



IDENTITY SECURITY CERTIFICATION COUNCIL

# ISCA

## Identity Security Certified Administrator

### Official Candidate Guide

Edition 1.0 • 2024–2025

Organized by  
**Identity Security Certification Council (ISCC)**  
Community Partner  
**WHYNOTIAM**

[certification.cyberxdelta.com](https://certification.cyberxdelta.com)



## About the Identity Security Certification Council (ISCC)

The Identity Security Certification Council (ISCC) is an independent, globally-oriented professional body established with a singular purpose: to define, uphold, and advance the standards of excellence in the Identity and Access Management (IAM) discipline.

In a digital world where identity is the new perimeter, the ISCC exists to build a globally recognized ecosystem of certified professionals who demonstrate mastery across the full spectrum of identity security — from access governance and privileged access management to authentication, federation, and directory services.

The ISCC is committed to:

- Developing rigorous, vendor-neutral certification frameworks that reflect real-world IAM challenges.
- Recognizing professionals who uphold the highest ethical and technical standards in identity security.
- Bridging the skills gap in the cybersecurity industry by championing identity-first thinking.
- Collaborating with industry partners, academic institutions, and global communities to continuously evolve certification content.

*“Identity is not just a technology problem. It is the cornerstone of digital trust. The ISCC exists to certify those who build and protect that trust.”*

— Identity Security Certification Council

## About CyberXDelta Academy

CyberXDelta Academy is a premier cybersecurity learning and certification body dedicated to equipping professionals with cutting-edge skills in Identity and Access Management, Privileged Access, Cloud Security, and beyond. With a strong focus on applied, practitioner-level education, CyberXDelta Academy serves as the organizing institution behind the ISCA certification program.

Rooted in the belief that security begins with identity, CyberXDelta Academy designs programs that are hands-on, current, and globally relevant — ensuring that certified professionals can immediately apply their knowledge in enterprise environments.

### Community Partner: WHYNOTIAM

WHYNOTIAM is a vibrant, practitioner-driven IAM community that brings together identity professionals from across the globe. As the community partner for the ISCA certification,

WHYNOTIAM plays an integral role in amplifying industry voices, supporting peer learning, and driving awareness of the ISCA program within the global IAM ecosystem. Join Community here: <https://www.linkedin.com/company/the-why-not-iam>

# Mission, Vision & Goals

---

## Our Mission

To create a globally recognized, vendor-neutral standard for identity security professionals — empowering them to design, govern, and protect digital identities at scale across enterprises of all sizes.

## Our Vision

A world where every organization is defended by identity-aware professionals who understand not just the tools, but the principles, policies, and practices that make identity security resilient, adaptive, and trustworthy.

## Certification Goals

- Validate professional competency in core IAM domains including IGA, AM, PAM, Authentication & Federation, and Directory Services.
- Establish a global benchmark for identity security skills that employers, vendors, and institutions can rely on.
- Inspire a generation of identity-first cybersecurity professionals equipped to tackle evolving threats.
- Promote best practices in IAM implementation, governance, and operations across industries.
- Create a trusted, community-backed credential that opens doors to career advancement globally.

## Global Validation of the ISCA Credential

The ISCA certification is structured to be recognized globally, reflecting best practices and industry standards from leading IAM frameworks, regulatory guidelines, and enterprise deployment models worldwide.

Globally, organizations across banking, healthcare, government, technology, and critical infrastructure sectors are actively seeking professionals with validated identity security expertise. The ISCA is designed to meet this demand by:

- Aligning exam content with globally accepted IAM frameworks and standards (NIST, ISO 27001, IEC, GDPR, SOX, HIPAA, and others).
- Being accessible to professionals worldwide through an online, on-demand exam format.
- Issuing digital credentials and badges that can be shared on LinkedIn, professional portfolios, and employer portals for instant verification.
- Partnering with global IAM communities to ensure broad recognition and industry visibility.

