ISACA Belgium Chapter

ACCREDITED TRAINING ORGANISATION

NY Networking Pre-Session

ISACA Certification Updates

AAIA™ ISACA Advanced in AI Audit™

AAISM™ ISACA Advanced in AI Security Management™

AAIR™ Advanced in AI Risk™ An ISACA® Certification

CRISC® Certified in Risk and Information Systems Control® An ISACA® Certification

CDPSE® Certified Data Privacy Solutions Engineer™ An ISACA® Certification

ISACA Belgium Chapter 40+ YEARS

January 30, 2026

KPMG

Today’s Agenda

Brand-New AI Certifications

01 **Peter Geelen**

AAIA (Advanced in AI Audit)

02 **Geert Nobels**

AAISM (Advanced in AI Security Management)

03 **Liviu Luca**

AAIR (Advanced in AI Risk)

Freshly Updated / New Materials

04 **Liviu Luca**

CRISC (risk + resilience, updated content you’ll want to know about).

05 **Egide Nzabonimana**

CDPSE (privacy engineering—what’s new in the latest materials)

ISACA Belgium Chapter 40 YEARS

HOT OFF THE PRESS!!

ISACA BELGIUM ACCREDITED FOR AAISM

ISACA
Belgium Chapter
ACCREDITED TRAINING ORGANISATION

On January 26, APMG confirmed that ISACA Belgium has been accredited for AAISM, and has there by extend our suite of APMG products to seven:

AAISM, CISM, CRISC, CGEIT, CDPSE, CISA, and COBIT 2019.

Geert Nobels is our first APMG approved trainer for ISACA AAISM

2026 Agenda

CISM Certified Information Security Manager. An ISACA® Certification	26-31 MAR IN - PERSON	14 - 17 SEPT IN - PERSON	
CISA Certified Information Systems Auditor. An ISACA® Certification	20 - 23 APR IN - PERSON	14 - 17 SEPT IN - PERSON	07 - 10 DEC IN - PERSON
CGEIT Certified in the Governance of Enterprise IT. An ISACA® Certification	14 & 24 - 26 MAR HYBRID	28 NOV & 8 - 10 DEC HYBRID	
CRISC Certified in Risk and Information Systems Control. An ISACA® Certification	19 - 22 MAY IN - PERSON	17- 22 SEPT IN - PERSON	01 - 04 DEC IN - PERSON
COBIT 2019	11 - 12 MAY IN - PERSON	07 - 08 SEPT ONLINE	03 - 04 DEC IN - PERSON

Inhouse Training from

ISACA Belgium Chapter
ACCREDITED TRAINING ORGANISATION

ISACA Belgium offers early-career and trend-focused training. For group or in-house upskilling

Get access to all trainings at a discounted price. Materials included

USE THE CODE AT CHECKOUT !

DISCOUNT COUPON

15% OFF

CODE : NYEVENT26

SCAN ME BEFORE 15 FEBRUARY 2026!

ISACA Belgium Chapter 40+ YEARS

ISACA Belgium Chapter
ACCREDITED TRAINING ORGANISATION

AAIA (Advanced in AI Audit)

First Edition

AAIA™ ISACA Advanced in AI Audit™

What's in it?

ISACA Belgium Chapter 40+ YEARS

Peter Geelen

CISA, CISM, CDPSE ISACA accredited trainee & Accredited Auditor
ISACA CISA, CISM, CDPSE+ ISC2 + PECB ISO Master

What is AAIA?

Designed for IT Audit professionals with a CISA, CIA (IIA) or CPA (AICPA) certification looking to gain recognition for their expertise, assuring AI-driven processes comply to the highest industry standards.

Image generated with Perplexity

What is AAIA?

Focus on audit domains

- AI Governance and risk
- AI operations
- AI Auditing Tools and Techniques

Image generated with Perplexity

AAIA Key Domain 1

AI Governance and Risk

A

AI Models, Considerations, and Requirements

B

AI Governance and Program Management

C

AI Risk Management

D

Privacy and Data Governance Programs

E

Leading Practices, Ethics, Regulations, and Standards for AI

AAIA Key Domain 2

AI Operations

A
Data Management Specific to AI

B
AI Solution Development Methodologies and Lifecycle

C
Change Management Specific to AI

D
Supervision of AI Solutions (e.g., outputs, impacts, and decisions)

E
Testing Techniques for AI Solutions

F
Threats and Vulnerabilities Specific to AI

G
Incident Response Management Specific to AI

AAIA Key Domain 3

AI Auditing Tools and Techniques

A
Audit Planning and Design

B
Audit Testing and Sampling Methodologies

C
Audit Evidence Collection Techniques

D
Audit Data Quality and Data Analytics

E
AI Audit Outputs and Reports

Resources To Get Started

AAIA Online Review Course

AIA Exam prep Store>Exam Prep > AAIA

AAIA Questions, Answers & Explanations Database

The ISACA® Advanced in AI Audit Questions, Answers & Explanations (QAE) Database 2025 is a comprehensive pool of practice questions designed to help prepare candidates for the AAIA Certification Exam.

A 12-month subscription to a comprehensive 200+ question pool of items. Build a custom study plan with a personalized dashboard, track progress and review previously answered questions

AAIA Review Manual (Print/Digital Versions)

This is an (electronic/print) book designed to be accessible anytime through your browser without the need for downloads or printing. Please review the FAQs to ensure you understand the requirements prior to purchase, as all sales are final.

Tips for Earning Your Certification

Scan this QR Code to get the tips

Tips for Earning Your ISACA® AAIA™ Certification

ISACA Advanced in AI Audit.

1. Confirm eligibility early
Make sure you already hold an CISA® or recognized audit/accounting credential (CIA, US CPA, ACCA or FCCA, Canadian CPA, Australian CPA or FCPA, Japanese CPA).
Don't wait until after registering to check this.

2. Download the exam content outline
Exam domain breakdown:
- AI Governance & Risk (33%)
- AI Operations (46%)
- AI Auditing Tools & Techniques (21%)

Use this to organize and structure your study plan.

3. Prioritize high-weight domains
Spend more time on AI Governance & Risk, since it's the largest portion of the exam.

4. Use official ISACA study resources
The *AAIA Review Manual,* Online Course, and QAE (Questions, Answers & Explanations) Database are exam-aligned. The QAE is especially helpful to understand question style.

5. Study AI from an auditor's perspective
Don't get lost in coding details—focus on auditing, governance, risk, ethics, and compliance in AI systems.

6. Practice with timed exams
The exam is 90 questions in about 2.5 hours. Use practice tests to build speed and endurance.

7. Stay current with AI regulations
Be aware of evolving standards like the EU AI Act, NIST AI RMF, ISO/IEC 42001—these are often tested.

8. Join study groups or ISACA chapters
Local ISACA chapters and online forums are great for accountability, clarifying tough concepts, and sharing resources.

9. Plan around the 12-month exam window
After registering, you get **12 months** to take the exam. Don't procrastinate—aim to schedule within three to six months so you have time for retakes if needed.

10. Plan for Your CPEs
You'll need 10 AI-focused Continuing Professional Education (CPE) hours **per year** to keep your AAIA active. Start tracking AI-related webinars, courses, and conferences now.

For more information, go to www.isaca.org/aaia

ISACA

ISACA Belgium Chapter 40+ YEARS

ISACA Advanced in AI Audit.

