LEARNING OBJECTIVES

- LO#01: Explain Different Information Security Controls
- LO#02: Summarize Network Segmentation Concepts
- LO#03: Use Network Security Solutions
- LO#04: Explain Data Leakage Concepts
- LO#05: Summarize Data Backup Process
- LO#06: Explain Risk Management Concepts and Frameworks
- LO#07: Summarize Business Continuity and Disaster Recovery Process
- LO#08: Explain Cyber Threat Intelligence

- LO#09: Explain Threat Modeling Methodology
- LO#10: Explain Different Types of Penetration Testing and its Phases
- LO#11: Summarize Security Operations Concepts
- LO#12: Explain Different Phases of Computer Forensic Investigation
- LO#13: Explain Software Development Security
- LO#14: Summarize Security Governance Principles
- LO#15: Explain Asset Management Process

LO#01: Explain Different Information Security Controls

Notes: _____
_____
_____
_____
_____
_____
_____

Information Security Management Program

CEH

- ❏ Programs that are designed to **enable a business to operate in a state of reduced risk**
- ❏ Encompasses all **organizational** and **operational processes**, and participants relevant to information security

Information Security Management Framework

A combination of **well-defined** policies, processes, procedures, standards, and guidelines to establish the required **level of information security**

Security Policy

Roles & Responsibilities	Security Guidelines & Frameworks

Risk Management	Technical Security Architecture	Asset Classification	Security Management and Operations

Business Resilience

Business Continuity Management	Disaster Recovery

Training & Awareness

Security Metrics & Reporting

Governance | Compliance

Enterprise Information Security Architecture (EISA)

CEH

- ❏ EISA is a set of requirements, processes, principles, and models that **determines the structure and behavior of an organization's information systems**

EISA Goals

1. **Helps to monitor and detect network behaviors** in real time, acting upon internal and externals security risks

2. Helps an organization **detect and recover from security breaches**

3. Helps to prioritize the resources of an organization and **monitor various threats**

4. **Benefits organization's budget in cost prospective** when incorporated in incident response, disaster recovery, event correlation, and other security provisions

5. Helps to analyze the procedure needed for the IT department to function properly and **identify assets**

6. **Helps to perform risk assessment** of an organization's IT assets with the cooperation of IT staff

Notes: _____
_____
_____
_____
_____
_____
_____