

# Welcome to the (ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP) Training Course

# Course Agenda

**Domain 1:** Security and Risk Management

**Domain 2:** Asset Security

**Domain 3:** Security Architecture and Engineering

**Domain 4:** Communication and Network Security

**Domain 5: Identity and Access Management (IAM)**

**Domain 6:** Security Assessment and Testing

# Course Agenda (continued)

**Domain 7: Security Operations**

**Domain 8: Software Development Security**

# Domain 5

## Identity and Access Management (IAM)

# Domain Objectives

1. Identify standard terms for applying physical and logical access controls to environments related to their security practice.
2. Apply physical and logical access controls to environments with relation to the (environment's or access controls') security practice.
3. Define the process of user and systems access review.
4. Apply the appropriate control types/categories for provisioning and deprovisioning of identities.
5. Classify various identification, authentication, and authorization technologies and for use in managing people, devices, and services.

## Domain Objectives (continued)

6. Differentiate the languages and protocols that are related to roles and systems that support federation.
7. Select the appropriate technologies and protocols for establishing a federated environment that satisfies business requirements.
8. Appraise various access control models to meet business security requirements.
9. Name the significance of accountability in relationship to identification, authentication, and auditing.

# Domain Agenda

---

Control Physical and Logical Access to Assets

---

Identity and Access Provisioning Lifecycle

---

Identification and Authentication of People, Devices, and Services

---

Identity Management Implementation

---

Implement and Manage Authorization Mechanisms

---

# Domain Agenda (continued)

---

Accountability

---

Domain Review

---



# Module 1

Control Physical and Logical  
Access to Assets

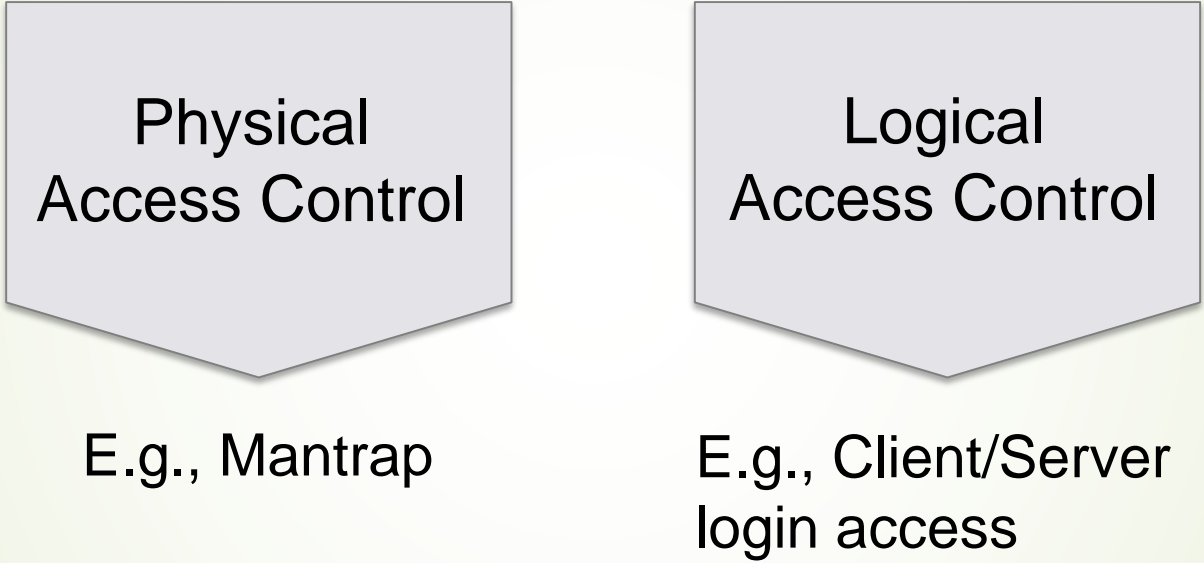
# Module Objectives

1. Identify standard terms for applying physical and logical access controls to environments related to their security practice.
2. Apply physical and logical access controls to environments with relation to the (environment's or access controls') security practice.

# Systems

- **Access control:** Authorization and restriction of access as specified by business and security requirements.
- **Logical access control system:** Automated system, controlling an individual's ability to access computer systems.
- **Physical access control system:** Automated system that maintains passage of people or assets through a controlled opening.

# Logical and Physical Access Control Systems



Physical  
Access Control

E.g., Mantrap

Logical  
Access Control

E.g., Client/Server  
login access

# Devices

- Hardware/software
- Access control tokens
- Biometric readers



# Facilities Case: Department of Homeland Security

1. What distinct roles can you locate within the physical access control systems (PACS) application's four areas? What are general security roles that can be used as placeholders for the PACS application roles?
2. Name the logical or physical systems that are described in the PACS application.
3. What assumptions could you make about the nature of the information related to identification in the PACS application cited below?

