IDENTITY MANAGEMENT INSTITUTE
Center for Identity Governance

Certified Identity Governance Expert® (CIGE)
Overview & Curriculum

Overview

Identity and Access Governance (IAG) provides the link between Identity and Access Management (IAM) rules and the policies within a company to protect systems and data from unauthorized access, streamline processes, reduce risk, and ensure compliance with the appropriate requirements.

Threats and Risks

Between the development of new technologies and a growing reliance on the insights offered by big data, enterprise security is becoming more complex every day. Employees use a variety of devices to access data from diverse locations, and the Internet of Things (IoT) is creating webs of connectivity with unprecedented scope. The adoption of Artificial Intelligence (AI) and machine learning further complicates security, giving rise to the need for detailed programs addressing Identity and Access Management.

Access to data, systems and devices requires the protection provided by a comprehensive combination of IAG and IAM policies and procedures. As companies continue to adapt to changing technologies and look forward to what may come in the future, it's essential for organizations to prepare for the inevitable security challenges.

Identity Governance Expertise

The Certified Identity Governance Expert (CIGE)® professional designation is the first and leading registered identity governance certification designed to promote a lifecycle framework for the authority of the identity management field and related functions. Executives and corporate officers who set the rules for identity and access management within organizations can benefit by becoming a Certified Identity Governance Expert®. The CIGE designation demonstrates the knowledge and skills of the IMI members who hold the designation which is awarded to qualified professionals who set the rules at the highest levels of their organizations for addressing the growing societal and organizational concerns regarding privacy, security, customer expectations, identification and authentication, as well as regulatory and contractual compliance, and efficient IT and access management processes to name a few.

CIGE Benefits

Learning to assess risks and apply the proper identity and access governance rules gives certified professionals the knowledge and control they need to manage data security at the enterprise level. Certified Identity Governance Expert® (CIGE) professionals are capable of defining and effectively communicating why identity governance is critical for their organizations. They understand good governance benefits and can see the big picture as well as the evolving identity risk landscape. They are also capable of proposing and implementing an identity governance lifecycle framework which helps their organizations meet the established identity management objectives.

Critical Risk Domains™

The following Critical Risk Domains (CRDs) define the specific knowledge areas and skills that CIGE professionals need to become certified:

1. Governance
2. Identity and Access Management Lifecycle
3. Strategy, Roadmap, Framework, and Planning
4. Roles, Responsibilities, and Accountability
5. Program, Policies, and Procedures
6. Risk Management and Internal Controls
7. Funding, Resource Allocation, and ROI
8. Independent Audits, Monitoring, and, Performance Measurement
9. Compliance
10. Technology

The following are detailed sections to describe each Critical Risk Domain used to develop the CIGE study guide and testing:

1. Governance

Identity and Access Governance is the centralized oversight of user identity management and access controls based on established policies. In clearer terms, it may be described as “the establishment and management of policies, processes and accountabilities” to create roles and entitlements related to information access and manage access approvals and requests.

Identity and Access Governance helps to standardize enterprise identity information and works together with IAM to create a comprehensive framework for mitigating risks while allowing companies to achieve their objectives with a minimal amount of hindrance.

Governance tends to be overlooked when businesses seek to implement IAM programs, leading to confusion, poor access control, difficulty enforcing policies and the accumulation of bad data.

The primary purpose of IAG is managing risks and ensuring compliance in a consistent, efficient and effective manner. Governance goes beyond basic compliance and access control to provide a method for overseeing and implementing the tactical aspects of IAM including:

- Establishing user identity
- Authenticating users
- Controlling access to information, data and applications
- Monitoring and auditing user activities

Managing enterprise-level risk

Many platforms and tools are available to handle large bases of users and the massive amounts of data they create so that companies don't become overwhelmed with the task of establishing and executing access governance programs. With these tools, you can more easily manage data availability, maintain the integrity and confidentiality of information and comply with privacy laws.

