Certified Identity Management Professional ™ (CIMP)
Overview & Curriculum

Overview

There are many factors contributing to the growing need for identity management professionals and technologies. First, the number of devices and their users are growing. These devices are increasingly interconnected and must communicate with one another in order to authenticate the machines and users for requesting services and completing transactions.

Managing access for dispersed and diverse users such as employees, customers, and business partners to systems whether hosted internally or externally is another challenge as users require quick access while businesses and regulators need to identify users, and authorize the appropriate access consistent with changing user roles and responsibilities. In fast paced organizations with a high user turnover rate, identity and access management is even more challenging and important to reduce fraud and secure data.

Lastly, decentralized and unstructured nature of many directory services has led to an inefficient and sometimes unmanageable user access provisioning, auditing, and reporting, exposing organizations to significant security, reputation, and regulatory compliance risks. Centralizing distributed directories is critical for efficient management of user identities, and, compliance with related regulations.

Identity Management Solutions

In order to address various identity management risks and challenges some of which are described above, organizations are increasingly considering technology solutions to enable centralized and automated user access management.

Certified Identity Management Professional ™ (CIMP)
Overview & Curriculum

Identity management is a collection of technology components and processes. One of the major components of an identity management architecture is a directory service or repository of the identity information such as user name, department, email, and access rights. The service interacts with other components to authenticate users and manage access to authorized functions and records. Distributed directory services are commonly used, however, the ultimate goal is to centralize and integrate identity management as much as possible to improve the identity management process and efficiency.

Although the rewards of implementing an identity management solution are immense, such initiatives are often very challenging and require the expertise of identity management experts to create and manage teams, gather the requirements, design the system, develop project plans, and oversee the successful implementation and deployment of the system. CIMPs are experts in gathering identity management requirements and design processes while they rely on the highly technical skills of Certified Identity and Security Technologist (CIST) experts for highly technical tasks.

Why pursue a CIMP certification?

Identity management is growing career field which helps businesses streamline, automate, and track user access. By earning the Certified Identity Management Professional (CIMP) designation, members demonstrate their expertise in gathering identity management requirements, designing processes, and managing projects.

Critical Risk Domains™

The following Critical Risk Domains (CRDs) are developed by IMI and define the specific areas used for CIMP training, testing and certification:

1. Identity Management Framework
2. Business Process and System Design
3. Access and Security

4. Audit and Compliance
5. Project Management

1) Identity Management Framework The identity management framework provides a structure intended to serve as a support or guide for the building of an identity management solution which is of utmost value to an organization for identifying individuals in a system and controlling their access to resources based on their roles and associated system access rights. CIMPs must be able to define and interpret an identity management framework which sets the ground rules for developing processes and systems to identify users, store user information, automate and streamline user access with the established access rights information, and track access in the most efficient manner.

2) Business Process and System Design Upon establishment of a framework, business requirements must be gathered to finalize business processes and design the system. CIMPs must be able to interview the appropriate parties to document the current process and propose improvements. They must be able to translate business requirements into technical requirements for the technical staff who are involved with coding, testing and implementation to make sure the system operates in accordance with the business requirements. This understanding must be monitored throughout the project to ensure consistency and alignment.

3) Access and Security As the system is designed, access and security controls must be incorporated to ensure the system access is in accordance with the directory services and access rights. In addition to user provisioning, entitlement management, and access reviews, the system security must be designed to meet the established standards including authentication, identity federation, exception alerts and notification, and single sign-on.

4) Audit and Compliance There are many regulatory requirements related to identity management which certain companies must comply with including user identification and activity tracking. CIMPs must establish continuous audit procedures to ensure than not

only regulatory requirements are being complied with but also systems and processes are operating as designed and follow the established standards. Automated monitoring is essential for detecting unauthorized access, violation of policies, and system malfunctions.

5) Project Management CIMPs must develop, adjust and follow a project pan to achieve their established objectives which may be expressed in terms of output, outcome, benefits, or strategy. As such, CIMPs must be able to apply sound project management principles to provide a greater likelihood of achieving the desired result, ensure efficient use of resources, and satisfy the needs of the project stakeholders. The core components of project management include project justification, requirements, timetable, cost, plan, communication, and monitoring which CIMPs must address as they plan and execute their project plans.

Certification Process

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

Certified Identity Management Professional ™ (CIMP)
Overview & Curriculum