ISACA AAIA

The world's first Advanced AI Audit Certification

ISACA Advanced in AI Audit™

Learn more here:

ISACA Belgium Chapter 40+ YEARS

ISACA Belgium Chapter
ACCREDITED TRAINING ORGANISATION

AAISM (Advanced in AI Security Management)

First Edition

AAISM™ ISACA Advanced in AI Security Management™

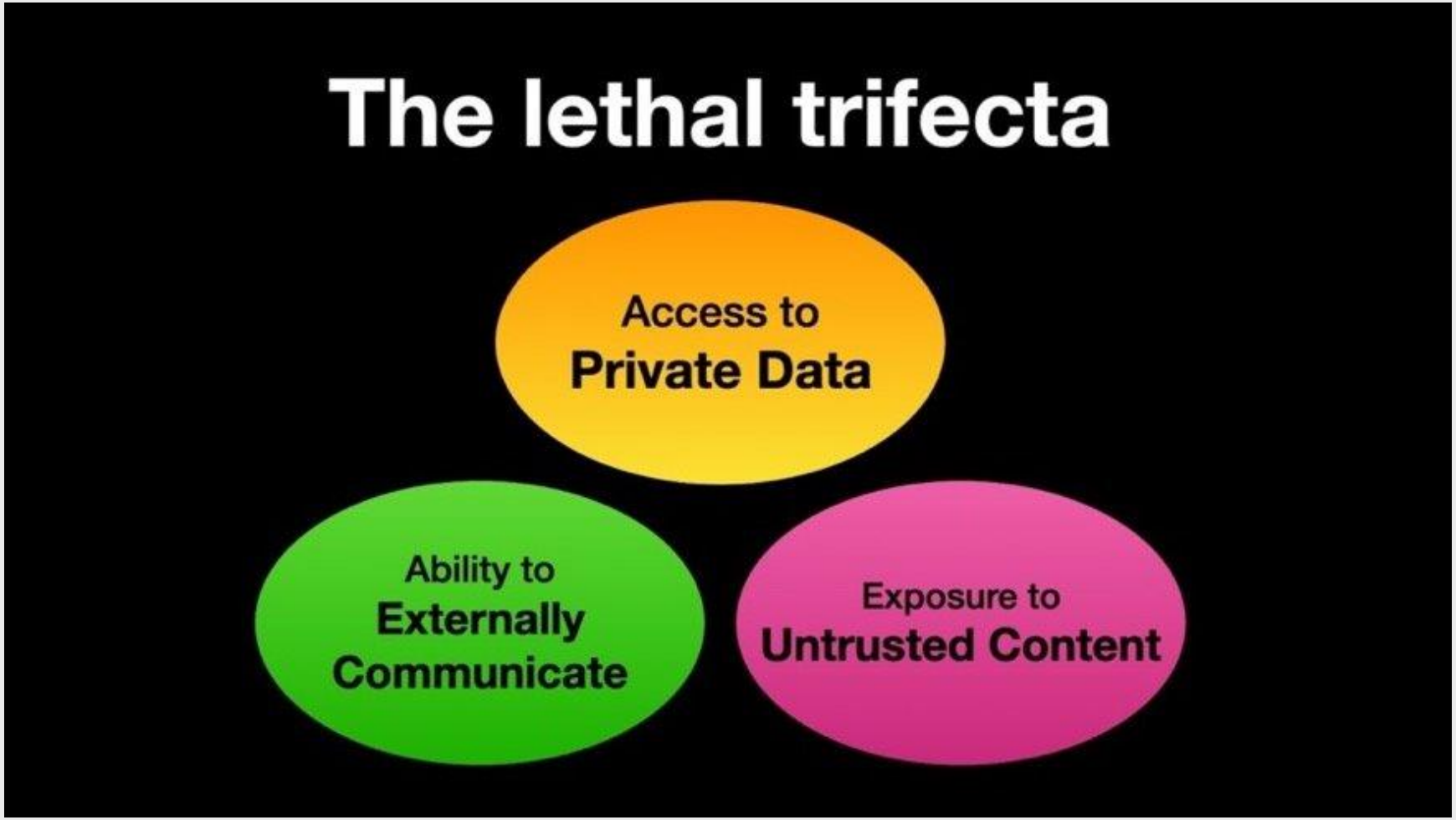
Geert Nobels

ISACA Belgium Chapter 40+ YEARS

Recent AI Security Breaches

- Slack: https://promptarmor.substack.com/p/slack-ai-data-exfiltration-from-private
- Salesforce: https://noma.security/blog/forcedleak-agent-risks-exposed-in-salesforce-agentforce/
- Microsoft (Echoleak): https://www.arxiv.org/pdf/2509.10540
- Other exfiltration attacks: https://simonwillison.net/tags/exfiltration-attacks/
- Design patterns against prompt injection: https://simonwillison.net/2025/Jun/13/prompt-injection-design-patterns/

AI can be a perfect storm….



