

# TAISE Knowledge Guide

## All About Earning Your Trusted AI Safety Expert Certificate

### Introduction to TAISE

If AI is going to shape the world, we need people who know how to shape it safely.

The [Trusted AI Safety Expert \(TAISE\)](#) certificate, created by the Cloud Security Alliance (CSA) and Northeastern University, is a rigorous, research-backed program for professionals who build, manage, or audit intelligent systems. Through 10 comprehensive modules and a final certificate exam, learners gain practical skills to evaluate and mitigate real-world AI risks, apply AI safety and security controls, navigate compliance frameworks, and lead responsible AI adoption across industries. TAISE is more than a certificate—it's a commitment to advancing safe, secure, and responsible AI.

### Receive a Respected Industry Credential

TAISE is co-issued by **CSA, the global leader in cloud security standards**, and **Northeastern University, a top academic institution for AI ethics and experiential learning**. This joint recognition enhances your professional credibility, providing a globally respected credential to highlight on resumes, LinkedIn, and professional profiles.

### Acquire In-Demand Skills

Professionals will learn to work with frameworks such as **NIST AI RMF, CSA AICM, ISO standards, and MITRE ATLAS** while mastering **threat classification, data privacy, model governance, and AI-specific incident response**. These capabilities directly map to the urgent needs of enterprises adopting AI.

## Go Beyond Theory

The **TAISE Prompt Library** transforms concepts into hands-on practice. It offers curated prompts and exercises that show learners how to use large language models to reinforce and apply safety principles from each module. While not an exam prep tool, it helps professionals **translate training into job-ready skills**.

## Who Should Pursue TAISE?

The TAISE program is applicable to a [wide variety of roles and use cases](#). **Consider earning TAISE if you intend to do any of the following:**

### Lead Responsible AI Adoption

**TAISE empowers you to lead and drive organizational change with confidence.** You'll learn AI fundamentals, governance frameworks, and communication best practices essential for your role. The curriculum covers business value assessment, legal implications, and ethical considerations—giving you the tools to build and communicate a top-down AI strategy effectively.

### Avoid the Legal and Reputational Risks of AI

**TAISE provides a clear roadmap for building and managing an AI governance program.** You'll learn to interpret regulatory frameworks, apply risk management models, and design comprehensive documentation practices. The certificate demonstrates your proficiency and commitment to AI safety, serving as a badge of honor in this critical field while providing specific tools and frameworks to protect your company from legal and reputational damage.

### Safeguard Data Privacy

**TAISE includes a dedicated module on data security and privacy in AI systems, offering the specific, practical skills you need.** You'll learn to implement data anonymization, minimization, and governance techniques while managing data access and establishing proper lineage and metadata management. Build the credibility and knowledge to establish a robust data privacy program for AI systems, protecting your organization and building customer trust.

## Address the New Generation of Security Challenges

**TAISE provides a comprehensive framework for managing AI-specific risks and threats throughout the entire AI model lifecycle.** You'll learn to classify threats, conduct risk assessments using industry frameworks, and perform periodic risk reviews. The program prepares you to proactively identify threats before they become problems while validating your ability to protect AI systems and demonstrating your preparedness for next-generation security challenges.

## Enhance Your Career Prospects

**TAISE is a practical, skills-based program that gives you tools to immediately apply security best practices.** You'll learn to secure MLOps pipelines, implement Zero Trust Architecture for AI workloads, and develop comprehensive incident response plans. The certificate enhances your career prospects by showcasing expertise in critical and rapidly growing areas of AI development while demonstrating proficiency in securing AI systems in modern IT environments.

## Getting Started with TAISE

### Purchase the TAISE Training + Exam Bundle

**The TAISE bundle is available exclusively through the [CSA Training](#) site for \$795.** It includes:

- 10 self-paced modules with a completion certificate awarded at the end
- Comprehensive study guide
- Exam token (2 attempts, valid for 2 years)
- Access to the TAISE Prompt Library
- TAISE certificate & digital badge upon passing the final exam

Your training completion certificate can be submitted for CPE credits in compliance with NASBA standards set by CPE providers.

Note that unlike other CSA programs, **there is no exam-only option** for TAISE. Future formats like instructor-led training will become available by late 2025.

## No Prerequisites Required

No prerequisites are required before you take the TAISE training and exam. A basic familiarity with AI, cloud, and cybersecurity is recommended. For foundational knowledge that will aid in your understanding of the TAISE material, consider exploring CSA's [Certificate of Cloud Security Knowledge \(CCSK\)](#) first.

