WISEMAN CYBERSEC
BE WISE , BE SECURE

36-HOUR INSTRUCTOR-LED CERTIFICATION PREPARATION

ADVANCED IN AI SECURITY MANAGEMENT

AAISM | ISACA Certification Preparation

AI Governance, Enterprise Risk and Security Controls

A practical programme for experienced security professionals who need to govern enterprise AI, assess AI-specific risk and guide security controls across the AI lifecycle.

36 Hours
INSTRUCTOR-LED

12 Sessions
3 HOURS EACH

Applied
ENTERPRISE CAPSTONE

ADVANCED IN AI SECURITY MANAGEMENT

Student Course Guide | Be Wise. Be Secure.

Structured around the current ISACA AAISM exam content outline

www.wisemancybersec.com

info@wisemancybersec.com

AAISM CERTIFICATION PREPARATION

PROGRAMME OVERVIEW

Lead practical security decisions for enterprise AI

Secure AI with a management lens

AI security management brings governance, enterprise risk, architecture and operational controls together. This programme helps experienced professionals evaluate how AI is selected, built, bought, deployed and monitored, and how the organization responds when risk changes or an incident occurs.

LEARNING OUTCOMES

- Advise on AI security governance, roles, policies and program responsibilities.
- Assess AI risks, set thresholds, select treatments and trigger reassessment.
- Identify AI threats and vulnerabilities and recommend proportionate testing.
- Assess security requirements for AI vendors and supply-chain dependencies.
- Review AI security architecture, data controls and lifecycle decisions.
- Plan AI incident handling, business continuity and recovery.

Course at a glance

DURATION
36 instructional hours

STRUCTURE
12 sessions x 3 hours

CURRICULUM
3 exam domains + capstone

APPROACH
Instructor-led, scenario-based

ASSESSMENT
Knowledge checks and casework

Intended participants

- Security managers and leaders
- AI, cyber risk and governance professionals
- Security architects and technology risk teams
- Consultants and experienced security practitioners

AAISM EXAM ELIGIBILITY

ISACA requires an active CISM or CISSP certification to sit the AAISM exam. Candidates must also pass the exam and submit a certification application under ISACA requirements. Course attendance does not grant exam eligibility or the AAISM credential. Confirm current rules with ISACA before registering.

DOMAIN 1 | 31% OF THE AAISM EXAM

CURRICULUM

AI governance and security program management

01 Stakeholders, Frameworks & Requirements

DOMAIN 1 | ALIGN AI SECURITY WITH BUSINESS CONTEXT

- Identify business owners, security, data and AI teams, privacy, legal, procurement and other affected stakeholders.
- Define charters, roles, decision rights, escalation paths, risk appetite and governance forums.
- Interpret applicable industry frameworks, standards, regulatory requirements and contractual obligations.
- Consider business use cases, consumer versus enterprise environments, and responsible-use expectations.

APPLIED EXERCISE

Create a stakeholder and accountability map for an organization adopting a generative AI service.

02 Policies, Lifecycle & Program Management

DOMAIN 1 | ESTABLISH REPEATABLE AI SECURITY PRACTICES

- Develop AI-related strategies, policies, standards, acceptable-use guidance and procedures.
- Inventory, classify and manage AI assets, models, data and dependencies through their lifecycle.
- Plan an AI security program with ownership, resources, measures, review cadence and improvement actions.
- Integrate AI security awareness, business continuity and incident response into established processes.

APPLIED EXERCISE

Draft a policy-to-control map and identify evidence that would demonstrate implementation.

DOMAIN 2 | 31% OF THE AAISM EXAM

CURRICULUM

AI risk, threats and supply chain

03 AI Risk Assessment & Treatment

DOMAIN 2 | SET THRESHOLDS AND MANAGE CHANGING RISK

• Identify AI-specific risks, opportunities, business impacts and affected stakeholders.
• Assess likelihood, impact, risk appetite and thresholds; select and document treatment options.
• Monitor internal and external changes that may require reassessment of AI risk.
• Use AI impact assessments, metrics and governance escalation to support decisions and residual-risk acceptance.

APPLIED EXERCISE

Assess a proposed AI use case and recommend risk thresholds, treatments, owners and review triggers.

04 Threat, Vulnerability & Vendor Management

DOMAIN 2 | TEST DEFENSES AND MANAGE DEPENDENCIES

• Understand AI threat and vulnerability themes across data, models, applications, infrastructure and use.
• Plan risk-based testing, vulnerability identification, remediation tracking and ongoing monitoring.
• Assess AI vendor and supply-chain risks, including model providers, datasets, software and service dependencies.
• Embed, monitor and verify security requirements in procurement, contracts, integrations and vendor reviews.

