CS4050 – WEEK 13: INFORMATION SYSTEMS AUDIT AND CONTROL

FAST NUCES – SPRING 2024

BS COMPUTER SCIENCE

CHAPTER 5: PROTECTION OF INFORMATION ASSETS

- Part A: Information Asset Security & Control
  - Information Asset Security Frameworks, Standards & Guidelines
  - Privacy Principles
  - Physical Access and Environmental Controls
  - Identity & Access Management
  - Network & End-Point Security
  - Data Classification
  - Data Encryption & Encryption-related Techniques
  - Public Key Infrastructure
  - Web-based Communication Technologies
  - Visualized Environments
  - Mobile, Wireless & Internet-of-things-devices
- Part B: Security Event Management
  - Security Awareness Trainings and Programs
  - Information System Attack Methods and Techniques
  - Security Testing Tools and Techniques
  - Security Monitoring Tools and Techniques
  - Incident Response Management
  - Evidence Collection and Forensics

PART A: INFORMATION ASSET SECURITY & CONTROL

- Information Asset Security Frameworks, Standards & Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity & Access Management
- Network & End-Point Security
- Data Classification
- Data Encryption & Encryption-related Techniques
- Public Key Infrastructure
- Web-based Communication Technologies
- Visualized Environments
- Mobile, Wireless & Internet-of-things-devices

INFORMATION ASSET SECURITY FRAMEWORKS, STANDARDS AND GUIDELINES

- Auditing the Information Security Management Framework
  - Reviewing Written Policies, Procedures and Standards
  - Formal Security Awareness and Training
  - Data Ownership
  - Data Owners
  - Data Custodians
  - Security Administrator
  - New IT Users
  - Data Users
  - Documented Authorizations
  - Terminated Employee Access

Security Baseline

PRIVACY PRINCIPLES

- **Breakthrough:** General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States
- Good practice to ensure Privacy:
  - It should be considered from the outset and be built in by design.
  - It should be systematically built into policies, standards and procedures from the beginning. •
  - Private data should be collected fairly in an open, transparent manner.
  - Private data should be kept securely throughout their life cycle.
  - Private data should only be used and/or disclosed for the purpose for which they were collected.
  - Private data should be accurate, complete and up to date.
  - Private data should be deleted when they are no longer required.

PRIVACY PRINCIPLES

Auditor's Considerations: Privacy should also be considered when conducting an audit. The following seven categories of privacy should be considered when developing audit objectives:

1. Privacy of person
2. Privacy of behavior and action
3. Privacy of communication
4. Privacy of data and image (information)
5. Privacy of thoughts and feelings
6. Privacy of location and space (territorial)
7. Privacy of association

PHYSICAL ACCESS & ENVIRONMENTAL CONTROLS

Control Methods

Category	Description
Managerial (administrative)	Oversight, reporting, procedures and operations of a process. These include policy, procedures, balancing, employee development & compliance reporting.
Technical	Logical controls, provided through the use of technology. E.g. include firewalls, network or host-based intrusion detection systems (IDSs), passwords, and antivirus software.
Physical	Locks, fences, closed-circuit TV (CCTV), and devices that are installed to physically restrict access to a facility or hardware. Physical controls require maintenance, monitoring and the ability to assess and react to an alert should a problem be indicated.

Control Matrix

	Managerial	**Technical**	**Physical**
Preventive	User Registration	Login Screen	Fence
Detective	Audit	Intrusion Detection System (IDS)	Motion Sensor
Corrective	Remove access	Network Isolation	Close fire doors

PHYSICAL ACCESS & ENVIRONMENTAL CONTROLS

- **Control Monitoring & Effectiveness** - If the organization is using a managed security service provider (MSSP) or a security information and event management (SIEM) system, the ability to capture data, and the notification to the operations staff on the deployment of the system, are necessary.
- **Environmental Exposures & Controls** - Equipment Issues and Exposures Related to the Environment, Controls for Environmental Exposures
- **Physical Access Exposures & Controls** - Physical Access Issues and Exposures, Physical Access Controls

IDENTITY AND ACCESS MANAGEMENT

- System Access Permission
- Mandatory and Discretionary Access Controls
- Information Security and External Parties - Identification of Risk Related to External Parties, Addressing Security When Dealing With Customers, Human Resources Security and Third Parties
- Logical Access - Logical Access Exposures (access breaches, data leakage, shutdowns), Familiarization With the Enterprise's IT Environment, Paths of Logical Access
- Access Control Software
- Identification and Authentication
- Logon Ids and Passwords
- Biometrics
- Single Sign-on
- Authorization Issues
- Audit Logging In Monitoring System
- Naming Conventions For Logical Access Controls
- Federated Identity Management

NETWORK AND END-POINT SECURITY

- IS Network Infrastructure
- Enterprise Network Architectures
- Types of Networks (PANs, LANs, WANs, SANs, MANs)
- Network Services
- Network Standards And Protocols
- OSI Architecture
- Application of the OSI Model In Network Architectures
- Network Infrastructure Security

DATA CLASSIFICATION

Data classification is a major part of managing data as an asset. It should define the:

- Importance of the information asset
- Information asset owner
- Process for granting access
- Person responsible for approving the access rights and access levels
- Extent and depth of security controls

Classification of Information	
Public Information	Company website on internet, company brochure, etc.
Private Information	Internal policies, procedures, business email messages, information controlled by legislation, etc.
Sensitive Information	Unpublished financials, trade secrets, future plans, etc.

