Audit

Information Security

Course Outline

Course Name: Information Security
Credit Hours: 3(3-0)
Prerequisites: Data Communication and Computer Networks
Course Outline:
Basic notions of confidentiality, integrity, availability; authentication models; protection models; security kernels; Encryption, Hashing and Digital Signatures; audit; intrusion detection and response; database security, hostbased and network-based security issues operational security issues; physical security issues; personnel security; policy formation and enforcement; access controls; information flow; legal and social issues; identification and authentication in local and distributed systems; classification and trust modeling; risk assessment
Reference Materials:
1. *Computer Security: Art and Science*, Matthew Bishop
2. *Cryptography and Network Security* by William Stalling 6th Edition, 2012
3. *Principles of Information Security* 3rd E by Michael E. Whitman and Herbert J. Mattord

Audit

- An audit in information security refers to the ***systematic evaluation*** of an ***organization's security*** **controls**, **processes**, and **practices** to assess their ***effectiveness***, ***compliance with standards*** and ***regulations***, and ***overall security posture***.

Audit cont...

Audit cont...

- The **primary objective** of an ***information security audit*** is to **identify potential** ***vulnerabilities***, ***weaknesses***, and ***areas of non-compliance***, and to **provide** ***recommendations for improvement***.
- Here are the key aspects of an information security audit:

Audit cont...

- **1- Scope Definition:** The ***audit scope*** should be ***clearly defined***, ***outlining the specific systems***, ***processes***, or ***areas*** of the organization that ***will be examined during the audit***.
- It helps ensure that the **audit** ***covers*** the ***relevant aspects of information security***.

Audit cont...

- **2- Compliance Assessment:** The ***audit assesses*** whether the organization's information ***security practices*** comply (fulfil) with ***relevant standards***, ***regulations***, and ***policies***.
- This may include industry-specific standards (e.g., **ISO 27001**), data protection laws (e.g., **GDPR**), and **internal security policies**.

Audit cont...

- **3- Risk Assessment:** The audit evaluates the organization's risk management processes and procedures.
- It assesses **how risks** are ***identified***, ***analyzed***, and ***mitigated*** to **protect** ***sensitive information*** and ***critical assets***.

Audit cont…

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Audit cont...

- **4- Security Controls Evaluation:** The audit examines the ***effectiveness*** of ***security controls*** implemented by the organization.
- This includes **technical controls** (e.g., ***firewalls***, ***access controls***), **administrative controls** (e.g., ***policies***, ***procedures***), and **physical controls** (e.g., ***access control systems***, ***surveillance***).

Audit cont...

- **5- Vulnerability Assessment:** The audit may include ***vulnerability scanning*** and ***penetration testing*** to identify **potential weaknesses** in the organization's infrastructure, applications, and systems.
- It helps **uncover** vulnerabilities that could be exploited by attackers.

Audit cont...

Asset discovery

Detect and manage local and remote endpoints, roaming devices, and closed network (DMZ) machines.

Vulnerability scanning

Spot all OS and third-party vulnerabilities, including vulnerabilities in content management systems, web servers and database software.

Vulnerability assessment

Visualize, analyze, and prioritize vulnerabilities based on CVSS scores, age, exploitability, patch availability, impact type, affected asset count and more.