https://simonwillison.net/2025/Jun/16/the-lethal-trifecta/

…despite AI guardrails

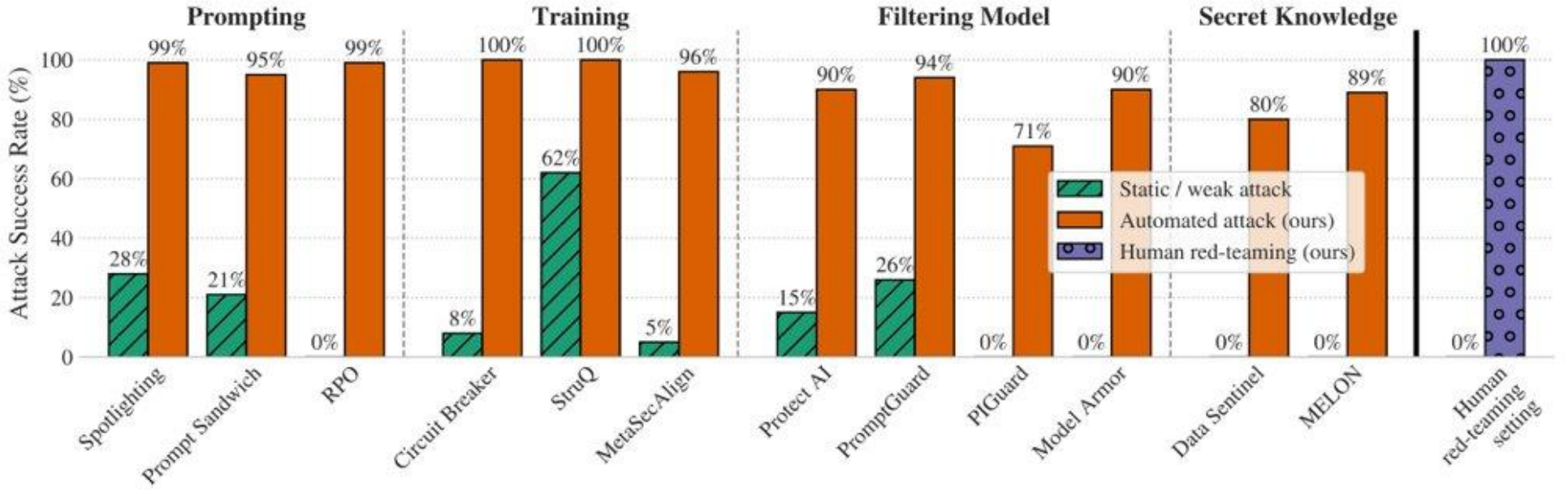
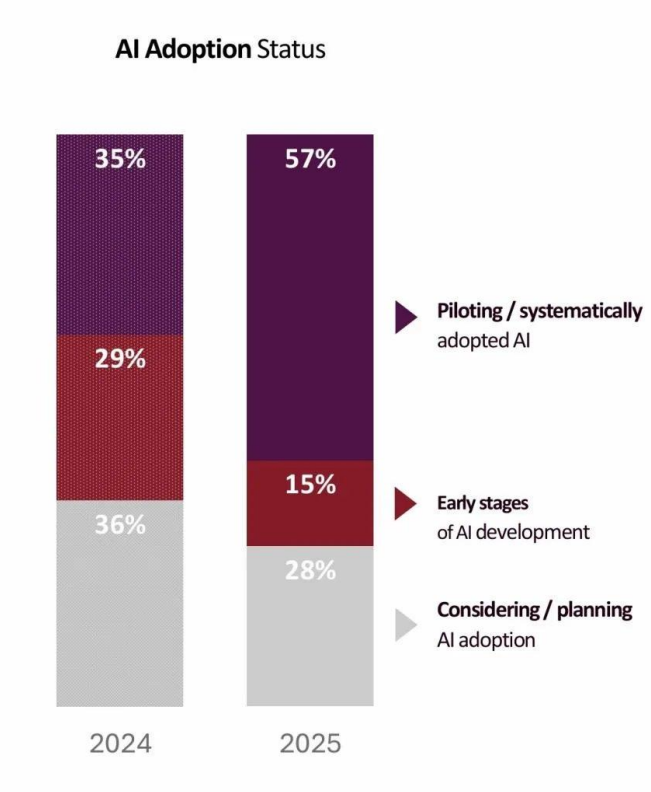
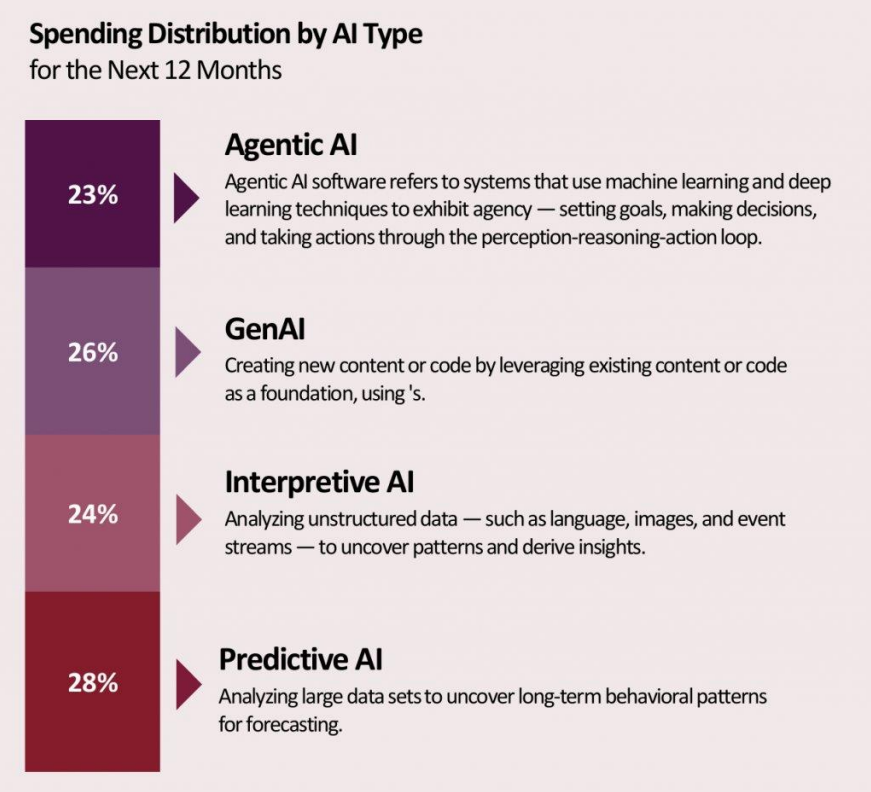


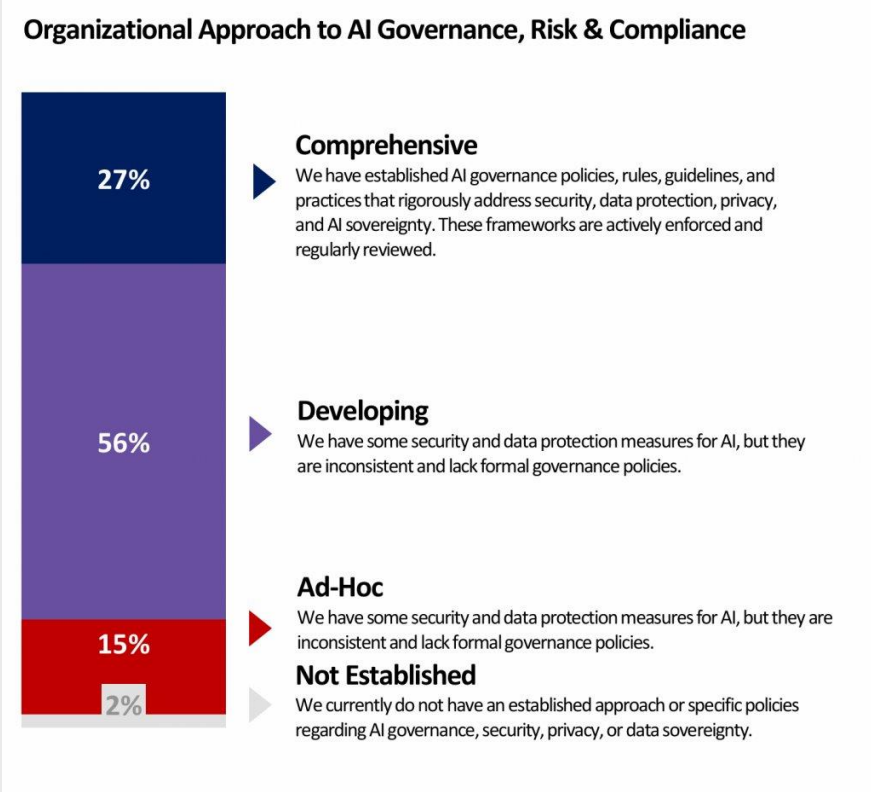
Figure 1: Attack success rate of our adaptive attacks compared to the weaker or static attacks considered in the original paper evaluation. None of the 12 defenses across four common techniques is robust to strong adaptive attacks. On the rightmost bars, human red-teaming succeeds on all of the scenarios while the static attack succeeds on none.

https://arxiv.org/pdf/2510.09023

But what about AI Governance?







AAIASM Key Domain 1

AI Governance and Program Management

31% DOMAIN 1 – AI GOVERNANCE AND PROGRAM MANAGEMENT

This Domain demonstrates your ability to advise stakeholders on implementing AI security solutions through appropriate and effective policy, data governance, program management and incident response.

