Certified Identity and Access Manager® (CIAM)
Overview & Curriculum

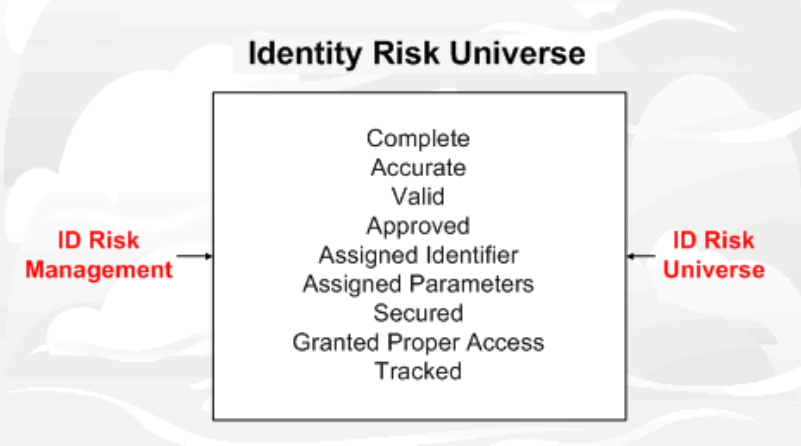
Identity and access management (IAM) is the most important discipline of the information security field. It is the foundation of any information security program and one of the information security management areas which interacts with users the most. IAM defines and enforces which systems users can access and ensures that their identities are properly managed throughout the identity lifecycle from on-boarding, identification, initiation, and authentication, to access provisioning, activity monitoring and termination.

The Certified Identity and Access Manager® (CIAM) designation is a registered program developed for risk conscious professionals who manage identity risks and user access to systems.

CIAMs are capable of managing and transforming an organization's IAM program by establishing a desired objective and continually assessing the organization's existing IAM capabilities through a formal capability assessment model. The continuous reconciliation of the current state to the desired state allows the CIAM® professional to prioritize business investments, close compliance gaps, mitigate risks, and identify process improvements to reduce operating costs. The success of an IAM program is directly tied to the interaction between an organization's people, processes, and technologies.

Identity Lifecycle

Identity management practices throughout an organization strive to ensure that an identity is complete, accurate, valid, approved, readily identified, secured, granted proper logical and physical access, monitored through its lifecycle, and deactivated upon its useful life as listed in the following illustration.



Certified Identity and Access Manager® (CIAM)
Overview & Curriculum

About CIAM®

The Certified Identity and Access Manager® (CIAM) designation is created to independently validate a professional's experience and understanding of identity and access management practices. Many groups and functions within an organization are involved in managing the identities of employees, customers, and business partners. Professionals dealing with internal or external identities as part of their job functions must not only understand the identity and access risks within the boundaries of their daily tasks but must also understand how their individual efforts contribute to the collective efforts of the enterprise for properly managing the identities as well as related access and activities of employees, customers and third parties. As such, the CIAM® program aims to:

1) Increase a candidate's awareness of all evolving identity and access management risks and related solutions including the contributions made by other functions within the company for a collective and effective identity and access management, and

2) Independently validate an individual's understanding and experience for managing identity and access risks.

The Challenge

Although technology is an important part of identity and access management, technology alone can not solve today's identity and access management challenges. Adopted solutions in the past have often focused on just technologies which were poorly designed and implemented resulting in high costs and limited value. Organizations often struggled to meet compliance demands, and the solutions were deployed to manage limited number of systems.

As companies become more aware of identity an access management risks, compliance requirements, emerging threats such as cyber crime facing their organizations, new technologies, and the benefits of an effective IAM program, the highly needed skills of Certified Identity and Access Manager professionals are recognized for countering threats and managing risks.

The following are several areas and business risks which demand companies to embrace IAM programs, skilled professionals, and technologies:

- Mobile Computing

- Cloud Computing
- Connected Devices
- Social Media
- Big Data
- Data Loss and Theft
- Privacy
- Regulations
- Identity Theft
- Cyber Crime & Terrorism

Regulatory Compliance

From a regulatory compliance standpoint, there are many overlapping laws pertaining to customer identification, privacy, and fraud prevention that companies must manage as effectively and efficiently as possible. For example, companies are required to establish a formal Customer Identification Program (CIP), monitor account activities, ensure the security of private information, authorize data access, report suspicious activities, and prevent identity fraud.