## Who Should Attempt the ISCA?

The ISCA is designed for professionals who work in, or aspire to work in, the Identity and Access Management space. If your role touches digital identities, access controls, or security governance, the ISCA is for you.

<b>IAM Administrators</b>	Professionals managing identity platforms, provisioning, deprovisioning, and access lifecycle.
<b>Security Engineers</b>	Engineers building and securing identity infrastructure across hybrid and cloud environments.
<b>PAM Specialists</b>	Practitioners implementing and managing privileged access management solutions.
<b>GRC Professionals</b>	Governance, Risk, and Compliance analysts focused on access governance and identity auditing.
<b>IT Architects</b>	Solution and enterprise architects designing IAM frameworks and identity ecosystems.
<b>Security Analysts</b>	SOC and security analysts who work with identity data, anomaly detection, and access reviews.
<b>Cloud Engineers</b>	Professionals deploying identity solutions on cloud platforms (AWS, Azure, GCP).
<b>Consultants</b>	IAM consultants and advisors guiding clients through identity transformation journeys.
<b>Career Changers</b>	Cybersecurity professionals looking to specialize in the high-demand identity security domain.

*No formal prerequisites are required to attempt the ISCA. However, candidates with at least 1 year of experience in IAM or cybersecurity will find the examination most aligned with their background.*

# Exam Overview

<b>Certification Name</b>	ISCA — Identity Security Certified Administrator
<b>Issued by</b>	Identity Security Certification Council (ISCC)
<b>Organized by</b>	CyberXDelta Academy
<b>Community Partner</b>	WHYNOTIAM
<b>Exam Format</b>	Online, multiple-choice + scenario-based questions
<b>Number of Questions</b>	30 Questions
<b>Exam Duration</b>	60 Minutes
<b>Passing Score</b>	70% (21/30 correct)
<b>Retattempt Policy</b>	No reattempt allowed — ensure you are fully prepared before starting
<b>Language</b>	English
<b>Validity</b>	2 Years (Renewal available)
<b>Credential Type</b>	Digital Certificate + Verifiable Badge
<b>Badge Delivery</b>	Within 3 business days of passing the exam
<b>Exam Access</b>	On-demand — start anytime after registration
<b>Registration Portal</b>	<a href="https://certification.cyberxdelta.com">certification.cyberxdelta.com</a>
<b>Support</b>	<a href="mailto:support@cyberxdelta.com">support@cyberxdelta.com</a>   +91 7840614065

# Exam Domains

The ISCA examination covers six core domains of Identity Security. Each domain represents a critical area of knowledge and practice that modern identity professionals must master.

## Domain 1 Identity Governance and Administration (IGA)

Identity Governance and Administration (IGA) is the foundational pillar of any enterprise IAM strategy. It encompasses the policies, processes, and technologies that manage digital identities and control access to resources throughout an employee or entity lifecycle.

### Key Topics:

✓ Identity Lifecycle Management	✓ Joiner-Mover-Leaver Processes
✓ Role-Based Access Control (RBAC)	✓ Access Request and Approval Workflows
✓ Segregation of Duties (SoD)	✓ Access Certification and Recertification
✓ User Provisioning and Deprovisioning	✓ Identity Data Quality and Governance
✓ IAM Policy Frameworks	✓ Compliance Reporting and Audit Trails
✓ Role Mining and Role Management	✓ Identity Analytics and Insights

## Domain 2 Access Management (AM)

Access Management governs how and when users can access applications, data, and systems. It ensures that the right people get access to the right resources at the right time — and that unauthorized access is effectively prevented and detected.

### Key Topics:

✓ Access Control Models (DAC, MAC, RBAC, ABAC)	✓ Single Sign-On (SSO) Concepts
✓ Session Management and Token Handling	✓ Adaptive and Risk-Based Access
✓ Zero Trust Access Principles	✓ Application Integration with IAM
✓ Policy Enforcement Points (PEP/PDP)	✓ Access Reviews and Attestation
✓ Fine-Grained Authorization	✓ Context-Aware Access Policies

## Domain 3 Privileged Access Management (PAM)

Privileged Access Management addresses the security risks associated with elevated access rights granted to administrators, service accounts, and other privileged users. PAM is one of the most critical controls in any cybersecurity framework due to the significant risk posed by compromised privileged accounts.

