ISACA Advanced in AI Security Management

The first and only AI-centric security management certification.

A McKinsey study found that **72% of respondents said that their companies have implemented AI in at least one business function.** *The State of AI: Global survey | McKinsey (March 2025)*
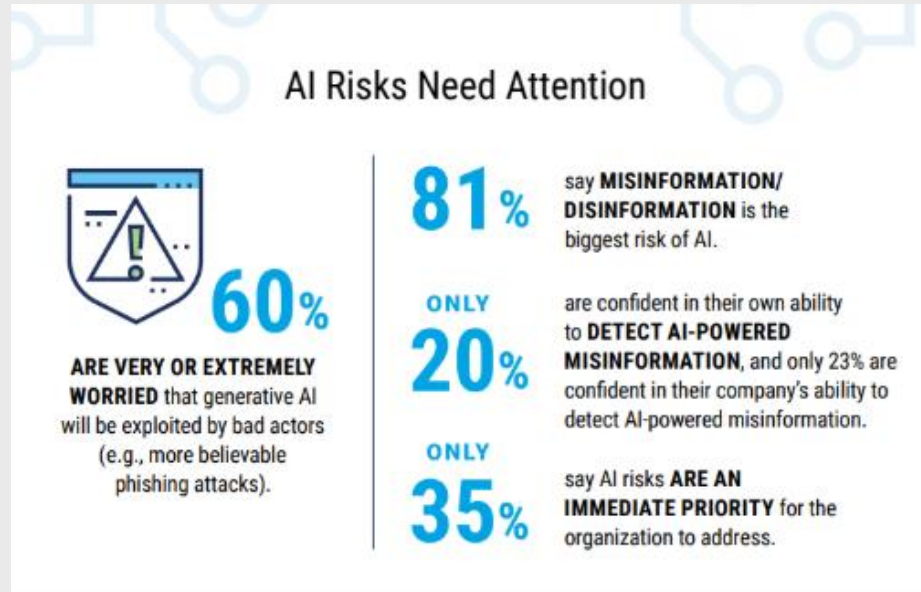
Meanwhile, **40% of organizations** are offering **no** AI training at all. *ISACA AI Pulse Poll (2024)*

This means that most of your customers are right now implementing and using AI—oftentimes **without a solid strategy on how to mitigate the associated risk.**

Artificial Intelligence is the **fastest growing technology** and is expected to continue to grow at a very high rate becoming a **multi trillion-dollar industry** in the next few years.

Growing Need for AI Security Professionals

AI Risks Need Attention

60% ARE VERY OR EXTREMELY WORRIED that generative AI will be exploited by bad actors (e.g., more believable phishing attacks).

81% say MISINFORMATION/DISINFORMATION is the biggest risk of AI.

ONLY **20%** are confident in their own ability to DETECT AI-POWERED MISINFORMATION, and only 23% are confident in their company's ability to detect AI-powered misinformation.

ONLY **35%** say AI risks ARE AN IMMEDIATE PRIORITY for the organization to address.

AI POLICIES LACKING

ONLY 15% of organizations have a formal, comprehensive policy governing the use of AI technology at their organization.

- AI is being incorporated at a rapid pace, and organizations need expertise to be able to secure AI tools while leveraging their immense power to innovate.

- Regulation is expanding around AI, including the California AI Transparency Act, Colorado AI Act, and the EU AI Act. The regulatory landscape remains dynamic.

- Privacy regulations may not specifically mention AI but given the immense amount of data required to train AI models, they will apply in cases where personal data is utilized or adjacent.

ISACA

AAISM ISACA Advanced in AI Security Management

What is AAISM?

ISACA's Advanced in AI Security Management (AAISM) is **the first certification that enables security management professionals to validate their expertise and experience in securing enterprise AI solutions and leveraging AI to improve security operations**.

Security managers must not only **evaluate and secure new products** but must be involved in the **continuous monitoring of existing enterprise solutions** that gain new AI functionality. **AAISM also enables security managers** to effectively leverage AI into their own security operations.

AAISM Domains:
- AI Governance and Program Management
- AI Risk Management
- AI Technologies and Controls

ISACA.