## Additional Study Resources

- **TAISE Study Guide:** The Study Guide (available only with [purchase of the bundle](#)) provides structured summaries and review exercises to reinforce learning.
- **Sample Questions:** Review the list of Sample Questions in the [TAISE Prep Kit](#) to see if you're ready to take the final exam.
- **CSA Research Publications:** Relevant AI, governance, and security publications are included in the 'Additional Resources' list in the [TAISE Prep Kit](#).

## Train Your Team

CSA offers team training deals based on TAISE so that you can give your staff the foundational knowledge they need to safely adopt AI systems. While any organization can take advantage of CSA team training opportunities, **CSA corporate members receive volume-based discounts on team training.** To verify your organization's membership status and see if you qualify for discounted team training, contact [teamtraining@cloudsecurityalliance.org](mailto:teamtraining@cloudsecurityalliance.org).

# Topics Covered in TAISE

## Module 1: Introduction to AI

Provides foundational knowledge of AI concepts, modalities, and their historical evolution.

## Module 2: Generative AI Architecture & Design

Explores the technical components, training methods, and deployment considerations of generative AI.

## **Module 3: AI Use Cases: GenAI, Multimodal & AI Agents**

Examines real-world applications of generative AI across industries while addressing ethical implications such as deepfakes, misinformation, and bias.

## **Module 4: Ethics, Transparency, & Explainability in AI**

Introduces key ethical principles and practical explainability methods to promote fairness, accountability, and transparency in AI systems.

## **Module 5: AI Model Lifecycle & Threat Taxonomy**

Covers the end-to-end AI model lifecycle and common threats, providing frameworks for risk assessment, monitoring, and ongoing security.

## **Module 6: Governance, Risk Management, & Compliance**

Focuses on governance structures, regulatory frameworks, and compliance models for managing AI systems responsibly at the organizational level.

## **Module 7: Introduction to AI Safety & Security**

Differentiates between AI safety and AI security, highlighting the unique challenges of securing GenAI.

## **Module 8: Cloud & AI Security**

Details cloud security fundamentals for AI, including deployment strategies, monitoring, Zero Trust, and incident response planning.

## Module 9: Data Security & Privacy in AI Systems

Explains techniques for ensuring data quality, privacy, and governance in AI systems, with a focus on authenticity, minimization, and secure handling.

## Module 10: Continuous Learning & Adaptation

Emphasizes ongoing monitoring, feedback loops, and MLSecOps practices to keep AI systems accurate, resilient, and safe over time.

For the full curriculum overview, check out the Curriculum guide in the [TAISE Prep Kit](#).

## TAISE Exam Structure

- **Environment:** Online, open-book, unproctored
- **Questions:** 60 multiple-choice questions (6 per module)
- **Time Limit:** 120 minutes
- **Passing Score:** 80%
- **Attempts:** 2 included with the training + exam bundle (valid for 2 years)

## After Passing the TAISE Exam

**Submit Your Continuing Education Credits:** Although there are currently no official CPE designations for any of CSA's training courses, we do issue a certificate of completion with a stated number of hours. You can then use this certificate of completion for CPE credit submission.

**Claim Your Digital Badge:** A TAISE digital badge is issued upon successful completion of the exam. Leverage the badge on your social media channels and resume to showcase your AI safety expertise.

**Join an AI Safety Working Group:** After earning your TAISE, start applying your knowledge by volunteering for one of CSA's [AI Working Groups](#). Working Group volunteers have the opportunity to contribute to and author research publications, and elevate their professional profile by receiving recognition across CSA's promotional channels.

# Contribute to the Future of the Industry

CSA maintains a [tiered donation initiative](#) to assist in the accessibility of TAISE. **Your support will help us fund training development, as well as enabling donation-based [global nonprofit access](#).**

There are 3 donation tiers with different associated benefits:

	Supporter	Benefactor	Corporate Patron
Donation Amount	\$1+	\$5,000	\$6,000
Who Should Donate to This Tier	Early-career professionals and students looking to build credibility	Senior leaders who want to give back, shape the future of AI safety, and champion the next generation	Organizations that want to support free AI safety education, while also training their teams on core AI safety principles
Benefits	<p>Social media graphic to showcase your support</p> <p>Recognition on our <a href="#">Thank You Wall</a> with a link to your LinkedIn profile</p>	<p>Social media graphic to showcase your support</p> <p>Recognition on our <a href="#">Thank You Wall</a> with a link to your LinkedIn profile, headshot, and short bio</p> <p>Token for the TAISE online training and exam</p> <p>Donation of 15 extra TAISE bundles in your name to <a href="#">nonprofits</a> (501c3) of your choice</p> <p>"Benefactor" certificate to display on LinkedIn</p> <p>LinkedIn shoutout from CSA's CEO or President</p> <p>Spotlight in one CSA newsletter</p> <p>Opportunity to publish one thought leadership article on CSA's blog</p> <p>Early visibility into new TAISE course modules</p>	<p>Social media graphic to showcase your support</p> <p>Recognition at the top of our <a href="#">Thank You Wall</a> with a link to your organization's LinkedIn corporate page, logo, and bio</p> <p>5 tokens for the TAISE online training and exam</p> <p>Donation of 10 extra TAISE bundles in your name to <a href="#">nonprofits</a> (501c3) of your choice</p> <p>Recognition in TAISE fundraiser campaigns through email and social media for 1 year</p> <p>LinkedIn shoutout from CSA's CEO or President</p> <p>Spotlight in one CSA AI newsletter</p> <p>Feature in a blog after one staff member has earned TAISE</p>