### Key Topics:

✓ Privileged Account Discovery and Inventory	✓ Password Vaulting and Rotation
✓ Just-In-Time (JIT) Privileged Access	✓ Session Recording and Monitoring
✓ Least Privilege Principle	✓ Privileged Access Workflows and Approval
✓ Service Account Management	✓ Break-Glass Emergency Access
✓ PAM Integration with SIEM/SOC	✓ Cloud Privileged Access Controls
✓ Credential Management Best Practices	✓ Insider Threat Mitigation via PAM

### Domain 4 Authentication and Federation

Authentication is the process of verifying who a user is. Federation extends this trust across organizational and system boundaries. Together, these capabilities form the backbone of modern identity security, enabling secure access across cloud, mobile, and enterprise environments.

#### Key Topics:

✓ Authentication Factors (Knowledge, Possession, Inherence)	✓ Multi-Factor Authentication (MFA)
✓ Passwordless Authentication	✓ SAML 2.0 Concepts and Flows
✓ OAuth 2.0 Framework	✓ OpenID Connect (OIDC)
✓ Identity Federation Protocols	✓ Identity Provider (IdP) Architecture
✓ Service Provider (SP) Configuration	✓ Trust Establishment and Metadata Exchange
✓ Social Login and External Identity Providers	✓ Token Types: JWT, SAML Assertions, Bearer Tokens
✓ WebAuthn / FIDO2 Standards	✓ Cross-Domain Identity Management (SCIM)

### Domain 5 Directory Services

Directory services form the identity backbone of enterprise environments. They store and organize identity data and serve as the authoritative source of truth for user attributes, group memberships, and resource access across the organization.

#### Key Topics:

✓ LDAP Protocol and Directory Structure	✓ Microsoft Active Directory (AD) Architecture
✓ Azure Active Directory / Microsoft Entra ID	✓ Organizational Units (OUs) and Group Policy
✓ Directory Synchronization and Replication	✓ Forest and Domain Trust Relationships
✓ Service Accounts in Active Directory	✓ Group Types and Membership Management
✓ LDAP Queries and Schema Extensions	✓ Directory Security and Hardening
✓ Hybrid Identity with Azure AD Connect	✓ Domain Controllers and DNS Integration

### Domain 6 IAM Business Scenarios

This domain bridges technical IAM knowledge with real-world business application. Candidates will be assessed on their ability to analyze, design, and recommend IAM solutions based on practical enterprise scenarios — testing both technical understanding and strategic thinking.

### Scenario Topics Include:

✓ Mergers, Acquisitions, and Identity Integration	✓ Onboarding and Offboarding at Scale
✓ Third-Party and Contractor Access Management	✓ Cloud Migration and Identity Strategy
✓ IAM for Regulatory Compliance (SOX, HIPAA, GDPR)	✓ Incident Response with Identity Context
✓ Zero Trust Implementation Scenarios	✓ IAM Tool Selection and Evaluation
✓ Access Governance in Large Enterprises	✓ Identity Sprawl and Shadow IT Management
✓ Customer Identity and Access Management (CIAM)	✓ Risk-Based Access Decision Making

### Exam Domain Weightage

Domain	Weight	Approx. Questions
Identity Governance and Administration (IGA)	17%	~5
Access Management (AM)	17%	~5
Privileged Access Management (PAM)	17%	~5
Authentication and Federation	17%	~5
Directory Services	16%	~5
IAM Business Scenarios	16%	~5

# Registration & Certification Process

The ISCA certification process is streamlined for maximum flexibility. You can register, prepare, and sit the exam entirely online — on your own schedule.

