Certified Identity Management Professional (CIMP)®
Overview & Curriculum

Overview

The **Certified Identity Management Professional (CIMP)®** program is designed by **Identity Management Institute (IMI)** for information technology, cybersecurity, and technical identity management professionals who design, develop, implement, and manage identity and access management (IAM) systems and solutions.

Demand for Technical IAM Experts

Below are some of the key factors that contribute to the increasing demand for Certified Identity Management Professional (CIMP) experts:

First, as organizations increasingly face sophisticated IAM threats, a detailed understanding of threat modeling and analysis is necessary to counter evolving threats with technical solutions. Becoming a Certified Identity Management Professional (CIMP) requires knowledge of common identity and access management (IAM) risks and the ability to propose technical identity and access management solutions.

Second, as CIMP experts deploy systems and solutions to counter IAM threats, they must be aware of various international standards for ensuring optimum IAM architecture and cloud security by leveraging Secure Software Development Framework (SSDF) and best practices in SDLC, product implementation, and project management.

Third, as the number of IoT devices grows and businesses embrace cloud computing, SaaS applications, and blockchain for decentralized data processing and storage, CIMP experts must ensure adequate API and access controls with advanced systems such as multi-factor and biometric authentication, machine learning, and artificial intelligence.

Last, 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 with adequate KYC and customer identification programs. Meeting the needs for speedy access, KYC for onboarding, system security, and regulatory compliance introduces technical challenges that CIMP experts must address.

Certified Identity Management Professional (CIMP)®
Overview & Curriculum

Why pursue a CIMP certification?

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 improve and 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 technical identity management experts to create and manage project teams, gather the requirements to design and develop systems, help select an external product solution, develop project plans, and oversee the successful implementation and deployment of IAM systems.

In summary, identity management is growing career field which helps businesses streamline, automate, and manage system access. By earning the Certified Identity Management Professional (CIMP) designation, IMI members demonstrate their expertise in gathering identity management requirements, designing systems, and managing IAM projects.

Who should pursue the CIMP designation?

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

Some IAM related titles that CIMPs typically hold include:

- System Architect
- System Engineer
- System Programmer
- Technical Consultant, Lead, or Analyst

- Access Control Specialist
- Project Director or Manager
- Program Administrator

Critical Risk Domains™

The following Critical Risk Domains™ (CRDs) are developed by IMI which organize the study guide chapters used for CIMP training and testing for 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. Digital Identity Guidelines

Critical Risk Domain Summary Descriptions

1) **Threat Management** - A large part of a Certified Identity Management Professional (CIMP) job duties is to manage identity and access management risks which requires knowledge of threat modeling and analysis, gap identification, and IAM solutions. CIMP certification prepares IT professionals to become threat management experts in identity and access management.

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, 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 or SSDF 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 for context-based identity management. Automated monitoring is essential for detecting unauthorized access, violation of policies, and system malfunctions.

9) **Compliance Assurance** - 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.

10) **Digital Identity Guidelines** - These guidelines provide technical requirements for government agencies and organizations implementing digital identity services. The guidelines define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions. These guidelines are based on the US government NIST Special Publication 800-63-3.

Certification Process

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