AAISM
ISACA Advanced
in AI Security
Management

Overarching Outcomes

- **Enhanced Threat Detection and Response:**
  - Cybersecurity requires vigilance and threat actors will be taking advantage of AI. The **AAISM validates security professionals' knowledge and skills to accurately detect and respond to complex threats.** Building upon established security best practices, this credential ensures professionals are equipped with the latest methodologies for robust organizational protection.
- **Maximizing Internal AI Opportunities:**
  - AI provides an opportunity to streamline business and security operations. **Security professionals holding this certification will be able to strategically leverage AI technologies to drive internal growth and foster innovation.** By integrating AI's transformative potential into everyday operations, organizations can benefit from increased efficiency, smarter decision-making, and a culture of continuous improvement.
- **Adapting to an Evolving Landscape:**
  - This credential emphasizes the importance of adaptability in the fast-paced, AI-driven environment. **AAISM holders will be able to demonstrate the knowledge and skills needed to navigate technological changes**, ensuring their organizations maintain a strategic edge and can anticipate and counter emerging threats.

ISACA.

AAISM
ISACA Advanced
in AI Security
Management.

Target Audience

Primary audience for AAISM are security professionals that hold a CISM or CISSP. Exam candidates must also have experience securing AI and leveraging AI within security programs.

Secondary Audience are enterprises and associated hiring managers who are looking for skilled, forward-looking security professionals with experience in AI.

Career level: Mid to late career

Experience level: Manager, Director or Executive

Market Segments: 2/3 of CISSP holders are in NA, robust presence throughout Western Europe (UK, Germany, France, Netherlands).

- **North America:** 28,343 CISMs
- **Europe:** 16,503 CISMs
- **APAC:** 15,207 CISMs

*Course and Exam available in English and Spanish

- [CISSP Holders by Region](#)
- [ISACA Cert Growth By Region](#)

ISACA

AAISM
ISACA Advanced in AI Security Management

Where AAISM Fits in ISACA's Current Offering

- AAISM is an opportunity for CISM and CISSP holders to demonstrate expertise in securing enterprise AI solutions and leveraging AI to improve security operations.

- AI Fundamentals and ISACA's AI Learning Pathway, including the AI Threat Landscape course can provide security professionals with supplemental AI knowledge.

How AAISM Suits Your Organization

Sales to complete with information about how this works for this specific customer.

Regional regulation or changes, specific learning pathway or staff requirements, etc.

Uptake of AI resources and tools.

ISACA

AAISM

ISACA Advanced in AI Security Management

Why ISACA?

ISACA's accredited training and certification resources distinguish themselves by providing comprehensive solutions for security management, auditing, risk, governance, data privacy, cybersecurity and more!

These resources empower professionals to stay at the forefront of technological advancements, equipping them with the skills needed. ISACA has a reputation for providing the best training, certifications, and information for IT professionals.

Upon AAISM Certification, Successful Candidates Will Be Able to:

- **Unlock** their potential as a leader in AI-driven security.
- **Enable** themselves to assess risks, optimize security processes, and drive innovation, ensuring the organization stays ahead in the digital age.
- **Validates** their knowledge and expertise against 3 globally-validated AI security domains.
- **Join** the ranks of trusted professionals, who are setting the standard for AI-enabled security.

ISACA.

AAISM ISACA Advanced in AI Security Management.

ATO AAISM Beta & Train-the-Trainer:

The Beta and Train-the-Trainer applications will be available on **June 2** (application link to come).
Eligible applicants will be selected on or before **June 16.**
Beta is available to CISM and CISSP holders; Train-the-Trainer is available to CISM accredited trainers.
The cost is $399 and includes exam and review manual.

Exam Preparation:
June 16: Selected participants will receive exam prep material.
•Volunteers should begin studying and preparing to sit for the AAISM Certification exam.

Exam:
July 7 – July 21: Participants will be able to sit for the AAISM exam
•The exam will be self-scheduled through ISACA's exam administrator, PSI.
•The **exam must be completed by July 21**.
•During the beta, the AAISM exam will only be available through remote proctor.
•*Note: The exam will only be available during this two-week period. If you are unable to sit for the exam during this time, please refrain from applying. You will not be eligible for a refund.*

Train-the-Trainer – **seats are FREE for ATOs:**
July 21-25 (tentative)
1-day training session (virtual)
Requires CISM trainer accreditation.

Applications Due **June 16**
Seats are limited, don't wait to be a part of this exciting opportunity!
AAISM officially launches September 2025 (Exam and Exam Prep)

ISACA

AAISM
ISACA Advanced
in AI Security
Management

Appendix

Regulatory Factors

- The regulatory landscape is dynamic, and companies would be wise to get ahead of imminent additional regulations.

- Regulation is expanding around AI. With the EU AI Act, it is likely that other countries and regions will follow suit with additional regulation.

- Privacy regulations may not specifically mention AI but given the immense amount of data required to train AI models, they will apply in cases where personal data is utilized or adjacent.

- Policy and control of AI is still lacking in organizations:

AI POLICIES LACKING

ONLY 15%

of organizations have a formal, comprehensive policy governing the use of AI technology at their organization.