

 **SailPoint**

Course Objective

- ▶ Understand the fundamental concepts of Identity and Access Management (IAM) and Identity Governance & Administration (IGA) in modern enterprises.
- ▶ Learn the importance of identity life cycle management (Joiner–Mover–Leaver), least privilege, and access governance in securing organizational resources.
- ▶ Explore the role of and SailPoint Identity Security in managing user identities, access requests, certifications, and compliance requirements.
- ▶ Gain insights into key IAM governance components, including access reviews, segregation of duties (SoD), role management, and policy enforcement.
- ▶ Develop foundational knowledge of audit readiness, compliance reporting, and regulatory alignment using IAM tools.
- ▶ Understand how IAM supports Zero Trust security models and reduces insider threats and unauthorized access risks.
- ▶ Build practical awareness of enterprise IAM architectures, integrations, and best practices used across regulated industries.

Course Prerequisites

- ▶ Familiarity with basic cyber security concepts such as authentication, authorization, access control, and least-privilege principles is recommended.
- ▶ A basic understanding of enterprise IT environments, including users, applications, and directories, will help in grasping IAM concepts effectively.
- ▶ Knowledge of networking fundamentals and identity-related protocols such as LDAP, SAML, OAuth, or MFA is beneficial but not mandatory.
- ▶ Proficiency in using Windows and Linux operating systems will aid in understanding identity logs, access events, and system interactions.
- ▶ Foundational knowledge of IT administration concepts, including users, roles, permissions, and compliance requirements, will help learners navigate the course material smoothly.
- ▶ Prior exposure to cloud platforms or enterprise applications is advantageous but not required.

Identity Governance and SailPoint Fundamentals

- ▶ Introduction to Identity and Access Management
- ▶ Identity Governance and Administration Concept
- ▶ Overview of SailPoint Platform
- ▶ SailPoint Architecture and Components

SailPoint Identity Now Core Concepts

- ▶ Introduction to Identity and Access Management
- ▶ Identity Governance and Administration Concept
- ▶ Overview of SailPoint Platform
- ▶ SailPoint Architecture and Components

Access Lifecycle Management

- ▶ Joiner Mover Leaver Process
- ▶ Access Request Management
- ▶ Provisioning and De-Provisioning
- ▶ Lifecycle Event Configuration

► Roles, Policies, and Compliance

- Role-Based Access Control
- Business Roles and IT Roles
- Access Certifications
- Policies and Segregation of Duties

► Administration, Integrations & Operations

- Application Onboarding
- IdentityNow Administration
- Integrations and APIs
- Monitoring, Troubleshooting, and Best Practices

► Certification & Capstone Project (Extra Module)

- SailPoint Certification Overview & Exam Preparation
- SailPoint Certification on Paths & Exam Readiness
- Mock Tests & Scenario-Based Questions
- Capstone Project – Enterprise IAM Implementation: Design an end-to-end IAM governance model using SailPoint.

► Course Outcomes

► At the end of the course, the student will:

- CO1 :** Students will gain a comprehensive understanding of Identity and Access Management (IAM) and Identity Governance & Administration (IGA) concepts, roles, and enterprise responsibilities, enabling them to effectively support identity-driven security operations.
- CO2 :** Participants will develop the skills required to manage identity lifecycle processes, including joiner–mover–leaver (JML), access requests, approvals, and role assignments, enhancing secure and compliant access control across enterprise systems.
- CO3 :** Students will become proficient in using SailPoint Identity Security platforms, including their architecture, core components, and governance workflows, empowering them to manage identities and access in complex IT and cloud environments.
- CO4 :** Participants will acquire the knowledge and techniques necessary to perform access certifications, segregation of duties (SoD) analysis, risk assessment, and audit reporting, enabling them to identify access violations and meet regulatory and compliance requirements.
- CO5 :** Learners will develop expertise in identity governance best practices, access policy enforcement, and IAM integration techniques, enabling them to design and implement secure, audit-ready IAM solutions aligned with Zero Trust principles and enterprise security standards.

REFERENCE 1:

- Introduction to Identity & Access Management (IAM) and Identity Governance (IGA) <https://www.sailpoint.com/identity-library/what-is-identity-governance>

► HARDWARE REQUIREMENT:

- Desktop / Laptop with Core i5 or higher Processor, Windows 10 OS / 16 GB of RAM
- Minimum 10 MBPS download speed of the internet connection

Industry Scope

- ▶ The industry scope for this course is extensive and closely aligned with the growing emphasis on identity-centric security and governance in modern enterprises. As organizations increasingly adopt cloud services, remote work models, and digital transformation initiatives, the need for robust Identity and Access Management (IAM) and Identity Governance & Administration (IGA) solutions has become critical.
- ▶ Enterprises across sectors such as information technology, banking and financial services, healthcare, government, telecommunications, and e-commerce require skilled professionals to manage user identities, enforce least-privilege access, ensure regulatory compliance, and protect sensitive data from unauthorized access and insider threats.
- ▶ Graduates of this program can pursue careers in roles such as IAM Engineer, Identity Governance Analyst, Access Management Administrator, GRC and Compliance Analyst, Security Consultant, and Zero Trust Identity Architect. With increasing regulatory requirements and the growing adoption of platforms like SailPoint Identity Security, the demand for IAM professionals is expected to continue rising.
- ▶ As cyber risks become more complex and identity remains the primary attack vector, professionals with strong IAM and governance expertise will play a vital role in securing enterprise environments, making this course a valuable pathway into a high-demand and rewarding cybersecurity career.

