



## **Certified Identity Risk Manager™ (CIRM) Overview & Curriculum**

Identity management is a critical component of many functions within an organization and thus is a distributed process. In particular, sound identity management practices are even more important in organizations where 1) critical business information assets exist and must be accessed and protected, 2) consumer personal information are collected as part of the business process and must be protected, 3) employee and third party identities and access must be managed and 4) customer identities must be validated in member based organizations such as social networking companies to ensure appropriateness, completeness and accuracy of member information. As such, distributed identity management practices are not solely established for information protection purposes and are interdependent for a full cycle identity management. Identity management practices throughout an organization strive to ensure 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.

The Certified Identity Risk Manager™ (CIRM) designation is created to independently validate a professional's experience and understanding of identity risks and best management practices. Many groups and functions within a business environment are involved in managing the identities of employees, customers, and business partners. Professionals working within a business function with some involvement in managing internal or external identities must not only understand the identity risks within the boundaries of their job functions but must also understand how their individual efforts contribute to the collective efforts of the enterprise for properly managing the identities of employees, customers and third parties. As such, the CIRM program aims to:

- 1) Increase a candidate's awareness of all evolving identity risks and related solutions within the boundaries of his or her job function, and, understanding of contributions made by other functions within the company for a complete and collective identity management risk coverage, and
- 2) Independently validate an individual's understanding and experience for managing identity risks.

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

Copyright by Identity Management Institute

All Rights Reserved

Page 1 of 4



## Certified Identity Risk Manager™ (CIRM) Overview & Curriculum

the enterprise and may require technical skills in many areas. For example, although many groups may be involved with common identity management practices such as operations security for maintaining privacy throughout the identity life cycle, below are some examples of departments involved in specific identity management practices within the boundaries of their functions:

**Human Resources & Payroll** - ensures the completeness and accuracy of an employee's identity at the time of hiring, assigns an employee number upon approval for tracking, and pays salaries to valid employees,

**Information Technology** - assigns and manages system access based on access provisioning processes including access approval, monitoring and deactivation. Also, ensures system security and implements technologies to streamline and automate the identity management practices,

**Information Security & Privacy** – ensures coherent protection of confidential business, customer and employee information from unauthorized changes and disclosure with proper oversight and policies,

**Investigations** - follows-up on discovered incidents to validate and resolve potential identity theft and fraud cases,

**Customer Service** - validates a customer identity before completing a transaction or sharing private customer information,

**Compliance & Legal** - in collaboration with other groups ensures regulatory requirements for protecting customer information are met,

**Physical Security** - ensures access to buildings, facilities and areas containing sensitive information is limited to the appropriate individuals and monitored to detect unauthorized access attempts including piggybacking,

**Internal Audit** - ensures all relevant internal controls are adequately designed and operating as intended through reviews of policies, procedures and standards as well as tests of controls,

**Risk Management** - through monitoring, escalation and coordination with management, helps determine a course of action for managing enterprise risks,

**Customer Relations** - acts as the main communication channel between the company and its customers regarding all matters of concern to customers such as identity breach incidents, and

**Operations** - ensures protection of confidential information outside of information systems and validates the identities of customers in some member based organizations ensuring completeness and accuracy of member information.



## **Certified Identity Risk Manager™ (CIRM) Overview & Curriculum**

The following are the Critical Risk Domains used for CIRM training and testing:

1. GOVERNANCE & MANAGEMENT
2. INTERNAL CONTROLS
3. TECHNOLOGY MANAGEMENT
4. AWARENESS & TRAINING
5. ACCESS MANAGEMENT
6. RISK ASSESSMENT
7. COMPLIANCE
8. AUDITING & MONITORING
9. COMMUNICATION
10. INCIDENT MANAGEMENT

- 1) *Governance and Management:* The critical components of a comprehensive identity risk governance and management program include identity management policies and procedures, assigned priority, resources as well as awareness and training.
- 2) *Internal Controls:* Risk assessments are performed at the functional levels to identify the identity risks to the enterprise for the assigned function, and, ensure the internal controls are designed, implemented and operating effectively to mitigate the risks.
- 3) *Technology Management:* Identity management technologies might be considered and implemented to automate and improve the access management and identity validation processes for internal and external parties.
- 4) *Awareness & Training:* The identity risk mitigation process requires the risk awareness and involvement of all parties including employees, customers and third parties such as vendors who have access to confidential information. As such, a comprehensive education program is necessary to increase risk awareness and comply with laws.
- 5) *Access Management:* Access to buildings, facilities, computer systems and information must be provided based on appropriate approval and minimum access rules to ensure data integrity and confidentiality.
- 6) *Risk Assessment:* New threats and solutions are constantly introduced. A periodic risk assessment allows for identification of risks whereby threats are not countered with the proper controls, hence, allowing management to make sound risk management decisions on a timely basis.
- 7) *Compliance:* Any business which operates within a regulated industry such as healthcare, insurance and financial services must implement programs to comply



## **Certified Identity Risk Manager™ (CIRM) Overview & Curriculum**

- with all applicable State and Federal privacy and security laws such as HIPAA, Red Flags, and GLBA.
- 8) *Auditing & Monitoring*: Auditing is an extension of the risk management process whereby internal controls are assessed for completeness and effectiveness. Monitoring is also a critical component for detecting unauthorized access or transactions. Auditing and monitoring processes may be distributed in certain organizations to properly validate, approve and track identities.
  - 9) *Communication*: All identified risks, decisions and resolutions must be documented and communicated timely to the appropriate parties.
  - 10) *Incident Management*: When incidents related to inappropriate access and identity fraud are introduced, either through monitoring or a reporting process, incidents must be followed up in due time to validate the incident, assess the risk level, remediate the issue, and formally communicate the conclusion of the investigation.