Governance Body

Because of the amount of data generated and accessed at the enterprise level, a successful IAG program requires a governing body made up of skilled individuals from various parts of the company. These individuals work to:

- Define policies relating to access control
- Offer feedback on the success or failure of current policies
- Oversee the implementation and execution of policies
- Reinforce policies among users

These core members are known as “policy stakeholders” and are responsible for the continued health and success of the identity governance program. Supporting members include those who have the most contact with the users accessing data on a daily basis, and it’s their job to educate these people regarding policies and keep them informed about proposed changes. This supervisory role ensures the clarity of policies is maintained when passed down from the committee to individual team members within the company.

A typical governance body may include:

- Auditors
- Business managers
- Compliance officers
- IAM analysts
- IT staff
- Resource owners

Core members should meet regularly to address policy questions, discuss challenges and propose any necessary changes.

2. Identity and Access Management Lifecycle

Each set of permissions within an IAM program has a lifecycle starting with the moment a new user enters the system. This may be during an onboarding process before the first official day on the job, or you may choose to phase employees in as they become comfortable with company policies and systems during their first few weeks. From here, the lifecycle goes through a series of continuous steps:

- Provisioning
- Enforcement of policies and identities
- Auditing of activities
- Review and certification of user actions

Reconciliation of bad data

When a user leaves the company, their identity must be removed through a deprovisioning process to ensure no unauthorized access takes place in the future. Deprovisioning, making new provisions, and adjusting the level of access are also necessary when a team member changes roles within the company.

3. Roles, Responsibilities, and Accountability

Clarity is also necessary when defining the permissions granted to various users within the company. IAG policies direct the reinforcement of responsibilities in each role and hold users accountable for their actions. Everyone with access to data must be educated about these policies to maximize efficiency in identity management.

To clarify roles, it’s necessary to:

- Identify the permissions required for users to do their jobs effectively
- Consider roles requiring multiple permissions
- Create basic roles defined by how people currently access or will need to access data
- Set up a model for easily creating new roles based on those already in place
- Focus on specificity in role reinforcement, including the resources used to fulfill individual data access requests

Data owners, business managers, IT and HR staff, the legal department and the governance body for the IAG program are all responsible and accountable for how permissions for roles are granted and reinforced. Policies must be stated in clear language so that users at every level understand what permissions are granted to them and why. Without such a comprehensive understanding of provisioning and permissions, bottlenecks are created when information requests are received and productivity can be slowed considerably.

4. Strategy, Roadmap, Framework, and Planning

The path to successful IAM and IAG strategies starts with an evaluation of where your company's security currently stands. Get your team together and start by assessing risk.

Consider several points in your assessment:

- The level of risk represented by the amount and types of data you collect and analyze each day
- What security measures you already have in place
- Known and suspected weak areas relating to data safety and integrity
- Risks posed by new technologies being implemented
- Necessary upgrades or fixes for existing security measures
- How or if you're monitoring access
- Tools needed to improve oversight in asset access and use

By classifying your data into distinct categories and identifying the greatest sources of risk, you get a clear picture of what areas your identity access program needs to address. If you haven't already established policies, it's likely your current IT tools don't have the features necessary to ensure the enforcement of the proper policies, procedures and guidelines. In some cases, professional certifications in identity and access management may be needed to prepare your team to handle the challenges of IAM and IAG.

As you lay out your plans for identity and access management and governance, envision IAG as a framework to "wrap around" and control your IAM policies. This gives you a roadmap for the scope and direction of the project, preventing it from going off course and losing touch with your company's objectives. Scalability is an important consideration, but it must be addressed in a practical way so that you remain in control of when and how new aspects of the program are introduced and implemented.