A–STAKEHOLDER CONSIDERATIONS, INDUSTRY FRAMEWORKS, AND REGULATORY REQUIREMENTS
B–AI-RELATED STRATEGIES, POLICIES, AND PROCEDURES
C–AI ASSET AND DATA LIFE CYCLE MANAGEMENT
D–AI SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT
E–BUSINESS CONTINUITY AND INCIDENT RESPONSE

AAIASM Key Domain 2

AI Risk Management

31% DOMAIN 2 – AI RISK MANAGEMENT

This Domain confirms your skill at assessing and managing risks, threats, vulnerabilities and supply chain issues related to the enterprise-wide adoption of AI.

A–AI RISK ASSESSMENT, THRESHOLDS, AND TREATMENT
B–AI THREAT AND VULNERABILITY MANAGEMENT
C–AI VENDOR AND SUPPLY CHAIN MANAGEMENT

AAIASM Key Domain 3

AI Technologies and Controls

38% DOMAIN 3 – AI TECHNOLOGIES AND CONTROLS

This Domain focuses on optimizing AI security and highlights your knowledge of security technologies, techniques and controls tailored to AI systems.

A–AI SECURITY ARCHITECTURE AND DESIGN
B–AI-RELATED STRATEGIES, POLICIES, AND PROCEDURES
C–DATA MANAGEMENT CONTROLS
D–PRIVACY, ETHICAL, TRUST AND SAFETY CONTROLS
E–SECURITY CONTROLS AND MONITORING

Supporting Tasks

Supporting Tasks

1. Collaborate on charter, roles, and responsibilities for governance and management of AI to align with business objectives.
2. Establish and maintain AI-specific security policies and procedures to inform the development and implementation of AI standards and guidelines.
3. Ensure the responsible use of AI by utilizing leading practices, ethical principles, regulatory requirements, and industry frameworks.
4. Participate in or oversee the AI risk management life cycle, including impacts on enterprise risk.
5. Identify and assess the AI threat landscape.
6. Monitor for internal and external AI-related factors to identify the need for reassessment of risk.
7. Design and implement testing and vulnerability management of AI solutions.
8. Conduct AI impact assessments and ensure conformity with regulatory requirements.
9. Embed, monitor, and verify AI security requirements when utilizing vendor AI-enabled solutions.
10. Design and implement security architecture specifically for AI.
11. Advise on the integration of AI architecture as part of enterprise architecture.
12. Design, implement, and regularly review AI security controls to treat risk to an acceptable level.
13. Establish and maintain processes to identify, inventory, and classify data and assets related to AI.
14. Identify and treat security risk associated with data used in the AI life cycle.
15. Establish and maintain AI-specific processes to investigate, document, and report on AI security incidents in accordance with regulatory and contractual requirements.
16. Establish and maintain AI incident handling processes, including containment, notification, escalation, eradication, and recovery.
17. Address AI security risk as part of business continuity and disaster recovery planning.
18. Define and monitor security metrics for AI solutions used throughout the organization.
19. Review and implement AI security tools as part of the information security program.
20. Conduct risk-based human oversight of AI inputs/outputs including trust and safety, quality, explainability, and robustness.
21. Develop and maintain AI-specific security awareness training and acceptable use guidelines.
22. Advise on security risk and controls related to the AI solution development life cycle within an organization.

Action	Key Subject
Collaborate	AI governance charter, roles, responsibilities
Establish & maintain	AI security policies and procedures
Ensure	Responsible AI use, ethics, regulation, frameworks
Participate / oversee	AI risk management lifecycle
Identify & assess	AI threat landscape
Monitor	Internal and external AI risk factors
Design & implement	AI testing and vulnerability management
Conduct	AI impact assessments, regulatory conformity
Embed & verify	AI security in vendor solutions
Design & implement	AI security architecture
Advise	Enterprise AI architecture integration
Design & review	AI security controls
Establish & maintain	AI data and asset inventory and classification
Identify & treat	AI data security risk
Establish & maintain	AI security incident investigation and reporting
Establish & maintain	AI incident handling processes
Address	AI risk in business continuity and disaster recovery
Define & monitor	AI security metrics
Review & implement	AI security tools
Conduct	Human oversight of AI outputs
Develop & maintain	AI security awareness and acceptable use
Advise	AI security risk in AI lifecycle development

ISACA Belgium Chapter 40 YEARS

AAISM ISACA Advanced in AI Security Management

ISACA A**AI**SM

Secure the Future of Enterprise AI

AAISM™ ISACA Advanced in AI Security Management™

Learn more here:

ISACA Belgium Chapter 40+ YEARS

ISACA Belgium Chapter
ACCREDITED TRAINING ORGANISATION

AAIR (Advanced in AI Risk)