# Module 2

## Identity and Access Provisioning Lifecycle

# Module Objectives

1. Define the process of user and systems access review.
2. Apply the appropriate control types/categories for provisioning and deprovisioning of identities.



# User Access Review

- Enforces security policy
- Continues over the lifecycle of access
- Mitigates vulnerabilities associated with aggregation
- Concludes with termination of access

# System Account Access Review

- Presents often-exploited vulnerability for attackers
- Securing begins with renaming account
- Some system accounts further complicated by being service accounts

# Provisioning and Deprovisioning

- Provision a user account and apply user permissions
- Modify user permissions
- Deprovision user account and end user permissions



## Activity: Identify the Roles and Control Types and Categories of Provisioning and Deprovisioning

### **INSTRUCTIONS**

Working together in small teams, answer the questions below.

- What additional controls (choose from the CIA triad) could be added to each of the three phases of the process flow?
  - Add control types
  - Add control categories
- What roles can you identify in the process flow (i.e., Custodian, Data Owner, etc.)?

# Module 3

Identification and Authentication of People,  
Devices,  
and Services

# Module Objectives

1. Classify various identification, authentication, and authorization technologies for use in managing people, devices, and services.

# Identity Management Implementation

These are the four elements of identity management implementation:

Identification

Authentication

Authorization

Accountability


# Session Management

RFC 2965 provides an example of session management with cookies. All transaction requests are maintained and tracked as a user engages requests from a website.



# Registration and Proofing of Identity

NIST SP 800-63-3 contains three levels of assurance for digital identities:



IAL1: Self-asserted

IAL2: Remote or in-person

IAL3: Verified by authorized credential  
service provider

# Module 4

## Identity Management Implementation

# Module Objectives

1. Differentiate the languages and protocols that are related to roles and systems that support federation.
2. Select the appropriate components for a federated environment relevant to business requirements.

# Federated Identity Management (FIM)

- **Federated Identity Management (FIM)** is specified and sought for use between different organizations or entities that need to share resources or have users in common.
- Services that provide federation:
  - Security Assertion Markup Language (SAML)
  - Open Authorization (OAuth)

# Security Assertion Markup Language (SAML) Roles

Roles:

- Identity provider (IdP)
- Service provider/relying party
- User/principal

# Security Assertion Markup Language (SAML)

## Components

Components:

- Assumptions
- Bindings
- Protocols
- Profiles

# Open Authentication

Roles:

Resource owner

Authorization server

Resource server

Client application

# Integrate Identity Management as a Third-Party Service

- On-Premise
- Cloud





## Activity: Select the Appropriate Components for a Federated Environment Linking Two or More Companies' Discrete Resources

### **INSTRUCTIONS**

As a team, reflect upon and discuss actual business needs within your corporation.

- Each team should allow every participant to relate business needs within each company.
- Instead of contributing to or jumping to a conclusion on what solution there might be, each participant should ask deeper questions of the presenter to uncover additional insights into the environment.
- Expose assumptions by asking “why” a thing is so or to give an example of a statement shared.
- Create a business case for utilizing either OAuth or SAML or both. What are actual business drivers?
- Also select if it should be solved on-premise or in the cloud and why.
- Create analogous connections between the roles in SAML and OAuth.

# Module 5

## Implement and Manage Authorization Mechanisms

# Module Objectives

1. Appraise various access control models to meet business security requirements.

# Types of Access Control

NIST SP 800-192 specifies the following types of access control:

- ➡ Discretionary access control (DAC)
- ➡ Mandatory access control (MAC)
- ➡ Nondiscretionary access control (NDAC)
- ➡ Role-based access control (RBAC)
- ➡ Rule-based access control (RBAC)
- ➡ Attribute-based access control (ABAC)



## Activity: Select the Appropriate Access Control Type (Rule, Role, Attribute, etc.) for Specific Business Needs

### **INSTRUCTIONS**

As a team, reflect upon and discuss actual business needs within your corporation.

- Each team should allow every participant to relate business needs within each company.
- Instead of contributing to or jumping to a conclusion on what solution there might be, each participant should ask deeper questions of the presenter to uncover additional insights into the environment.
- Expose assumptions by asking “why” a thing is so or to give an example of a statement shared.
- Create a business case for utilizing the previously reviewed access control methods. Use the best examples from each participant for each method.

# Module 6

## Accountability

# Module Objectives

1. Name the significance of accountability in relationship to identification, authentication, and auditing.

# Accountability

Ensuring that account management has assurance that only authorized users are accessing the system and that authorized users are using the system properly.