5. Program, Policies, and Procedures

Identity and Access Management Program

An IAM program consists of the actual tactics used to ensure appropriate access “across various systems of an organization.” Whereas IAG deals with accountability and provides oversight to ensure that risks are adequately mitigated, IAM focuses on ensuring that controls are implemented to mitigate risks through policies and procedures. IAM provides the basic framework necessary to make the right information available to the right people at the right time and prevent unauthorized access with the potential to undermine systems. This is especially important when dealing with proprietary information within your business and has become critical in the age of IoT technology.

Many companies make the mistake of creating an IAM program without addressing Identity and Access Governance. However, the two work together to support and reinforce each other. Access management strategies operate within the framework of IAG, which defines:

- Program objectives
- Essential areas of compliance
- How changes are handled
- How problems are addressed

Program updates in response to policy changes

Based on these principles, you can establish IAM rules to regulate access for all users within your company. IAM directs the creation of individual user identities and guides authentication processes across platforms and devices. Identity management also falls under the umbrella of IAM, including the assignment of privileges at various levels and rules guiding user verification when information requests are made. As enterprises expand into the global market, strong IAM programs will become even more important to prevent security breaches in all industries.

Policies and Procedures

Successful governance of identities and access depends on clear policies and the enforcement of procedures at every level in an enterprise. During your initial risk assessment, you'll discover the key processes, systems and data to be considered and gain an understanding of the number and types of users requiring various levels of access.

To grant this access, you'll need an IT platform designed for IAM and IAG and made to enforce guidelines in the interest of managing data security. Such programs should also include tools to document users' actions and behaviors, thereby ensuring accountability at all levels.

Work with company stakeholders when establishing policies, giving everyone a chance to voice their concerns about issues relating to data security. Identify key metrics to track and make the review of these metrics part of your standard IAG procedures. Tracking and analyzing users as they request and gain access to data gives you a better understanding of how different access levels affect risk and provides a continual source of information from which you can draw when reviewing and updating policies in the future.

Clarity in policies and procedures ensures the proper implementation of access governance and management processes. Everyone stays in the loop regarding the state of data security, and the whole system operates without the constant need for human intervention to correct problems or respond to emergency situations.

You IAM policy should address:

- The creation of clear roles and duties for each user, known as user provisioning
- Compliance enforcement
- Audit practices and policies
- Intelligence

6. Risk Management and Internal Controls

A thorough assessment of risk should be part of your original IAG planning. Understanding the risks involved with every type of permission makes it possible to implement policies and controls to minimize vulnerabilities. Controls include the tools and processes involved in the IAM lifecycle and may also make use of:

- Multi-factor authentication
- Multiple authorization levels
- Access control based on users' roles
- Access control based on specific rules to prevent risky access

Separation of Duties (SoD) policies are also essential to eliminate the problem of incompatible permissions. Because some roles require multiple provisions for access, it's possible to have a situation in which a conflict of interest or the potential for unethical practices arises. SoD protects against fraud, abuse and other risks associated with these conflicts.

Combining automated systems with robust tracking programs provides a platform through which the IAG governance body and those with the ability to approve access can monitor users' actions and manage permissions as necessary to increase efficiency and cut down on risk.

7. Funding, Resource Allocation, and ROI

Any worthwhile security policy requires some level of investment. New technology and tools, identity management certifications and recruitment of new team members must all be taken into account. Gauge the cost of every step, working out how much time and how many resources are necessary to get your IAM program and IAG in place. Consider:

- If your current team is adequate to handle the intricacies of management and governance
- The amount of education and training necessary to bring existing team members up to speed and onboard any new hires
- How many steps in the identity management process can be automated to save time and money
- The total amount of potential savings realized through automation and streamlining
- The potential increase in productivity when audits are automated, roles are well-defined and permissions are clear
- How much your IAM and IAG programs will improve the speed and consistency of information access

These same considerations may be applied when calculating the potential ROI of identity management and monitoring the ongoing success of your programs. For IAG, returns are defined in large part by how well you're meeting your goals for risk reduction. Less risk means less time and money spent mitigating the issues faced in the aftermath of a data breach and helps to ensure the integrity of your brand in the market. Continue to monitor the performance of your IAG system over time, and pay attention to how your risk rating changes as policies are implemented and updated.