Beta Edition / First Edition

AAIR™ Advanced in AI Risk™
An ISACA® Certification

Liviu Luca

CRISC & CISM ISACA accredited trainer
CISA, CISM, CRISC, CISM, CGEIT, CISSP

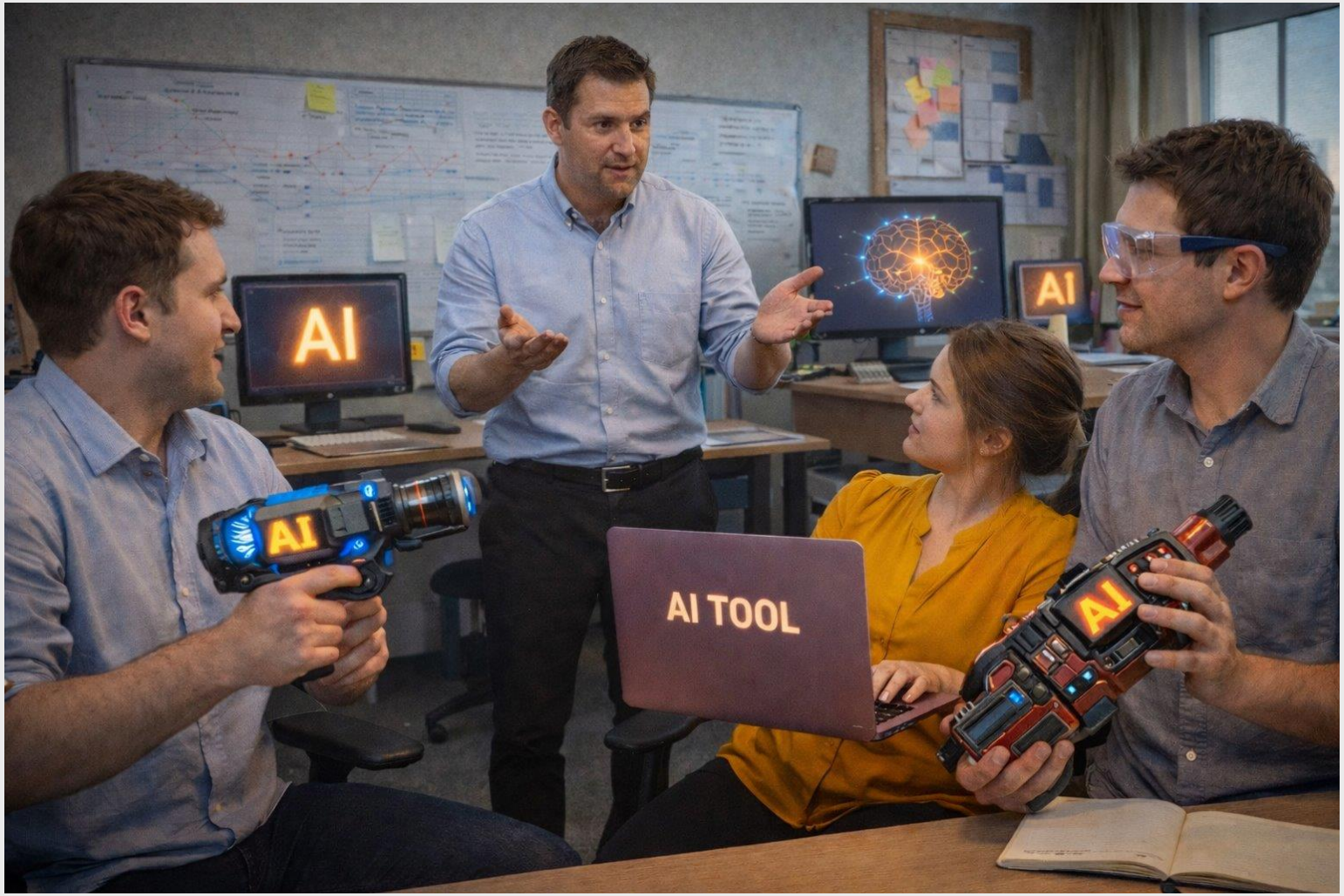
ISACA Belgium Chapter 40+ YEARS

Why AAIR?

- Governance & Operational Risks
- Security & Data Risks
- Legal & Ethical Risks
- Strategic & Financial Risks

Image generated with ChatGPT 5.2

Why AAIR?



AAIR (Advanced in AI Risk – beta program)

Target Audience: Professionals holding existing certifications such as CISA, CISM, CRISC, CGEIT, CDPSE, CISSP, or equivalent experience in IT risk and AI.

Subscription
Dec.2025

Exam Window
10th Feb - 09th March

Outcome

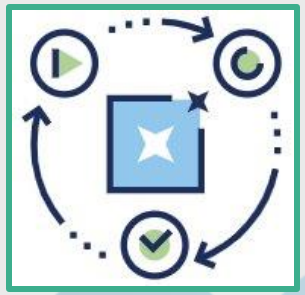
Participants can be among the first to hold this certification and help refine the final exam materials.

Full Release
Q2.2026

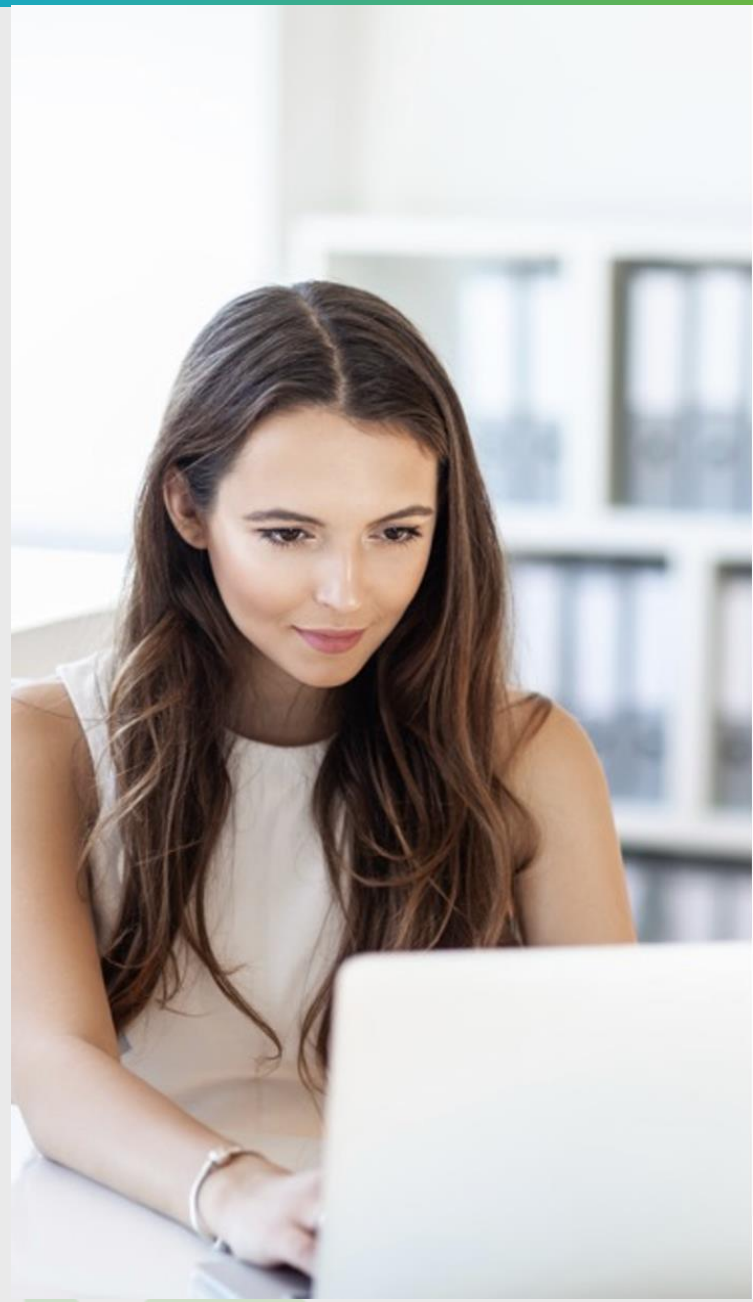
AAIR's Key Practices

AI Risk Governance and Framework Integration

AI Risk Program Management



AI Life Cycle Risk Management



Resources To Get Started (coming soon!)

AAIR Online Review Course

Coming soon! AAIR certification exam preparation online course that provides on-demand instruction and in-depth exam preparation.

AAIR Questions, Answers & Explanations Database

Coming soon! A12-month subscription to a comprehensive 200+ question pool of items. Build a custom study plan with a personalized dashboard, track progress and review previously answered questions.

AAIR Review Manual (Print/Digital Versions)

Coming soon! A comprehensive reference guide to prepare for the AAIR certification exam.

ISACA Belgium Chapter
ACCREDITED TRAINING ORGANISATION

CRISC (Certified in Information Systems Control)