Although, identity and access management is critical for protecting consumer information and complying with privacy and other regulations, IAM is evolving beyond compliance to become a risk-based function that can help an organization achieve competitive advantage through lower access costs, increased efficiency, and reduced risk of security breaches.

Critical Risk Domains Summary

The CIAM Critical Risk Domains (CRD) define the knowledge and experience areas that a professional must possess in order to effectively manage the identity and access risks for his or her assigned area of responsibility and also understand how others within the company contribute to the identity and access risk management efforts of the enterprise. As such, a CIAM needs to possess a general knowledge in all CRDs, however, is not expected to possess hands on experience in all CRDs as some identity and access management practices are distributed across the enterprise and may require specialized skills in some cases.

The following are the Critical Risk Domains used for CIAM training, testing, and certification:

Certified Identity and Access Manager® (CIAM)
Overview & Curriculum

1. Strategy and Governance
2. Program Management
3. Lifecycle and Transformation
4. Access Request and Approval
5. Provisioning and De-Provisioning
6. Enforcement
7. Auditing and Reporting
8. Access Review and Certification
9. Account Reconciliation
10. Tools

Critical Risk Domains Description

1) *Strategy and Governance:* Identity governance aligns the IAM program with both business objectives of the enterprise and identified risks facing the organization in the most efficient manner. When activities which can be centralized or automated remain distributed, they often lead to additional and unnecessary costs. It is also important to engage system and data users through education and training about the policies to actively seek their support for the identity governance objectives as well as the IAM program to ensure maximum efficiency and effectiveness in the identity management lifecycle.

   As companies develop a strategy and plan for their identity and access management, they should define a desired state and assess their current state using a capability assessment model to ensure improvement of the current state to address risks, regulatory requirements, automation, efficiency, metrics, and reporting.

2) *Program Management:* The IAM program should consist of all the elements required to assess, improve, and manage IAM in line with company's governance and strategic plans. The program defines ownership for various tasks, stakeholders, project management teams, processes, tools, reporting, etc. The program also incorporates processes to facilitate the interaction between people, processes, and technology which is necessary to make the program successful.

3) *Lifecycle and Transformation:* The identity and access management lifecycle consists of access request and approval, provisioning and de-provisioning, enforcement, auditing and reporting, access review and certification, and account reconciliation. IAM transformation relates to the assessment and improvement of current capabilities to meet the desired identity and access management objectives for managing risks and

meeting compliance needs efficiently and cost effectively while leveraging IAM tools as necessary.

4) *Access Request and Approval:* The first phase in the identity and access management lifecycle is the access request and approval processes which must be managed as centrally as possible with adherence to SLAs and compliance requirements. Business roles are used to not only define appropriate access profiles and rights which align with the job functions but also to increase users' and approvers' understanding of the requested access to reduce the risk of excessive access. A self-service functionality may be considered in this phase to make the access request process more efficient.

5) *Provisioning and De-Provisioning:* Companies may deploy automated provisioning solutions to enforce consistency and segregation of duties, and eliminate the formal request process for certain basic access to increase productivity. Companies must also improve the de-provisioning process to expedite the access removal process upon termination or role change to reduce the retention period of inappropriate access.

6) *Enforcement:* This phase of the IAM lifecycle includes a review of privileged access logs, analysis of segregation of duties, and improvement of password controls.

7) *Auditing and Reporting:* Audit, analytics, monitoring and reporting are key components for improving identity and access management programs. CIAMs must define their audit plans based on risks and produce remediation plans and metrics to report on performance based on established criteria. The audit and reporting efforts must be aligned with the business objectives for identity and access risk management, compliance, and improvement.

8) *Access Review and Certification:* To review and certify access, CIAMs must design a plan to identify target systems and data, determine review strategy and tools, identify review staff, establish a review and reporting frequency, and propose mitigation plans. A centralized and automated access review process can be considered to eliminate redundancy and lengthy processes. A risk-based review cycle must be considered to reduce the review efforts while reaching the established access certification and compliance goals. Focus must be placed on the most critical systems, roles, and data.

9) *Account Reconciliation:* This phase can be automated through IAM tools. It consists of ensuring that actual system access for any identity is consistent with the original approved access request.

10) Tools: As companies evolve their IAM programs and seek to achieve higher levels of maturity in their IAM lifecycle, they will deploy commercially available products to streamline their processes, automate the IAM processes as much as possible, and improve review, assessment, and reporting capabilities. CIAMs must be familiar at a high level with the latest market solutions and their features.

Certification Process

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