Certified Identity and Security Technologist ™ (CIST)
Overview & Curriculum

Overview

Identity management and security technologies are increasingly needed to address the growing needs of businesses to counter threats, meet requirements, and mitigate risks. According to recent studies, there will be a serious shortage of information security professionals with highly technical capabilities within just a few years which is required to develop, deploy, and manage these systems.

The increased need for identity management and information security technologists arises from the needs of many parties. Businesses are connecting more systems to communicate with one another, consumers are demanding easy access to data and transactions without having to remember multiple passwords, companies want more security, improved identity services, useful information about their customers, and regulators want accurate and timely identification of individuals, privacy, and transaction tracking and reporting to name a few. The rise in high profile attacks by highly technical cyber hackers which result in stolen business and consumer private data has led to increased pressures on businesses to take action and while businesses need to address these risks, they have access to many technologies to mitigate risks in the most cost effective, efficient, and effective manner. However, to be successful, Certified Identity and Security Technologist™ (CIST) professionals are needed to counter hacker threats and help develop or improve, select, deploy, and manage various identity and security products.

The following is a list of additional drivers for the increasing use of identity and security technologies:

1. Increased number of mobile devices,
2. Multitude of IAM and security products in a competitive market,
3. Interconnectivity and interoperability of devices,

4. Secure communication,
5. Increased technical capability of hacker attacks,
6. Need for better identity services such as biometric authentication,
7. Secure data and efficient operations,
8. Expanding regulations requiring improved customer identification, account activity reporting, ID theft prevention, and privacy,
9. Adoption of cloud computing, BYOD, and remote access, and
10. Global nature of employees, customers, and business partners.

Why pursue a CIST certification?

CIST professionals are highly technical leaders who understand the alignment of IT strategy with business requirements. They deploy and manage identity and security technologies to address various business risks and meet increasing challenges around system security, device communication, access, and identity management. While some CISTs are engaged in highly visible enterprise wide implementations of identity and security systems, other CISTs are engaged in the early product development or product improvement activities. The CIST technical program is a specialized identity management and IT security certification and CIST professionals are specialized technology leaders in system security, identity and access management.

Who employs CIST professionals?

CIST professionals may be employed by IT service providers, banking and financial services, government agencies, as well as insurance and healthcare companies. There are many reasons why companies need to engage identity and security technologists. They include efficient operations, system and data security, identity management, device connectivity, system communication, and compliance.

Critical Risk Domains™

Certified Identity and Security Technologist ™ (CIST)
Overview & Curriculum

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

1. Strategy and Analysis
2. Planning and Design
3. Transition and Implementation
4. Communication
5. Leadership

1) Strategy and Analysis CIST professionals must understand the threats facing their business or client organizations as well as their adopted policies, standards, frameworks, regulatory requirements, infrastructure design, management's risk and budget appetite, and market products. They must be able to assess and improve the existing control posture and recommend, plan and implement technical measures to manage the identity and security objectives. They must take an inventory of assets including existing tools and resources, perform risk analysis of existing operations to identify threats, and propose solutions to reduce risks. CISTs must be able to identify potential solutions and select the best technological path forward for the organization. They must build the identity management and security technology vision and engage partners to design high-level solutions and prepare technology plans. They are able to research new technologies and their applicability to business needs. CISTs prototype and perform research to support technology related decisions throughout the organization. CISTs must have knowledge of latest market trends, SDLC frameworks, as well as read and interpret technical reports. They must be able to understand system functionality through vendor demos or technical documents.

2) Planning and Design CISTs are expected to stay up-to-date on the latest intelligence, including hackers' methodologies, in order to anticipate security breaches. They also are responsible for preventing data loss and service interruptions by researching new technologies that will effectively protect networks and systems. They assess current products and services to ensure they align with business standards, industry guidelines and best practices. They evaluate and identify technology implications and perform

architecture reviews prior to product selection and rollout. They design, develop and implement security and identity management solutions by assessing risks, and develop remediation plans as gaps are identified.

3) Transition and Implementation CISTs must be well versed in project management, resource allocation, and personnel management to develop project plans and list milestones. They are capable of successful implementation of various identity management and security systems such as firewalls, IDS/IPS, data encryption, directory services, IAM, and other systems. They engage with their business and IT counterparts to make sure the implemented technology is properly tested and meets business. They must be able to design a security architecture, configure systems, and apply patches as necessary. They monitor system performance after implementation as well as changes in the market for improved and new functionalities.

4) Communication CISTs are able to translate technology concepts into non-technical language to project stakeholders. They bring key issues to the attention of stakeholders at each phase of the project (design, programming, implementation). They report progress, recommend security enhancements, and implement requirements. They train staff on identity and security management related systems and procedures. CISTs work closely with all parties to integrate identity directory services, as well as identification, authentication, authorization, security, and compliance requirements into all products. Interpersonal skills are also necessary to seek collaboration by other parties. Useful system reports must be designed and distributed as necessary to the appropriate parties. They must be able to provide advice to both technical and non technical people and be able to read and understand various documents such as audit reports, and technical specs.

5) Leadership. As technology advocates, CISTs are able to present vision and inspire enthusiasm for the technology and what it can do for the organization. They prepare presentations to key audiences, and provide specific documentation related to solutions (services, costs and staffing). They are able to look at emerging technology trends and apply them to target areas. Acting as highly technical leaders, CISTs provide consulting to all stakeholders, and follow product evolution in the marketplace. They provide

technical expertise in defining and maintaining the architectural frameworks, standards, guidelines, processes related to products/services, and business or data architecture. While they work on multiple technical initiatives, CISTs serve as the ultimate identity and security technology leaders for their clients or businesses and advisor to key business stakeholders. CISTs build trust and relationships through collaborative efforts and understand and leverage market products as well as those deployed in the company to solve security and identity management challenges with technology.

Certification Process

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