**Fill out the form to make a donation.** Upon submitting, you will be redirected to view your listing on our [Thank You Wall](#). You will also receive an email with further information about your benefits.

# Related CSA Certificates and Trainings

## Certificates

### Certificate of Cloud Security Knowledge (CCSK)

The [CCSK](#) is highly regarded as the benchmark for cloud security expertise. It provides a comprehensive and unbiased understanding of how to effectively secure data in the cloud. Learn how to develop a security program that meets international standards and addresses principles of Zero Trust, DevSecOps, cloud telemetry and security analytics, AI, and more.

### Certificate of Competence of Zero Trust (CCZT)

The [CCZT](#) is the authoritative Zero Trust training and certificate that delivers the knowledge needed to understand the core concepts of Zero Trust. Developed by CSA, the trusted industry leader for cloud security certificates, the CCZT builds knowledge to drive the definition, implementation and management of Zero Trust over time.

## Trainings

### Cloud Infrastructure Security

Focusing on fundamental areas of cloud computing such as Top Threats, Cloud Key Management, Microservices and Containers, DevSecOps and more, the [Cloud Infrastructure Security](#) courses are designed to be succinct, short-form courses composed of up to several units each and a five-question knowledge check at the end.

### STAR Lead Auditor

The [STAR Lead Auditor](#) training is a self-paced course designed to help assessors, service providers, and consultants better manage the security of cloud services, as well as provide the credentials necessary to become a qualified STAR Auditor. This course equips individuals with the skills and knowledge required to audit cloud service providers (CSPs) against the STAR Certification scheme.



# What the Industry is Saying About TAISE

*"The course's depth and architecture, as well as its proactive approach, are particularly forward-looking. The course equips professionals with essential technical knowledge on the ethics of AI, allowing practitioners to utilize best practices in the field. CSA's remarkable global standing and commitment to world-class standards make TAISE invaluable to professionals aspiring to advance in AI governance and safety."*

- Elastos Chimwanda, Founder & CEO, Cyber Defence Consultancy

*"TAISE helps separate the noise from the substance to make sure no time is wasted, and those responsible for securing enterprises hit the ground running and understand the risk that their organizations can be exposed to."*

- Roger Ofarril, Information Security Architecture & Engineering Manager, Federal Reserve Bank of Chicago

*"The program offers comprehensive coverage, not only on Model Governance, Risk Management, and Compliance, but also on AI Security and Threat Analysis, AI Risk Assessment, and the responsible use of AI. I highly recommend this course to security professionals seeking to enhance or validate their expertise in AI security."*

- Henry Hon, Senior Lead Security Professional, Lumen Technologies

*"The way I see it, TAISE is a movement disguised as a credential. At its core, it is about shaping leaders who treat AI Safety as non-negotiable. What's more, it gives you the confidence to lead AI with both vision and responsibility."*

- Goutama Bachtiar, Global Advisory Board, EC-Council

*"The material is clearly designed with practitioners in mind, offering both a strong foundational understanding and practical takeaways that can be applied immediately in the workplace."*

- Aby Rao, Deputy CISO, Paylocity

*"The TAISE program provides an exemplary model for how industry organizations can harness collective knowledge to address complex, evolving challenges in cybersecurity."*

- Cecil Su, Director of Cybersecurity, BDO LLP

# Begin Your TAISE Journey Today

The [Trusted AI Safety Expert \(TAISE\)](#) certificate program will help you ensure the safe, secure, and responsible development and deployment of AI systems. Take advantage of the combined expertise of CSA and Northeastern University to go beyond theory and immerse yourself in real-world strategies for addressing AI risks. Upon completion of the program, showcase an industry-leading credential that validates your AI safety knowledge and immediately begin leveraging your newfound expertise across the AI lifecycle.

**So... are you ready to [become a Trusted AI Safety Expert](#)?**