APPLIED EXERCISE

Review a third-party AI service and propose security due diligence, contract safeguards and ongoing checks.

DOMAIN 3 | 38% OF THE AAISM EXAM

CURRICULUM

AI technologies, architecture and controls

05 AI Security Architecture & Lifecycle

DOMAIN 3 | SECURE DESIGN, SELECTION AND VALIDATION

- Apply AI security architecture principles and integrate AI components into enterprise architecture.
- Evaluate model selection, sourcing, training, validation and deployment decisions from a security perspective.
- Assess security risks across development, acquisition, integration, operation, change and retirement.
- Consider access control, secure configuration, testing, resilience and security requirements throughout the lifecycle.

APPLIED EXERCISE

Sketch a secure architecture for an AI-enabled business workflow and mark trust boundaries and control points.

06 Data, Privacy, Trust & Security Controls

DOMAIN 3 | PROTECT INPUTS, OUTPUTS AND OPERATIONS

- Apply data management controls for identification, classification, access, integrity, retention and lifecycle protection.
- Consider privacy, ethical, trust and safety controls, including risk-based human oversight of outputs and decisions.
- Implement and monitor security controls for AI systems, data flows, services and supporting infrastructure.
- Define security measures, incident handling, continuity and recovery actions for AI-enabled services.

APPLIED EXERCISE

Build a control set for an AI solution and define how owners will monitor its effectiveness.

SESSION PLAN

36-HOUR LEARNING JOURNEY

Twelve focused sessions | 3 hours each

1 AAISM context & AI security

- Exam domains and security-manager role
- AI use cases and enterprise context

PRACTICE Frame an AI adoption decision

2 Stakeholders, frameworks & requirements

- Governance roles and forums
- Framework, regulatory and contract context

PRACTICE Map stakeholders and obligations

3 Policies, assets & program management

- AI policies and acceptable use
- Asset/data lifecycle and program measures

PRACTICE Draft control ownership

4 AI risk assessment

- Risk identification and impact
- Thresholds, treatment and reassessment

PRACTICE Build a risk register entry

5 Threat and vulnerability management

- AI threat landscape and testing
- Monitoring and remediation decisions

PRACTICE Prioritize a control response

6 Vendor and supply-chain risk

- Provider and dependency review
- Procurement and contract safeguards

PRACTICE Review AI vendor evidence

7 Security architecture and design

- Architecture patterns and trust boundaries
- Enterprise integration and security requirements

PRACTICE Sketch security architecture

8 Model and solution lifecycle

- Selection, sourcing and development
- Training, validation, release and change

PRACTICE Trace lifecycle controls

9 Data and privacy controls

- Data inventory, access and integrity
- Privacy, ethics, trust and safety

PRACTICE Assess data control gaps

10 Security monitoring and resilience

- Security controls and metrics
- Continuity, incident response and recovery

PRACTICE Design response measures

11 Integrated enterprise case

- Risk, architecture and control decisions
- Stakeholder briefing and residual risk

PRACTICE Present an AI security plan

12 Capstone and exam readiness

- Capstone review and feedback
- Domain knowledge checks and exam strategy

PRACTICE Defend recommendations

Enterprise capstone: Develop and present a security management plan for an AI-enabled service, covering governance, risk treatment, architecture, controls, monitoring and incident readiness.

PROGRAMME OUTCOMES

FROM LEARNING TO SECURITY LEADERSHIP

Make defensible AI security decisions across the enterprise

01 Govern responsibly

Set roles, policies and program measures for AI security.

02 Manage AI risk

Assess risk, set thresholds and choose proportionate treatments.

03 Test threats

Address vulnerabilities and monitor AI supply-chain dependencies.

04 Secure architecture

Apply controls to AI design, models, data and lifecycle decisions.

05 Protect operations

Plan monitoring, incident response and continuity for AI services.

06 Brief stakeholders

Communicate risk, evidence, residual exposure and next steps.

ISACA AAISM EXAM REFERENCE

ISACA describes the AAISM exam as 90 questions across three domains: AI Governance and Program Management (31%), AI Risk Management (31%), and AI Technologies and Controls (38%). This 36-hour course allocates 9, 9 and 12 hours to the domains, plus 6 hours for guided integration, capstone and exam preparation.
To sit the exam, candidates must hold an active CISM or CISSP. Passing the exam and meeting ISACA's application requirements are separate steps. Check ISACA's current exam and certification rules before

OFFICIAL REFERENCE

- ISACA AAISM Exam Content Outline: https://www.isaca.org/credentialing/aaism/aaism-exam-content-outline
- ISACA AAISM certification requirements: https://www.isaca.org/credentialing/aaism/get-aaism-certified
- This is independent exam preparation and is not represented as an ISACA-issued course or certification.