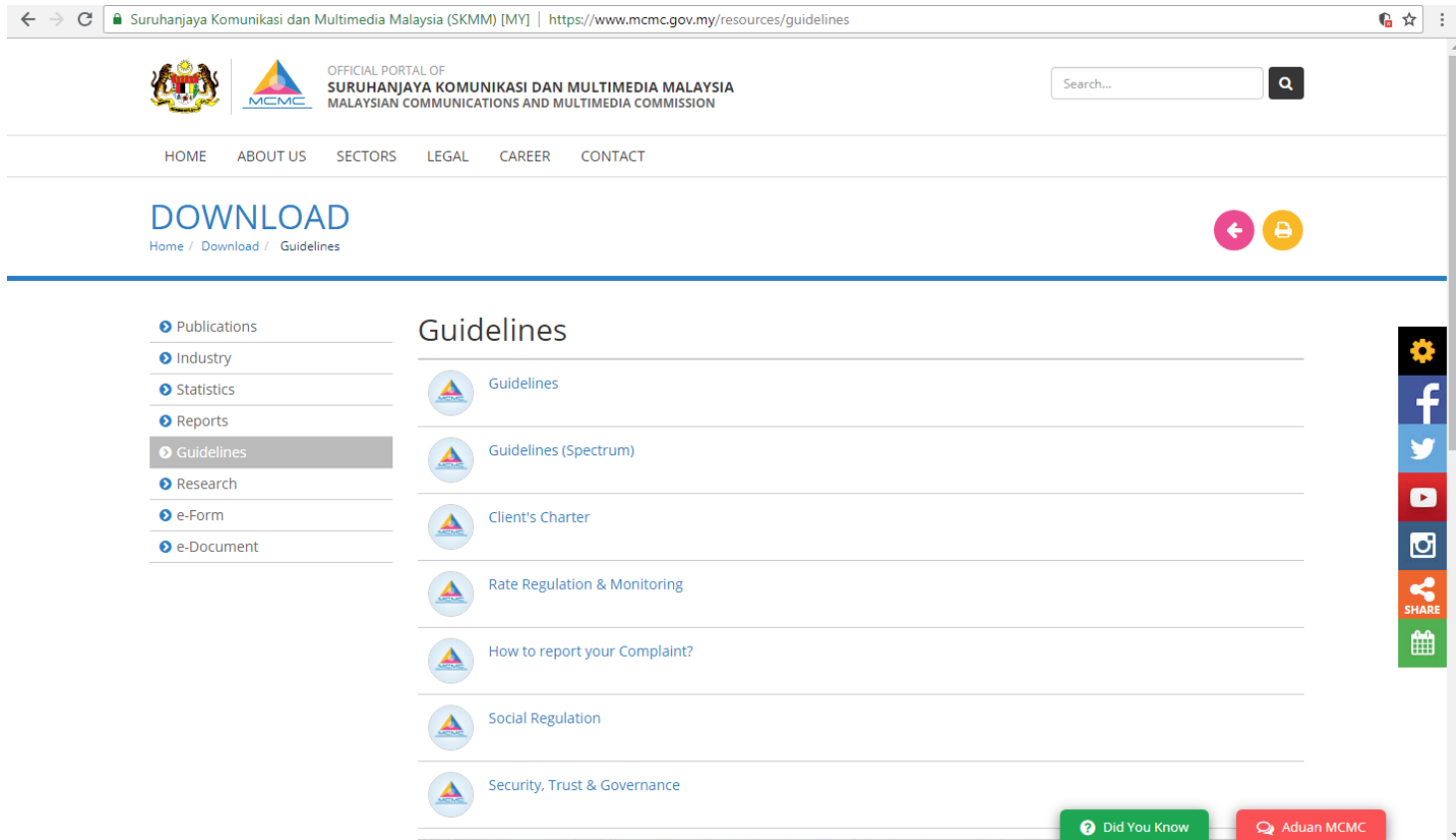
Guidelines provided by MCMC