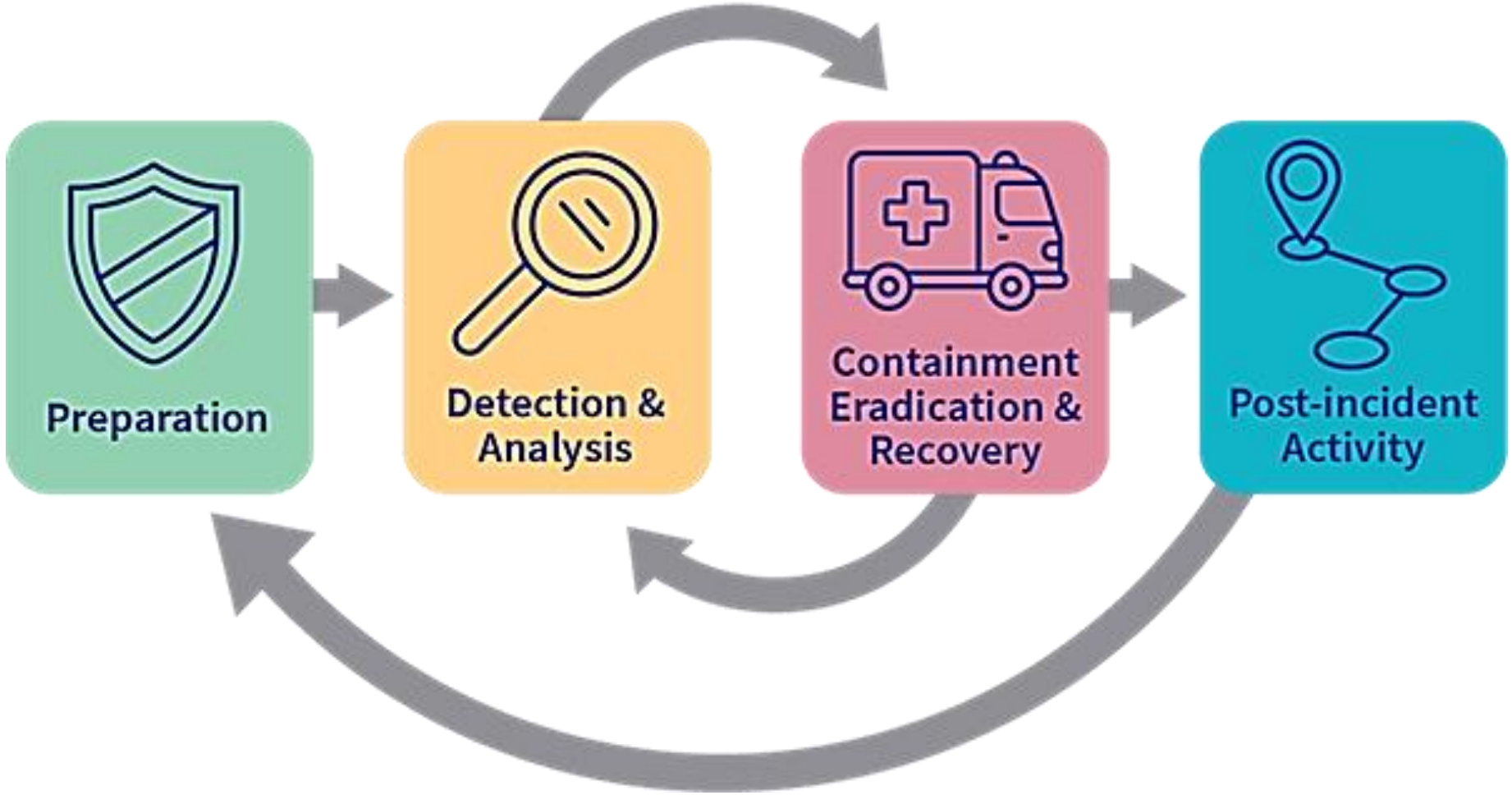
Vulnerability remediation

Deploy automatically correlated patches to seal vulnerabilities, and leverage alternative mitigation measures if no patch is available.

Audit cont...

- **6- Incident Response Evaluation:** The audit assesses the ***organization's incident response capabilities***, including its ***ability to detect***, ***respond to***, and ***recover*** from **security incidents**.
- It evaluates the incident management processes, incident handling procedures, and the effectiveness of incident response plans.

Audit cont...



Audit cont...

- **7- Documentation Review:** The audit **examines** the ***documentation*** related to ***information security***, such as ***policies***, ***procedures***, ***security incident reports***, and ***system configuration*** documentation.
- It ensures that proper documentation exists and is maintained to support security practices.

Audit cont...

- **8- Reporting and Recommendations:** At the end of the audit, a **comprehensive report** is prepared that ***summarizes*** the **findings**, including ***identified vulnerabilities***, ***non-compliance issues***, and ***areas of improvement***.
- The report also provides **recommendations** and **actionable steps** to enhance the organization's security posture.

Audit cont...

- Information security audits play a crucial role in helping organizations identify security gaps, improve their security posture, and demonstrate compliance with regulatory requirements.
- They provide valuable insights and recommendations for enhancing the overall security of an organization's information assets.