8. Independent Audits, Monitoring, and Performance Measurement

Auditing, analytics, monitoring and reporting are key components for improving identity and access management programs. Using a single tool to handle all components provides the clearest, most comprehensive feedback on how well your management and governance strategies are working. Choose a platform with the ability to record as much pertinent information as possible, logging the activities of all users as they interact with the system.

Although the way companies analyze this information differs slightly based on the objectives of individual IAM and IAG efforts, all enterprises can benefit from analyzing certain common metrics:

- Monthly password reset volume
- The number of accounts held by each user
- The number of new accounts put in place in a given period of time
- Accounts without owners, often not deprovisioned after the departure of team members
- How quickly provisioning and deprovisioning can be performed
- The amount of time required to authorize changes
- How many exceptions are made as users' actions are authenticated, reconciled and re-certified

Relating these metrics to specific risks reveals where improvements are necessary, how much bad data is being generated and where you continue to deal with any major points of vulnerability. Thanks to advanced big data analytics tools, you can conduct audits and retrieve reports without spending the majority of your time trying to make sense of information relating to users' actions. Instead, you get the clarity you need regarding system access and user provisioning, making it possible to respond quickly and implement adjustments to prevent data theft or loss.

9. Compliance

The rules and regulations with which your company needs to remain in compliance depend on the industry in which you operate. For example, some organizations are required to comply with privacy laws, and others are subject to customer identification and monitoring, employement, and identity theft prevention laws.

Only about 20 percent of organizations are fully compliant with the rules and regulations for their industries. Common challenges include:

- Lack of clarity in users' roles
- Users being granted too many access rights
- Allowing developers the freedom to make excessive changes
- Failure to deprovision identities
- Excessive orphan and privileged accounts

Noncompliance carries a number of potential penalties, including costly fines and a loss of the trust customers and clients once placed in your brand. Make sure your team is familiar with all current domestic and international regulations. Know how you're expected to handle information and keep data safe, and work with the IAG team to establish and maintain policies supporting consistent compliance.

10.Technology

As you refine the components of your IAM program, you'll need stronger, more intelligent tools for tracking, assessment and reporting. Commercially available technology products make it possible to balance IAM and IAG in modern enterprises. By employing software to handle the complexities of access management and identity governance, you reduce risk, improve security, minimize the time necessary for users to obtain information and have access to a number of options for automating common processes.

To find best solution for your company among the many IAM platforms available, determine:

- The services, processes and reporting tools offered
- The quality of customer service and support
- Security measures used by the provider
- Compatibility with current systems
- Time and steps necessary for proper implementation
- Long-term scalability
- Ease of establishing and managing roles
- Types of authentication used
- Ability to support and manage the entire IAM lifecycle
- Education necessary to onboard all team members
- Management tools for multiple device types
- Flexibility to incorporate future technologies

The best IAM and IAG technology supports your identity and access management policies and helps your company stay on target with its objectives. Any platform lacking the tools you need to improve efficiency and maintain security should be passed over in favor of a better option.

Robust security incorporating IAM and IAG is essential for modern companies. When you have both in place, IAG serves to check and balance IAM, providing policies through which you can control access, monitor actions and make changes as necessary. Investing in the proper technology ensures you have the right auditing and reporting tools to clean up bad data and prevent unauthorized access. With every step of the lifecycle covered, it’s easier to assign roles, manage permissions and close down access in response to growth and change within your team.

Sixty-six percent of board members lack confidence in the ability of their companies to launch a proper defense in the event of a cyberattack, but establishing clear roles and carrying out regular audits helps your company minimize the risk of breaches and prevent data loss associated with poor access control. Plan today for stronger, more secure access in the face of rapidly changing technology. Educate your team, allocate resources properly to handle the challenges of IAM and IAG and enjoy better security at every level within your enterprise.

Certification Process

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