Certifications

- ▶ SailPoint IdentityNow / IdentityIQ Certification
- ▶ SailPoint Identity Security Certification (Foundational / Professional)
- ▶ Vendor-Neutral IAM & Identity Governance Certification (Conceptual – aligned with industry best practices)

Job Roles

- ▶ IAM Engineer / Identity Engineer
- ▶ Identity Governance Analyst (IGA Analyst)
- ▶ Access Management Administrator
- ▶ GRC & Compliance Security Analyst
- ▶ Zero Trust Identity Architect
- ▶ IAM Consultant / Security Consultant – Identity
- ▶ Cloud IAM Administrator (Azure AD / AWS IAM integration)

Industry Use Cases

- ▶ Implement and manage Joiner–Mover–Leaver (JML) identity lifecycle automation using IAM platforms.
- ▶ Enforce least-privilege access through role-based and entitlement-based access controls.
- ▶ Conduct access certification and review campaigns to identify excessive or unauthorized access.
- ▶ Implement and monitor Segregation of Duties (SoD) policies to reduce fraud and compliance risks.
- ▶ Integrate IAM platforms with Active Directory, Azure AD, HR systems, and enterprise applications.
- ▶ Design and maintain Zero Trust identity architectures aligned with modern enterprise security strategies.
- ▶ Mode of Delivery: - Virtual Instructor Led Training + Project Mentoring
- ▶ Software Configuration to be arranged in Institution Premises: - Free Account on virtualization, SOC / SIEM & security tools
- ▶ Hardware Configuration to be arranged in Institution Premises: - Windows 10, 16 GB RAM, Good Internet Connection
- ▶ Course Evaluation: - Online Assessment + Project Evaluation
- ▶ Applicable Streams (IT/Non-IT):- Applicable for both IT and Non IT
- ▶ Internship/Placement Opportunities: - Career Fair will be organized for Internships / Placements
- ▶ Train-the-Trainer: Faculty Development Program

Assessment & Evaluation

- ▶ The total score is for 100 Marks, which is a combination of both online assessment and project evaluation
- ▶ Online Assessment – 30 Marks
- ▶ Project Evaluation – 70 Marks
- ▶ Both Industry and Faculty Evaluators will do the Project Evaluation with equal weightage of 50% each

▶ Assessment & Evaluation

- ▶ The total score is for 100 Marks, which is a combination of both online assessment and project evaluation
- ▶ Online Assessment – 30 Marks
- ▶ Project Evaluation – 70 Marks
- ▶ Both Industry and Faculty Evaluators will do the Project Evaluation with equal weightage of 50% each

▶ Final Project Score Metrics & Computation

S. No	Evaluation Metric	Score	Faculty Evaluator Score Weightage	Industry Evaluator Score Weightage	Faculty Evaluator Score (A)	Industry Evaluator Score (B)
1	Technical Training, Assignments & Quizzes	5	50%	50%	2.5	2.5
2	Innovation & Problem Solving	10	25%	75%	2.5	7.5
3	Project Design using Design Thinking	10	25%	75%	2.5	7.5
4	Requirement Analysis using Critical Thinking	10	25%	75%	2.5	7.5
5	Technology Stack	5	25%	75%	1.25	3.75
6	Hacking & Solutioning	15	25%	75%	3.75	11.25
7	Solution Performance	5	25%	75%	1.25	3.75
8	Project Documentation	5	25%	75%	1.25	3.75
9	Project Demonstration	5	50%	50%	2.5	2.5
10	Teamwork	10	100%	0%	10	0
11	Time Management	10	100%	0%	10	0
12	Attendance & Punctuality	10	100%	0%	10	0

- ▶ Final Project Score = Faculty Evaluator Score + Industry Evaluator Score
 Final Score = Online Assessment Score + (Final Project Score) * 70%
- ▶ Ex: if a student's score given by industry evaluators is 43 and the faculty evaluator is 47
- ▶ Total Project Score = 90 Marks
- ▶ The assessment score for the student is 23 out of 30 Marks, then

Identity Governance and SailPoint Fundamentals

- ▶ Introduction to SailPoint IdentityNow UI
- ▶ Understanding Identity Cube and Data Flow
- ▶ Exploring SailPoint Architecture Components
- ▶ Identity Governance Use Case Mapping

