Certified Identity Management Professional® (CIMP)
Overview & Curriculum

Overview

There are many factors contributing to the growing need for technical Certified Identity Management Professionals (CIMP). First, the number of devices and users is growing. These devices are increasingly interconnected and must communicate with one another in order to be authenticated for requesting services and authorized for completing transactions. Thus, adequate IoT and API access controls must be in place.

Second, as businesses leverage cloud computing and storage, SaaS applications, and identity and access management solutions such as multi factor and biometric authentication, CIMPs must be aware of cloud security, Secure SDLC, product implementation, and project management requirements.

Third, with the advancement of technology, CIMPs must be aware of the Machine Learning and Artificial Intelligence possibilities in the identity and access management domain.

Next, 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 assurances that users are properly identified and authorized to access systems and data consistent with their changing roles and responsibilities. In fast paced organizations with a high user turnover rate, identity and access management is even more challenging and important to streamline the identity lifecycle while minimizing security and fraud risks. Therefore, CIMPs must know about the latest threats and how to assess risks, ensure compliance with business and regulatory requirements, as well as emerging IAM trends.

Lastly, 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 improve the identity management process and efficiency. The decentralized and unstructured nature of many identity directory systems has led to an inefficient and sometimes unmanageable user access provisioning, auditing, and reporting, exposing organizations to significant security, reputation, and regulatory compliance risks. CIMPs must be able to propose the best possible IAM architecture for their projects and leverage the industry IAM protocols and standards.

Certified Identity Management Professional® (CIMP)
Overview & Curriculum

Identity Management Solutions

Identity management is a collection of technology, processes and people. In order to address various identity management risks and challenges some of which are described in the above section, organizations are increasingly considering technology solutions to automate identity and access management as much as possible.

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 technical experts in threat assessment, gathering identity management requirements, designing solutions, and implementing systems.

Certified Identity Management Professional® (CIMP)
Overview & Curriculum

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, IMI members demonstrate their expertise in gathering identity management requirements, designing processes, and managing projects.

Who should pursue the CIMP designation?

Certified Identity Management Professional (CIMP) members are technical experts in gathering identity management requirements; designing, developing and implementing systems, and managing various IAM projects.

Some job titles that CIMPs typically hold include:

- IAM System Architect
- IAM System Engineer
- IAM Consultant, Lead, or Analyst
- IAM Access Control Specialist
- IAM Project Director or Manager
- IAM Program Administrator

Certified Identity Management Professional® (CIMP)
Overview & Curriculum

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. Threat Management
2. Project Management
3. Product Selection and Implementation
4. Software Security
5. Cloud Security
6. IAM Architecture, Protocols and Standards
7. IoT and API Security
8. Artificial Intelligence and Machine Learning
9. Compliance Assurance
10. Emerging Trends

1) **Threat Management** - A large part of a CIMPs job is to assess identity and access management (IAM) risks which requires knowledge of threat vectors and sources, threat modeling methods, as well as gap identification and gap remediation process.

2) **Project Management** - CIMPs must be aware of project management best practices and be able to propose a project strategy and roadmap, define business requirements, and have technical writing, communication, negotiation, presentation, and team management skills. Upon establishment of a framework, business requirements must be gathered to finalize business processes and system design. 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. Projects must be monitored throughout the project to ensure consistency and alignment.

3) **Product Selection and Implementation** - When third party IAM software products must be evaluated and selected for implementation, the criteria for how to select an IAM product must be established and used in alignment with business objectives and requirements. System integration and product features must be considered along with the vendor reputation, support and sustainability as well as product certification, independent quality assessments and consumer reviews. CIMPs must be able to select the right product to solve their unique IAM challenges.

4) **Software Security** - When a new IAM product is developed, or features of an existing application are modified, or when an organization must develop an API (Application Programming Interface) for a selected product, many critical areas must be considered such as business requirements and objectives, SDK (Software Development Kit), infrastructure, secure software coding practices including mobile apps, product development framework, OWASP, DevOps segregation of duties, software design and architecture, Service-Oriented Architecture (SOA), system and user acceptance testing, change management, and post implementation tasks.
5) **Cloud Security** - As organizations move their applications and data into global cloud computing environments, CIMPs must be aware of top cloud providers and their IAM capabilities and leverage Cloud Access Security Broker (CASB) to interject and expand enterprise security policies in the cloud.
6) **IAM Architecture, Protocols and Standards** - CIMPs must be familiar with and apply international IAM protocols and standards in their jobs and projects. Formalized international IAM protocols exist to support strong IAM policies. Generally known as “Authentication, Authorization, and Accounting” or AAA,

these identity management protocols provide standards for security to strengthen and simplify access management, aid in compliance, and create a uniform system for handling interactions between users and systems.

7) **IoT and API Security** - As Internet of Things (IoT) devices continue to be deployed by businesses and households with advanced features and data retention capabilities, CIMPs must be aware of the access risks within IoT and their connectivity with other systems and devices to ensure proper identification, authentication, and data integrity.
8) **Artificial Intelligence and Machine Learning** - With knowledge of advances in AI and ML, CIMPs can improve their products and processes through automated machine learning to achieve certain goals quickly and effectively such as when detecting threats and analyzing user behavior.
9) **Compliance Assurance** - There are many regulatory requirements related to identity management which certain companies must comply with including in the area of 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.
10) **Emerging Trends** - As the threat landscape changes constantly, the IAM industry and governments continue to propose new solutions and laws to help mitigate the risks. CIMPs must be aware of the latest IAM risks in order to propose the best solutions. They must be aware of general trends in market solutions such as adaptive MFA, Privileged Access Management (PAM), biometric authentication, and blockchain.

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