1	<b>Read the Official Guide</b> Download and thoroughly study this official candidate guide. Ensure you are familiar with all six exam domains before proceeding.
2	<b>Visit the Portal &amp; Click Pay Now</b> Go to <a href="https://certification.cyberxdelta.com">certification.cyberxdelta.com</a> , review the certification details, and click the Pay Now button — no account creation required.
3	<b>Complete Payment</b> Complete the payment securely on the portal. Confirmation is instant. Ensure you enter a valid email address at checkout as all exam details will be sent there.
4	<b>Receive Your Exam Credentials by Email</b> Within minutes of successful payment, you will receive an email containing: your Certification Guide, unique Access Code, Exam URL, and Exam Password.
5	<b>Start the Exam — Anytime You Are Ready</b> Use the exam URL, access code, and password from your email to launch the exam. You can start at any time that is convenient — there is no fixed scheduling window.
6	<b>Complete the Exam</b> Answer all 30 questions within the 60-minute time limit. Questions are distributed evenly across all six domains. No reattempt is permitted, so ensure you are well-prepared before you begin.
7	<b>Receive Your Results</b> Upon completion, your score is calculated immediately. A passing score of 70% or above qualifies you for certification.
8	<b>Certification &amp; Digital Badge</b> Upon passing, your official ISCA Certificate and verifiable digital badge will be delivered to your registered email address within 3 business days.

**IMPORTANT:** No reattempt is allowed for the ISCA exam. Once you begin, the session is live and final. Keep your exam credentials (access code, exam URL, and password) confidential. Make sure you have read this guide fully and feel confident across all six domains before clicking Start.

## Support & Contact

We are committed to ensuring a smooth and supportive certification experience. If you encounter any issues at any stage — from registration to badge delivery — our support team is here to help.

<b>Email Support</b>	support@cyberxdelta.com
<b>Phone / WhatsApp</b>	+91 7840614065
<b>Portal</b>	certification.cyberxdelta.com
<b>Response Time</b>	Within 24 business hours

# A Message to Every Candidate

---

In the age of digital transformation, identity is the most contested frontier in cybersecurity. Every breach, every unauthorized access, every data theft — at its core — is an identity problem.

By choosing to pursue the ISCA, you are not just earning a certificate. You are stepping forward as a guardian of digital trust. You are committing to the idea that access should be earned, identities should be protected, and organizations should be secured from the inside out.

*“The future belongs to those who understand identity. Not just as a technology, but as a responsibility.”*

— CyberXDelta Academy

*“Security is not a product. It is a practice. And identity-first professionals are the practitioners the world needs today.”*

— ISCC

*“Your certification is not the end of the journey. It is the proof that your journey is worth following.”*

— WHYNOTIAM Community

The ISCA is your credential. But the mission is larger than a single exam. It is about raising the bar for the entire identity security profession — one certified professional at a time.

We believe in your potential. We are here to validate your expertise. And we look forward to welcoming you into the global community of ISCA-certified professionals.

***Good luck. Secure identities. Secure the world.***

— CyberXDelta Academy & ISCC

## Quick Reference Card

<b>Certification</b>	ISCA — Identity Security Certified Administrator
<b>Issuing Body</b>	Identity Security Certification Council (ISCC)
<b>Organized by</b>	CyberXDelta Academy
<b>Community Partner</b>	WHYNOTIAM
<b>Questions</b>	30 MCQ + Scenario-Based
<b>Duration</b>	60 Minutes
<b>Pass Mark</b>	70% (21/30)
<b>Retattempt</b>	Not allowed
<b>Domains</b>	IGA   AM   PAM   Auth & Federation   Directory   IAM Scenarios
<b>Exam Start</b>	Anytime after receiving credentials via email
<b>Badge Delivery</b>	Within 3 business days of passing
<b>Register At</b>	certification.cyberxdelta.com
<b>Support Email</b>	support@cyberxdelta.com
<b>Support Phone</b>	+91 7840614065