8th Edition

CRISC
Certified in Risk and Information Systems Control®
An ISACA® Certification

ISACA Belgium Chapter 40+ YEARS

Liviu Luca

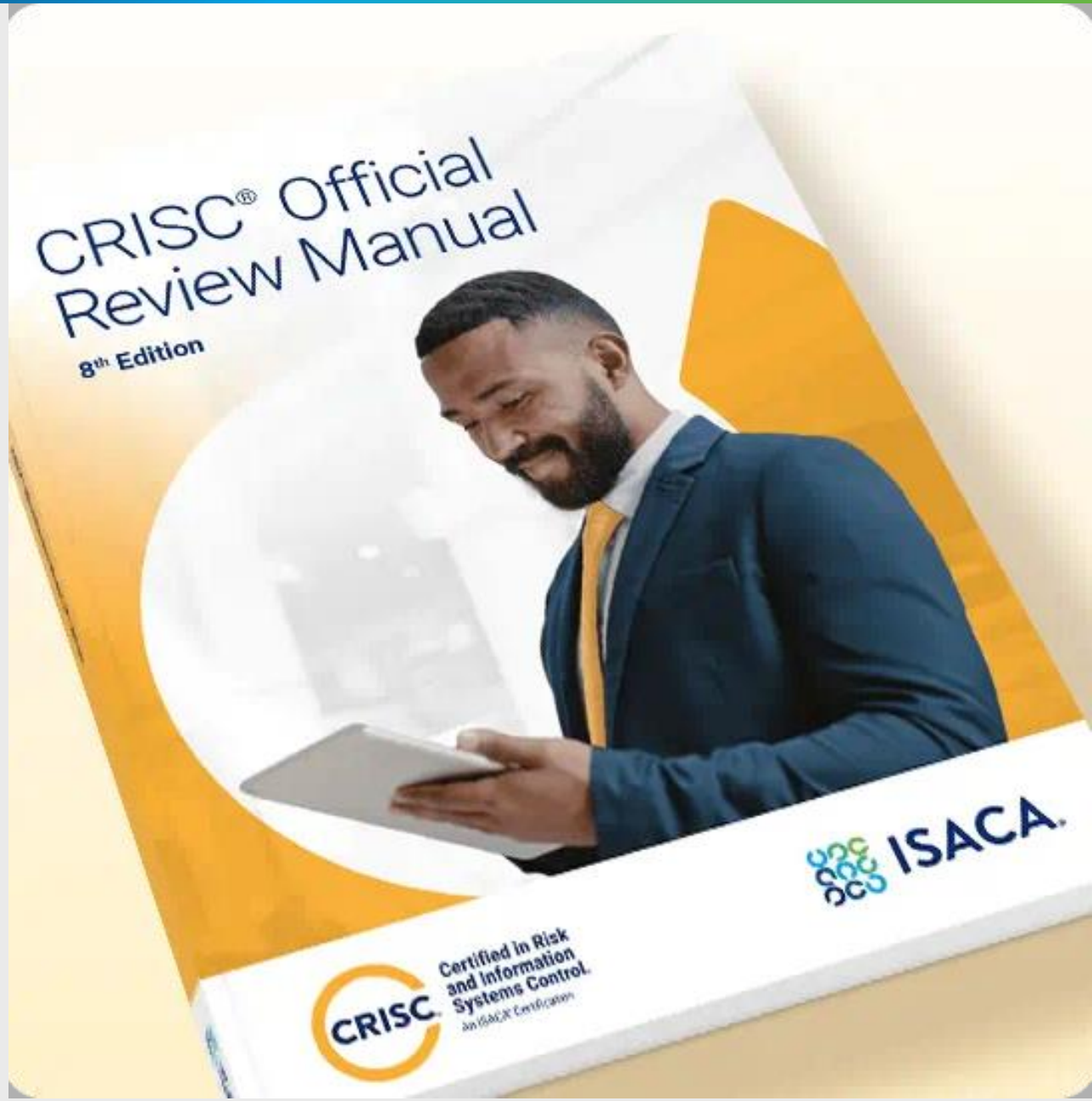
CRISC & CISM ISACA accredited trainer
CISA, CISM, CRISC, CISM, CGEIT, CISSP

CRISC Official Review Manual

8th Edition

The CRISC Official Review Manual, 8th Edition

Released in late 2025 for the updated exam effective starting with 3rd of November 2025) reflects a modernization of the risk landscape, specifically focusing on the rise of AI and the shift toward zero-trust security.



Shift in Domain Weightings

	Domain	7th Edition Weight	8th Edition Weight	Change
1	Governance	26%	26%	No change
2	Risk Assessment	20%	22%	+2%
3	Risk Response & Reporting	32%	32%	No change
4	Technology and Security	22%	20%	-2%

Major Content Additions

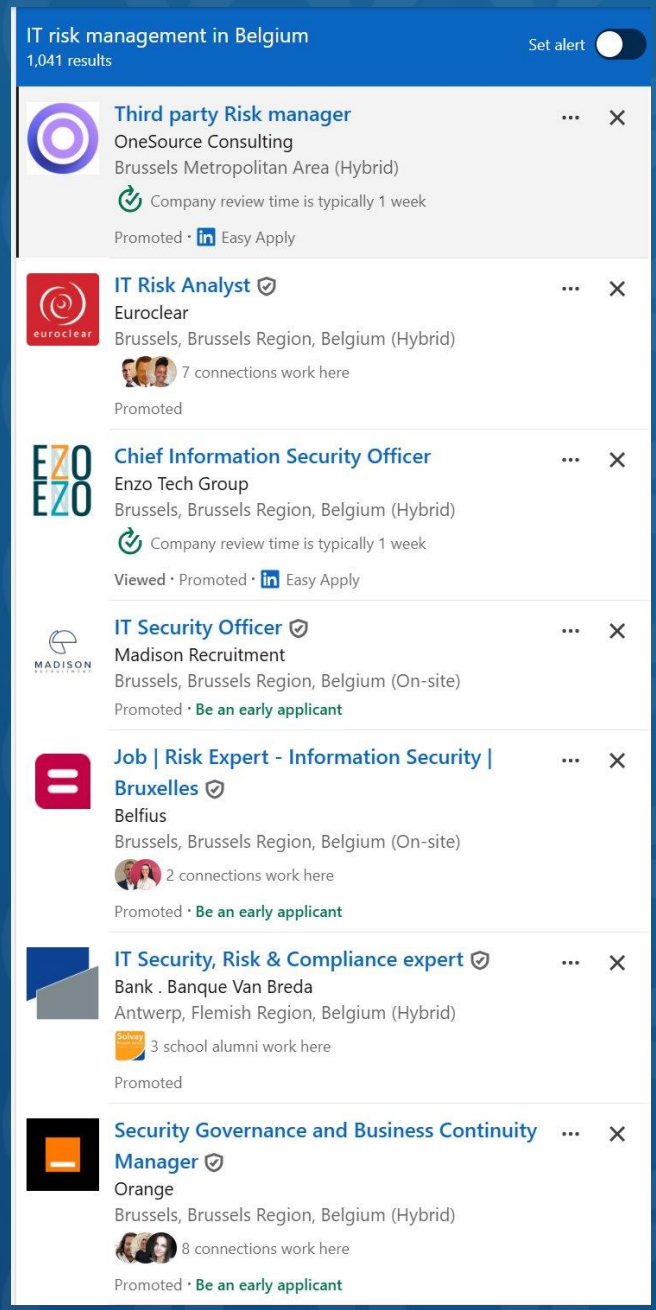
CRISC 8th Version

- Artificial Intelligence (AI) & Machine Learning (ML)
- Quantum Computing
- Zero Trust Architecture
- Business Process Resilience

Why I Would Get CRISC Certified?

1041 Job Offers

in Belgium related to IT Risks



ISACA Belgium Chapter 40 YEARS

CRISC Certified in Risk and Information Systems Control. An ISACA® Certification

Why I Would Get CRISC Certified?

- Differentiation from other pears not-certified.
- Increased trust in your risk management expertise.
- One of the criteria in call for tenders for professional services for Information/IT security / risk management services.
- Rarity of the personnel certified, in September 2025: only 120 ISACA Belgium members were CRISC certified.