Identity Now Core Concepts

- ▶ Adding an Identity Source
- ▶ Identity Aggregation and Correlation
- ▶ Identity Profile Creation
- ▶ Attribute Mapping and Identity Attributes Validation

Access Lifecycle Management

- ▶ Joiner Event Simulation
- ▶ Mover Event and Access Change
- ▶ Leaver Event and Access Revocation
- ▶ Access Request and Approval Workflow
- ▶ Provisioning and De-Provisioning Validation

Roles, Policies, and Compliance

- ▶ Creating Business and IT Roles
- ▶ Role Assignment and Inheritance
- ▶ Creating Access Certification Campaign
- ▶ Defining Policies and SoD Rules
- ▶ Detecting and Resolving Policy Violations

Administration and Integrations

- ▶ Application Onboarding Process
- ▶ Admin Roles and Permissions
- ▶ API Usage and Token Generation
- ▶ Integration with HR / ITSM Tool (Conceptual)
- ▶ Monitoring, Logs, and Troubleshooting

Week	Hour 1 (Technical)	Hour 2 (Lab / Practical)	Assessment
Week 1	IAM & IGA Fundamentals	Saviynt UI Walkthrough	-
Week 1	Saviynt Platform Overview	Understanding Identity Cube	-
Week 1	Saviynt Architecture	Data Flow Analysis	-
Week 1	Governance Concepts	IGA Use Case Mapping	-
Week 1	Revision & Q&A	Practice Lab	-
Week 1			Unit 1 Assessment
Week 2	Saviynt Identity Management	Identity Source Overview	-
Week 2	Authoritative Sources	Source Configuration	-
Week 2	Aggregation & Correlation	Aggregation Lab	-
Week 2	Identity Profiles	Profile & Attribute Mapping	-
Week 2	Accounts & Entitlements	Entitlement Validation	-
Week 2			Unit 2 Assessment
Week 3	Joiner Mover Leaver Process	Joiner Event Lab	-
Week 3	Access Request Management	Request Workflow Lab	-
Week 3	Provisioning Concepts	Provisioning Simulation	-
Week 3	De-Provisioning & Leaver	Access Removal Lab	-
Week 3	Lifecycle Policies	Policy Validation	-
Week 3			Unit 3 Assessment
Week 4	RBAC & ABAC Concepts	Role Exploration	-
Week 4	Enterprise & Application Roles	Role Creation	-
Week 4	Access Certifications	Certification Campaign Lab	-
Week 4	SoD Policies	SoD Rule Configuration	-
Week 4	Audit & Compliance	Violation Review	-
Week 4			Unit 4 Assessment
Week 5	Application Onboarding	Connector Configuration	-
Week 5	Admin & Security Settings	Admin Role Assignment	-
Week 5	Saviynt APIs Overview	API Token & Testing	-
Week 5	Integrations (HR/ITSM)	Integration Flow Review	-
Week 5	Monitoring & Best Practices	Troubleshooting Lab	-
Week 5			Final Assessment & Mock Interview

Unit 1 Labs

Identity Governance and SailPoint Fundamentals

- ▶ Lab 1.1 Introduction to SailPoint IdentityNow UI
- ▶ Lab 1.2 Understanding Identity Cube and Data Flow
- ▶ Lab 1.3 Exploring SailPoint Architecture Components
- ▶ Lab 1.4 Identity Governance Use Case Mapping

Unit 2 Labs

IdentityNow Core Concepts

- ▶ Lab 2.1 Adding an Identity Source
- ▶ Lab 2.2 Identity Aggregation and Correlation
- ▶ Lab 2.3 Identity Profile Creation
- ▶ Lab 2.4 Attribute Mapping and Identity Attributes Validation

Unit 3 Labs

IdentityNow Core Concepts

- ▶ Lab 3.1 Joiner Event Simulation
- ▶ Lab 3.2 Mover Event and Access Change
- ▶ Lab 3.3 Leaver Event and Access Revocation
- ▶ Lab 3.4 Access Request and Approval Workflow
- ▶ Lab 3.5 Provisioning and De-Provisioning Validation

Unit 4 Labs

Roles, Policies, and Compliance

- ▶ Lab 4.1 Creating Business and IT Roles
- ▶ Lab 4.2 Role Assignment and Inheritance
- ▶ Lab 4.3 Creating Access Certification Campaign
- ▶ Lab 4.4 Defining Policies and SoD Rules
- ▶ Lab 4.5 Detecting and Resolving Policy Violations

Unit 5 Labs

Administration and Integrations

- ▶ Lab 5.1 Application Onboarding Process
- ▶ Lab 5.2 Admin Roles and Permissions
- ▶ Lab 5.3 API Usage and Token Generation
- ▶ Lab 5.4 Integration with HR / ITSM Tool (Conceptual)
- ▶ Lab 5.5 Monitoring, Logs, and Troubleshooting



Our Students Are Placed In

Our Students Are Placed In										
										
										
										
										
										