Certified Access Management Specialist® (CAMS)
Program Overview

Overview

Access management also known as rights management is the execution of policies and procedures for granting authorized individuals the right to access services, functions, data, and physical locations while preventing non-authorized individuals from accessing systems, assets, and other services.

Access management is one of the information security disciplines which interacts with users and their management the most and is critical to the implementation of policies and procedures to support the enterprise security goals, maintain access controls, and mitigate risks.

Identity Management Institute® (IMI) developed the Certified Access Management Specialist® (CAMS) training program for testing, analysis, and evaluation of the knowledge, skills and abilities of professionals for the purpose of certification and re-certification in the field of access management. CAMS® is a registered trademark of IMI.

Access Management Role

In the fulfillment of their duties, CAMS professionals must in general ensure that:

- Users and their approvers are properly identified,
- Access is approved and granted on a timely basis,
- Access is removed timely and completely when users change jobs or roles,
- Access Control Matrix is maintained and periodically audited to ensure access permissions are valid and accurate,
- User activities are recorded, and
- Incidents or events are properly managed.

Critical Risk Domains™

The 10 Critical Risk Domains which CAMS professionals must understand and master include the following:

1. Security Objectives
2. Threats
3. Access Controls
4. Rights Management
5. Identification

6. Authorization
7. Authentication
8. Access Control Matrix
9. Logging and Monitoring
10. Event Management

Critical Risk Domain Details

1. *Security Objectives*: There are three security objectives or goals which CAMS must understand and help achieve which are as follows:
   - *Confidentiality* - also known as privacy or secrecy, meaning that the computing systems and data can be accessed and read only by authorized parties,
   - *Integrity* - meaning that the assets can only be modified or deleted by authorized parties in authorized ways, and
   - *Availability* - meaning that the systems, data and other assets are accessible to the authorized parties in a timely manner as determined by service level agreements and requirements.
2. *Threats*: Can be divided into internal and external threats. Internal threats arise from individuals who have authorized access. And external threats arise from outside intruders such as hackers. In information security, a threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm.
3. *Access Controls*: Access controls refer to security features that control who can access which resources. They are the selective restrictions of access to a physical location, system, data, services, and functions. Access control components include:

   - Elements
   - Models
   - Techniques
   - Access rights
   - Access Control Lists
   - Roles
   - Administration
   - Capabilities

- Methods
- Types
- Practices
- Access control systems

4. *Rights Management*: Rights or permission management refers to the policies and procedures which govern how individuals request and gain access to systems, resources and services as well as how access is managed throughout the identity lifecycle.
5. *Identification*: The act of identifying someone for the purposes of validating their requests is called identification. Before access requests can be processed, authorized, and granted, the person requesting and/or authorizing access as well as the user must be properly identified.
6. *Authorization*: Authorization is the function of specifying and approving access rights to various data, resources, services and assets. Authorization is one of the critical components of information security and access controls. In addition, the automated system authorization process enforces management authorization determining what types of activities, resources, or services a user is permitted to access.
7. *Authentication*: Various access control schemes provide a mechanism for identifying a user, typically by having the user enter a valid user name and password before access is granted, although, some entities and systems may select biometric authentication. The process of authentication is based on each user having a unique set of criteria for gaining access.
8. *Access Control Matrix*: ACM is a tool used for the documentation and accounting of user access (subject) to various resources (objects). It is an abstract model which provides an accounting of access rights at a given point in time.
9. *Logging and Monitoring*: Various tools may be considered, deployed, and used by CAMS such as electronic surveillance and event monitoring in order to monitor user activities and detect any deviations from the established policies and authorized access rights. It must be noted that authorized users may not be directly involved in violations as their login credentials may have been subject to theft and abuse by others.
10. *Event* Management: Any detected access violations or suspicious activities must be followed-up, investigated, resolved, and potentially escalated in accordance with event management policies and procedures to ensure access is maintained in compliance with established objectives.

Certified Access Management Specialist® (CAMS)
Program Overview

Who Should Become a CAMS

Professionals who are engaged in any of the following activities either directly or in a support role will greatly benefit by becoming a Certified Access Management Specialist as they will improve their skills and increase their credibility:

- Receiving and verifying access requests,
- Reviewing access right approvals,
- Granting, correcting and removing access rights,
- Monitoring access activities,
- Auditing access control lists,
- Following up on suspicious activities, and
- Investigating and resolving access incidents.

Certification Process

For CAMS eligibility, application process, costs and maintenance, please visit the CAMS page on the IMI website at http://www.identitymanagementinstitute.org