# Module 7

## Domain Review

# Domain Summary

- Identity and access management (IAM) includes controls related to physical and logical access to assets along with managing an identity and access provisioning lifecycle.
- The essential elements of an access provisioning lifecycle include a full range of items under system management related to people, devices, and resources.
- Identification, authentication, and authorization ensure that the right users or accessing the system and that the correct usage of resources is happening.

# Domain Review Questions

1. What are the two primary types of access control systems and what is one way that access control systems are maintained?
  - A. Physical and network; due diligence
  - B. Deterrent and corrective; due care and due diligence
  - C. Integrity and availability; by as much security as can be safely applied
  - D. Logical and physical; central administration of access control systems

# Answer

The correct answer is D.

NIST SP 800-53 defines two primary access control systems: logical and physical, and both are maintained by administration and security policy. Due diligence and care are overarching organizational posture and actions that aid in avoiding the accusation of negligence and liability. Using as much security as can be safely applied is not a prudent approach to security and doesn't answer the question. Integrity and availability are overarching tenants of information security.

# Domain Review Questions

2. What actions specify enrolling and the opposite of enrolling user IDs within an organization?
  - A. Identity creation and disposition
  - B. Disposition only
  - C. Creation only
  - D. Provisioning and deprovisioning

# Answer

The correct answer is D.

Identity creation is an activity that would be included in provisioning, but the only correct answer is provisioning and deprovisioning.

# Domain Review Questions

3. What are the three roles within Security Assertion Markup Language (SAML)?
  - A. Identity provider, relying party, service provider
  - B. Identity provider, relying party, user
  - C. Identity provider, service provider, relative token
  - D. Attributes, principal, bindings

# Answer

The correct answer is B.

Attributes and bindings are components of SAML. Relative token is a distractor. Relying party is an alternate term for a service provider.



# Domain Review Questions

4. Name two roles related to Open Authorization (OAuth).
  - A. Resource provider, resource server
  - B. Resource provider, resource relying party
  - C. Authorization server, resource server
  - D. Authorization server, authorization owner

# Answer

The correct answer is C.

There isn't a resource provider owner in OAuth, but there is a resource owner and server. There is also no authorization owner.

# Domain Review Questions

5. If an organization demanded that an enrolling party or claimant needed to present themselves in person at an enrolling agent to authenticate their assertion to their identity, what level of assurance would they be providing according to NIST SP 800-63-3?
- A. IAL1
  - B. IAL 2
  - C. IAL 3
  - D. None of the above

# Answer

The correct answer is B.

IAL 2 is remote or in-person authentication of an identity. IAL 1 is self-assertion. IAL 3 is assertion verified by a credential service provider.

# Domain Review Questions

6. What provides assurance that a user of a system is consuming resources as intended?
- A. Accountability
  - B. Noninterference
  - C. Spoliation
  - D. Subsystem

# Answer

The correct answer is A.

Noninterference is a security model. Spoliation is the destruction, concealment, or damaging of information. Subsystems are low level systems that support operating systems.

# Domain Review Questions

7. How does system account review differ from user account review?
- A. User account review is connected to systems and system account review is connected to users
  - B. User account and system account review are the same
  - C. User account review targets user IDs and system account review targets built-in administrative and other non-user ID accounts
  - D. None of the above

# Answer

The correct answer is C.

User account reviews are related to regular IDs and system account reviews are connected to administrator IDs and non-user IDs. Answer A is the inverse of the correct answer. Answers B and D are not true.



# Domain Review Questions

8. Special Publications 800-53r4 defines physical access control as an automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on (a)
- A. Audit and assurance
  - B. Scoping and tailoring
  - C. Guidelines and tailoring
  - D. Set of authorization rules

# Answer

The correct answer is D.

Tailoring and scoping are used to apply a set of controls within an environment that fit the internal requirement utilizing specific controls. Auditing the controls would provide assurance about the effectiveness of the controls.

# Domain Review Questions

9. What is an appropriate reason to disable or revoke a user account after a review?
- A. A user is voluntarily terminated from an organization
  - B. An account has been inactive for a period that surpasses the organizational policy
  - C. The user account is no longer appropriate for the job description or role
  - D. All of the above

# Answer

The correct answer is D.

Answers A through C are all correct because these are appropriate reasons to disable or revoke a user account.

# Domain Review Questions

10. Your organization shares a customer base with another organization that you partner with to provide a more complete solution. You will not be sharing the customer user IDs or passwords with your partner, so how will your partner allow your customers to access their resources in a secure fashion?
- A. They will not allow it because it is not ethical
  - B. Your organizations will use OAuth
  - C. XML will solve the needs related to the requirements
  - D. Set up two servers and exchange information in a sanitized fashion

# Answer

The only correct answer is B.

Answers A and D are illogical, incorrect, and don't solve the requirements. XML is the underlying language used by SAML and while SAML answers to the needs for federated security, SAML wasn't mentioned.