MISCELLANEOUS TOPICS OF INFORMATION ASSET SECURITY & CONTROL

- Data Encryption and Encryption-related Techniques
- Public Key Infrastructure
- Web-based Communication Technologies
- Visualized Environments
- Mobile, Wireless & Internet-of-things-devices

PART B: SECURITY EVENT MANAGEMENT

- Security Awareness Trainings and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

SECURITY AWARENESS TRAINING AND PROGRAMS

- Security awareness programs should consist of: (i) Training, (ii) Quizzes to gauge retention of training concepts, (iii) Security awareness reminders, such as posters, newsletters or screensavers, and (iv) A regular schedule of refresher training
- Mechanisms for raising information security awareness include the following:
  - Computer-based security awareness and training programs
  - Email reminders and security tips
  - Written security policies and procedures (and updates)
  - Nondisclosure statements signed by the employee
  - Use of different media in promulgating security (e.g., company newsletter, web page, videos, posters, login reminders)
  - Visible enforcement of security rules
  - Simulated security incidents for improving security
  - Rewarding employees who report suspicious events
  - Periodic reviews • Job descriptions
  - Performance reviews

INFORMATION SYSTEM ATTACK METHODS AND TECHNIQUES

- Fraud Risk Factors
- Computer Crime Issues And Exposures
- Internet Threats And Security
- Malware

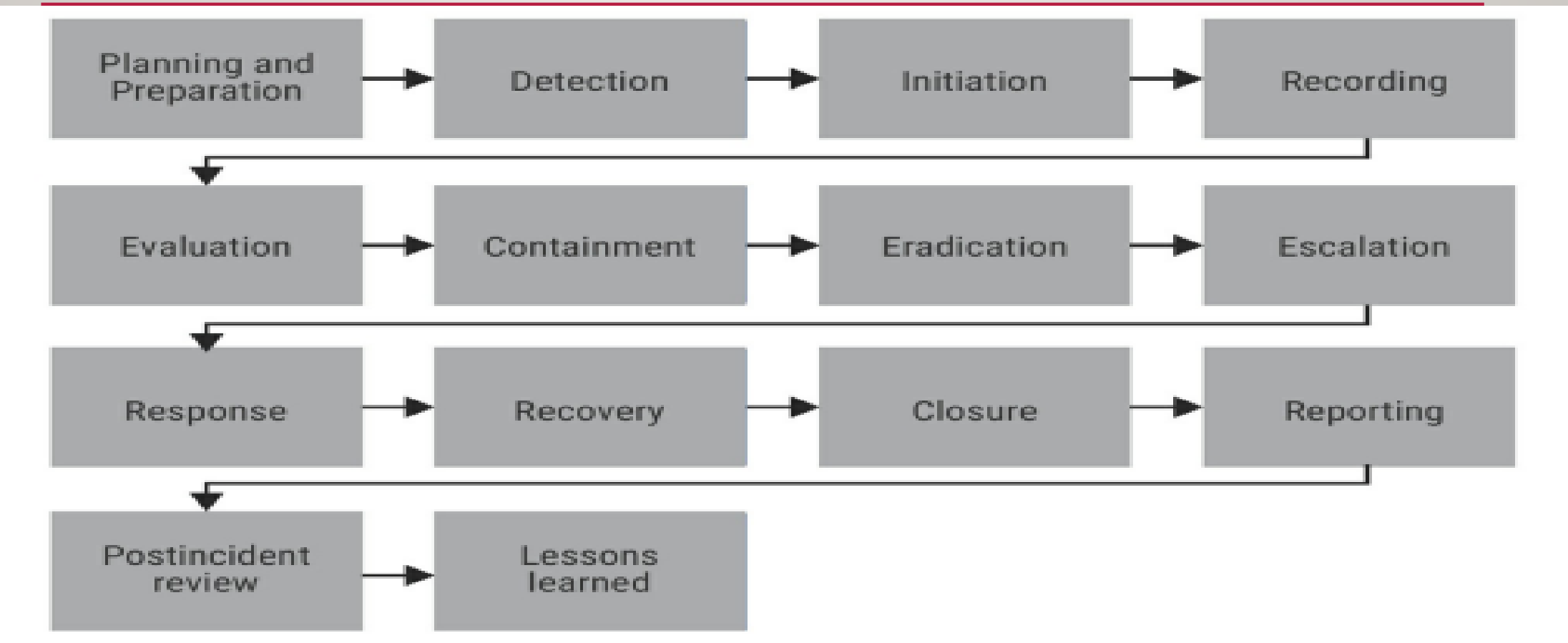
SECURITY TESTING TOOLS AND TECHNIQUES

- Testing Techniques For Common Security Controls
- Network Penetration Tests
- Threat Intelligence

SECURITY MONITORING TOOLS TAND TECHNIQUES

- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Security Information and Event Management (SIEM)

INCIDENT RESPONSE MANAGEMENT PROCESS



EVIDENCE COLLECTION AND FORENSICS

- Computer Forensics
- Protection of Evidence and Chain of Custody

EISENHOWER MATRIX