Strategic Identity and Access Management Implementation Training Course



16 - 20 Nov 2026

Sharm El-Sheikh

4100 € (Per Person)

Ref: #CYB9742_272453

Course Introduction / Overview:

This comprehensive training course provides a deep dive into the strategic implementation of Identity and Access Management (IAM) systems, transforming them from a purely technical security function into a core business enabler. In today's digital landscape, managing who has access to what, when, and why is paramount for security, compliance, and operational efficiency. This program moves beyond basic concepts to equip participants with the knowledge to design, build, and manage a robust IAM framework that aligns with organizational goals. As discussed by authors like Graham Williamson in works such as "Identity Management: A Primer," a successful IAM strategy is a journey, not a destination. This course, offered by BIG BEN Training Center, guides you through every step of that journey. We will explore the entire lifecycle, from initial assessment and roadmap development to selecting appropriate technologies like SSO and MFA, implementing privileged access management (PAM), and establishing strong governance and compliance protocols. Participants will learn to navigate the complexities of modern identity challenges, including cloud environments, remote workforces, and stringent regulatory demands, ensuring their organization's digital assets are secure and accessible to the right people at the right time.

Target Audience / This training course is suitable for:

- IT Security Managers and Professionals.
- Identity and Access Management Specialists.
- System and Network Administrators.
- Information Security Analysts.
- IT Auditors and Compliance Officers.
- Enterprise Architects.
- IT Project Managers responsible for security initiatives.
- Chief Information Security Officers (CISOs).

Target Sectors and Industries:

- Banking and Financial Services.
- Healthcare and Pharmaceuticals.
- Government and Public Sector Agencies.
- Telecommunications and Technology.
- Retail and E-commerce.
- Energy and Utilities.
- Education and Research Institutions.
- Consulting and Professional Services.

Target Organizations Departments:

- Information Technology (IT) and Infrastructure.
- Cybersecurity and Information Security.
- Internal Audit and Risk Management.
- Compliance and Legal Departments.
- Human Resources (for employee lifecycle management).
- Application Development and DevOps.
- Business Operations and Strategy.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop a comprehensive IAM strategy and roadmap aligned with business objectives.
- Design and architect a scalable and secure IAM framework.
- Evaluate and select appropriate IAM technologies and solutions.
- Implement Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) models.
- Master the principles and deployment of Single Sign-On (SSO) and Multi-Factor Authentication (MFA).
- Establish a robust Privileged Access Management (PAM) program.
- Integrate IAM with cloud services and hybrid environments.
- Manage the full user identity lifecycle from onboarding to offboarding.
- Conduct access certification campaigns and periodic reviews.
- Ensure IAM systems comply with regulations like GDPR, HIPAA, and SOX.
- Develop metrics and KPIs to measure the effectiveness of the IAM program.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, practical, and engaging, ensuring participants can apply the learned concepts directly to their work environments. We believe that strategic IAM knowledge is best acquired through a blend of expert instruction and hands-on application. The course will feature in-depth presentations on core IAM principles, architectural patterns, and governance frameworks. These sessions are complemented by real-world case studies that analyze both successful and failed IAM implementations, providing valuable lessons on common pitfalls and best practices. Participants will engage in collaborative group workshops to design sample access control policies, develop an IAM project plan, and debate solutions to complex identity scenarios. Interactive Q&A sessions and expert-led discussions encourage critical thinking and knowledge sharing among peers. The focus is not just on theoretical understanding but on building the practical skills needed to lead and execute strategic IAM initiatives within any organization, fostering a dynamic and effective learning experience.

Course Agenda (Course Units):

Unit One: Foundations of Strategic Identity and Access Management

- Introduction to Identity and Access Management (IAM).
- The business case for IAM: moving from a cost center to a value driver.
- Core principles: authentication, authorization, and auditing.
- Understanding key IAM terminology and concepts.
- Aligning IAM strategy with business goals and digital transformation.
- Identifying key stakeholders and establishing a steering committee.
- Conducting an initial IAM maturity assessment.

Unit Two: Designing and Architecting the IAM Framework

- Key components of a modern IAM architecture.
- Comparing access control models: RBAC, ABAC, and PBAC.
- Designing effective roles and entitlement catalogs.
- Architecting for scalability, resilience, and security.
- Introduction to Identity Governance and Administration (IGA).
- Principles of Privileged Access Management (PAM).
- Integrating IAM with on-premises and cloud environments (Hybrid IAM).

Unit Three: Implementing Core IAM Technologies and Solutions

- Deep dive into Single Sign-On (SSO) and federation protocols (SAML, OAuth, OIDC).
- Implementing Multi-Factor Authentication (MFA) and adaptive authentication.
- User lifecycle management: automating onboarding, transfers, and offboarding.
- Solutions for password management and self-service capabilities.
- Selecting the right IAM vendor and solution.
- Managing a successful IAM implementation project.
- Best practices for API security and access management.

Unit Four: IAM Governance, Risk Management, and Compliance

- Developing and enforcing IAM policies and standards.
- The role of IAM in achieving regulatory compliance (GDPR, SOX, HIPAA).
- Designing and executing access certification and recertification campaigns.
- Auditing and monitoring access to critical systems.
- IAM risk assessment and mitigation strategies.
- Managing segregation of duties (SoD) conflicts.
- Reporting, analytics, and creating an IAM dashboard with key metrics.

Unit Five: Advanced IAM, Program Management, and Future Trends

- Implementing a Zero Trust security model.
- The rise of passwordless authentication.
- Customer Identity and Access Management (CIAM) strategies.
- The future of identity: decentralized identity and blockchain.
- Managing and maturing the IAM program post-implementation.
- Change management and user adoption strategies for new IAM systems.
- Final project: developing a high-level IAM strategic roadmap.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

Beyond preventing breaches, how can a mature IAM strategy become a primary driver of business innovation and customer trust in an increasingly decentralized digital ecosystem?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing intently on the strategic and business-centric aspects of Identity and Access Management, rather than concentrating solely on the technical features of specific vendor products. While many programs teach how to operate an IAM tool, this training course teaches why and how to build a sustainable, business-aligned IAM program from the ground up. We emphasize the development of a strategic roadmap, the design of a resilient architecture, and the establishment of a robust governance framework that supports long-term organizational goals. The curriculum is built on a foundation of industry-agnostic principles and best practices, enabling participants to apply their learning in any technological environment. By integrating modules on risk management, compliance, and future trends like Zero Trust and decentralized identity, the course provides a holistic and forward-looking perspective. It equips leaders not just to manage identities, but to leverage identity management as a strategic asset for enhancing security, enabling digital transformation, and building a foundation of trust with both employees and customers.