ISACA CRISC

Get Ahead in Risk and Information Systems Control

CRISC®

Certified in Risk and Information Systems Control®

An ISACA® Certification

Learn more here:

ISACA Belgium Chapter 40+ YEARS

ISACA Belgium Chapter
ACCREDITED TRAINING ORGANISATION

CDPSE (Certified Data Privacy Solutions Engineer)

Third Edition

CDPSE Certified Data Privacy Solutions Engineer™
An ISACA® Certification

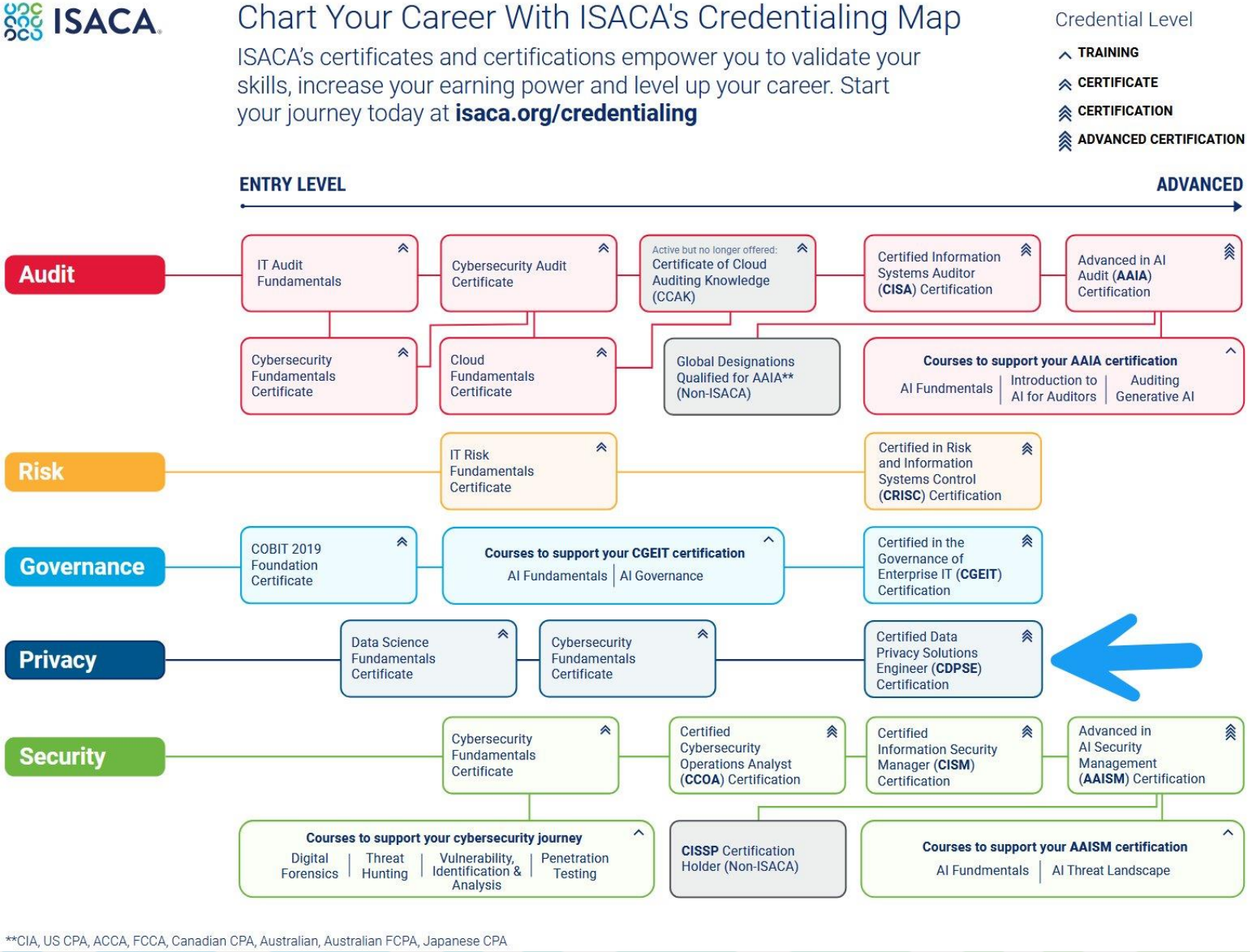
ISACA Belgium Chapter 40+ YEARS

Egide Nzabonimana

CDPSE Accredited Trainer
President, ISACA Belgium
Digital Trust Strategist / vCISO

Chart Your Career With ISACA's Credentialing Map

ISACA's certificates and certifications empower you to validate your skills, increase your earning power and level up your career. Start your journey today at **isaca.org/credentialing**



**CIA, US CPA, ACCA, FCCA, Canadian CPA, Australian, Australian FCPA, Japanese CPA

CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification

Certified Data Privacy Solutions Engineer

- Ranked as a Top Paying Certification Worldwide in Global Knowledge's 2024 Salary Survey
- Ranked #9 2024's Top Technology Certifications by *technologymagazine.com*
- 2023 Nominee for the Best Professional Certification Program Award

Prioritize privacy in today's data-driven AI Solutions

The first experience-based, technical privacy certification of its kind, the CDPSE® certification validates technology professionals' ability to implement customized privacy by design solutions into new and existing networks, platforms and products—building customer and stakeholder trust and mitigating risks of non-compliance.

Common career paths and target audience:

- Lead Software Engineer – Data and System Privacy
- Domain Architect – Legal Care Compliance, Privacy
- Security and Privacy Engineer
- Privacy Solutions Architect
- IT Project Manager
- Privacy Advisor
- Privacy Analyst
- Lead Privacy Manager

Key domains:

1. Privacy Governance
2. **Privacy Risk Management & Compliance**
3. Data Life Cycle Management
4. Privacy Engineering

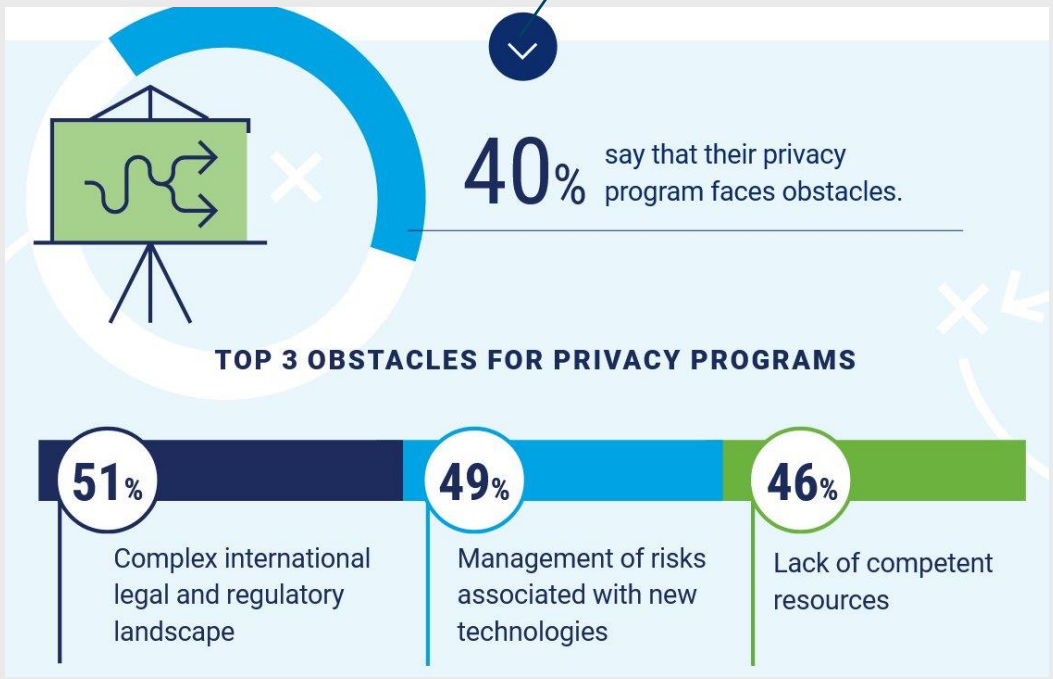
CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification

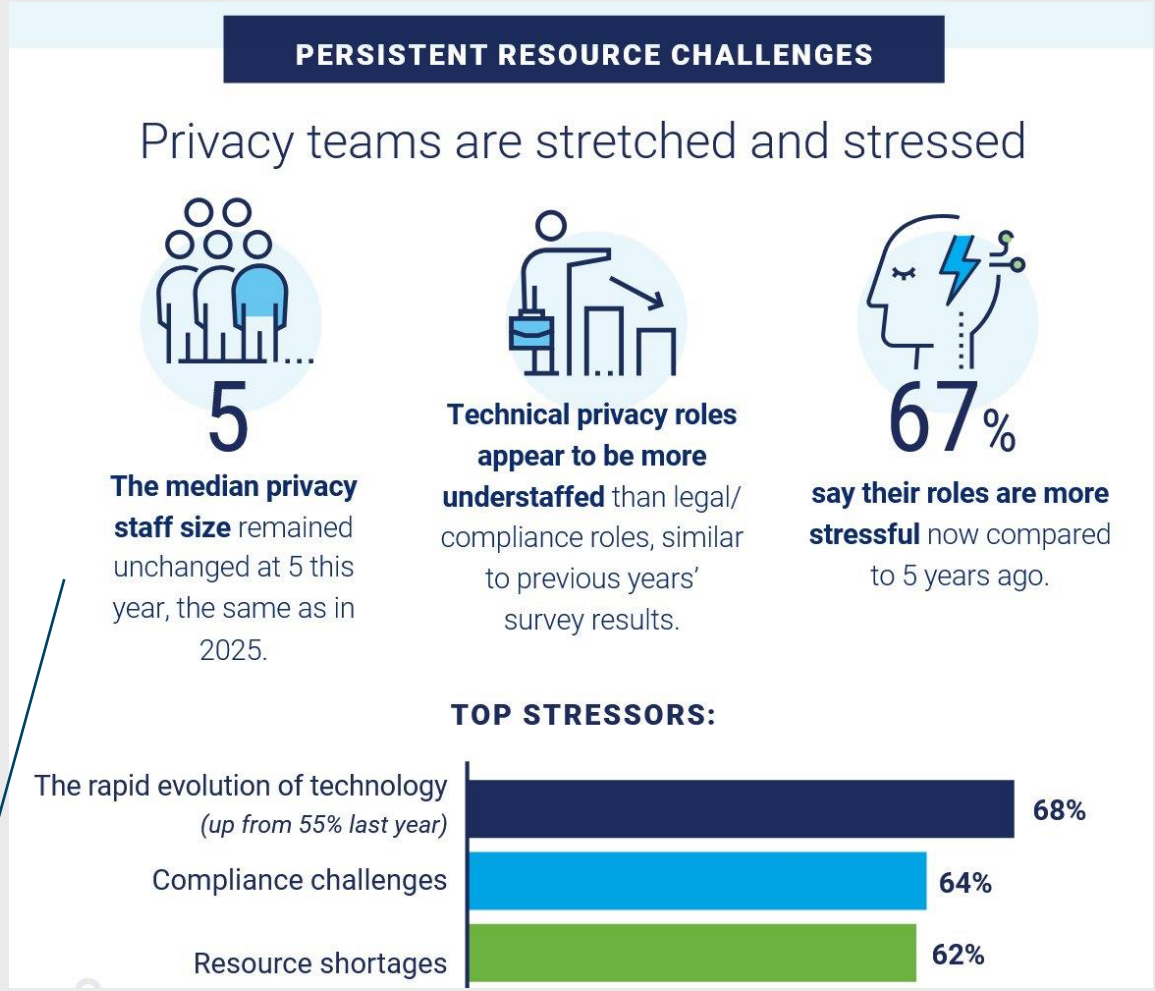
ISACA Belgium Chapter 40 YEARS

The New CDPSE Update:

Stay Relevant. Stay Credible. Deliver Privacy by Design.

Insights from more than **1,800** global privacy professionals





Including **485** in Europe

https://www.isaca.org/resources/reports/state-of-privacy-2026

Domain 1

Privacy Governance and Operations

Topics

- Personal Information
- Privacy Principles
- Privacy Laws and Regulations
- Privacy Documentation

Domain 2

Privacy Risk Management and Compliance

Topics

Domain 3

Data Life Cycle Management

Topics

Data Inventory, Dataflow Diagram, and Classification

Data Quality (e.g., Accuracy)

Data Use Limitation

Data Analytics (e.g., Aggregation, AI, Data Warehouse)

Domain 4

Privacy Engineering

Topics

- Infrastructure and Platform Technology
- Devices and Endpoints
- Connectivity
- Secure Development Life Cycle
- APIs and Cloud-Native Services

How To Request Your CPEs

Alternatively, browse to the following web page: https://forms.office.com/e/rMcdWZr0Yg
If you are unable to access the request form, please contact the event organizer

ISACA Belgium Chapter 40+ YEARS

ISACA Belgium Chapter 40+ YEARS

KPMG

To receive 1 CPE you need to register your attendance today:

1. Scan the QR Code with your mobile phone
2. Enter the following secret event key: **PRESESSION**
3. Include your registered ISACA e-mail address or your ISACA ID (one of both is required)

Keep a copy of your form as "Certificate of Attendance"

2026 Agenda

CISM Certified Information Security Manager. An ISACA® Certification	26-31 MAR IN - PERSON	14 - 17 SEPT IN - PERSON	
CISA Certified Information Systems Auditor. An ISACA® Certification	20 - 23 APR IN - PERSON	14 - 17 SEPT IN - PERSON	07 - 10 DEC IN - PERSON
CGEIT Certified in the Governance of Enterprise IT. An ISACA® Certification	14 & 24 - 26 MAR HYBRID	28 NOV & 8 - 10 DEC HYBRID	
CRISC Certified in Risk and Information Systems Control. An ISACA® Certification	19 - 22 MAY IN - PERSON	17- 22 SEPT IN - PERSON	01 - 04 DEC IN - PERSON
COBIT 2019	11 - 12 MAY IN - PERSON	07 - 08 SEPT ONLINE	03 - 04 DEC IN - PERSON

Inhouse Training from

ISACA Belgium Chapter
ACCREDITED TRAINING ORGANISATION

ISACA Belgium offers early-career and trend-focused training. For group or in-house upskilling

Get access to all trainings at a discounted price. Materials included

USE THE CODE AT CHECKOUT !

DISCOUNT COUPON

15 % OFF

CODE : NYEVENT26

SCAN ME BEFORE 15 FEBRUARY 2026!

ISACA Belgium Chapter 40+ YEARS

ISACA®

isaca.org/credentials

GET INVOLVED. STAY ENGAGED.