AI CERTs®

Executive Summary

Certification



TABLE OF CONTENTS

Introduction 1
Certification Prerequisites 1
Who Should Enroll? 2
Certification Goals and Learning Outcomes 2
The Impact of AI on Modern AI Security Compliance Strategies 2
What Is Next for AI? 4
How AI Can Transform Practices in Security Compliance Operations 4
How AI Can Address the Current Challenges in Security Compliance Practices 5
How Industries Are Adopting AI to Transform Security Compliance Practices 6
How to Integrate AI into Security Compliance Practices 7
Module 1: Foundations of AI-Enabled Security Compliance 8
Module 2: Using AI to Interpret Security Standards and Requirements 8
Module 3: AI-Assisted Security Risk and Compliance Gap Assessment 8
Module 4: AI for Security Policy and Procedure Management 9
Module 5: AI for Control Implementation and Evidence Management 9
Module 6: AI for Third-Party Security Compliance 9
Module 7: AI for Compliance Monitoring, Incident Management, and Auditing 10
Module 8: AI-Powered Security Compliance Program and Capstone 10
How Can AI CERTs Help Build an AI-Ready Culture? 10

Copyright© 2026. All rights reserved

Introduction

The AI+ Security Compliance Practitioner certification provides a comprehensive foundation in managing security, regulatory, privacy, and governance requirements across artificial intelligence, machine learning, generative AI, and enterprise knowledge systems. It is designed for learners who want to understand how to interpret AI-related regulations, develop compliance controls, assess security risks, document evidence, conduct audits, and maintainaccountability throughout the complete AI system lifecycle.

Throughout the certification, learners explore AI compliance roles and responsibilities, regulatory frameworks, risk assessments, security policies, data privacy, access controls, model governance, third-party risk, incident reporting, audit readiness, control testing, RAG compliance, sensitive information protection, documentation, monitoring, and continuous improvement. The course combines conceptual learning, industry frameworks, practical examples, case studies, compliance review exercises, and applied use cases to help learners design, evaluate, document, and maintain secure and compliant AI systems effectively.
This certification covers the following topics:

- Foundations of AI-Enabled Security Compliance
- Using AI to Interpret Security Standards and Requirements
- AI-Assisted Security Risk and Compliance Gap Assessment
- AI for Security Policy and Procedure Management
- AI for Control Implementation and Evidence Management
- AI for Third-Party Security Compliance
- AI for Compliance Monitoring, Incident Management, and Auditing
- AI-Powered Security Compliance Program and Capstone

Certification Prerequisites

- **Cybersecurity and Compliance Fundamentals:** Learners should understand basic security concepts, threats, vulnerabilities, access controls, policies, and compliance requirements.
- **AI and ML Awareness:** Basic familiarity with artificial intelligence, machine learning, and generative AI concepts is recommended.
- **Regulatory and Risk Awareness:** An introductory understanding of regulations, risk management, governance, and audit processes can support learning.
- **Data Privacy and Protection Basics:** Basic knowledge of data classification, privacy principles, sensitive information handling, and protection controls will be helpful.
- **Responsible Compliance Mindset:** Learners should value secure, ethical, transparent, accountable, and compliant AI development and use.

Copyright© 2026. All rights reserved

Who Should Enroll?

- **Cybersecurity and Compliance Professionals:** Individuals seeking to develop expertise in securing AI systems while meeting regulatory, privacy, governance, and industry compliance requirements.
- **Security Engineers and Architects:** Professionals responsible for designing compliant AI applications, security controls, data flows, access mechanisms, and cloud environments.
- **Risk, Governance, and Audit Professionals:** Individuals involved in AI risk assessments, control evaluations, internal audits, regulatory reviews, and governance activities.
- **Application, Cloud, and ML Professionals:** Developers, Develops engineers, cloud specialists, and ML engineers supporting secure and compliant AI development and deployment.
- **Privacy, Legal, and Responsible AI Teams:** Professionals responsible for data protection, policy interpretation, regulatory alignment, accountability, and responsible AI adoption.

Certification Goals and Learning Outcomes

- **Understand AI Security Compliance Fundamentals:** Explain AI compliance concepts, regulatory responsibilities, governance structures, security obligations, and the relationship between cybersecurity, privacy, ethics, and responsible AI.
- **Assess AI Compliance Risks**: Identify regulatory requirements, compliance gaps, security risks, data protection concerns, control weaknesses, and accountability requirements across AI systems and business processes.
- **Apply Security and Compliance Controls:** Implement policies, access controls, data protection measures, documentation practices, monitoring mechanisms, and governance controls across AI and GenAI applications.
- **Evaluate AI Systems for Compliance:** Assess AI applications for privacy risks, unauthorized access, sensitive information disclosure, bias, unsafe outputs, weak oversight, and non-compliance with applicable standards.
- **Manage AI Compliance Across the Lifecycle:** Support compliant design, development, deployment, monitoring, incident management, auditing, third-party oversight, and retirement of AI systems.

The Impact of AI on Modern AI Security Compliance Strategies

Over the past decade, artificial intelligence and cloud computing have accelerated innovation, economic growth, and the transformation of security compliance. According to a recent MarketsandMarkets™ report, the global AI market is estimated at $601.93 billion in 2026 and is expected to grow at a CAGR of 29.3% from 2026 to 2033. The revenue is predicted to reach $3638.08 billion by 2033. (Source: MarketsandMarkets). This growth reflects the expanding use of AI across education, healthcare, finance, retail, transportation, cybersecurity, and workplace productivity.

Copyright© 2026. All rights reserved

AI adoption is increasing worldwide. The United States is the leader with a 30.19% market share, followed by the Asia-Pacific region at 23.34%. Europe holds 19.62%, and Saudi Arabia accounts for 4.87%, indicating how AI is developing regionally (Source: MarketsandMarkets), highlighting continued investment in digital transformation, cybersecurity, risk management, and regulatory compliance.

The integration of AI and cloud technologies has changed how organizations detect threats, assess vulnerabilities, protect sensitive data, monitor controls, and respond to incidents. Modern platforms provide automated threat detection, continuous compliance monitoring, scalable security analytics, anomaly detection, intelligent alert prioritization, and faster incident response. These capabilities help teams analyze larger data volumes, identify emerging risks, improve security coverage, and support timely decisions.

For AI+ Security Compliance Practitioner learners, understanding these developments is essential. Professionals must understand AI architecture, threat modelling, prompt injection, generative AI security, RAG security, data protection, model security, adversarial attacks, compliance requirements, control assessment, and audit evidence. Human expertise remains critical for validating AI outputs, investigating findings, protecting confidential information, assessing control effectiveness, and ensuring AI systems align with organizational goals, regulatory requirements, and responsible practices.

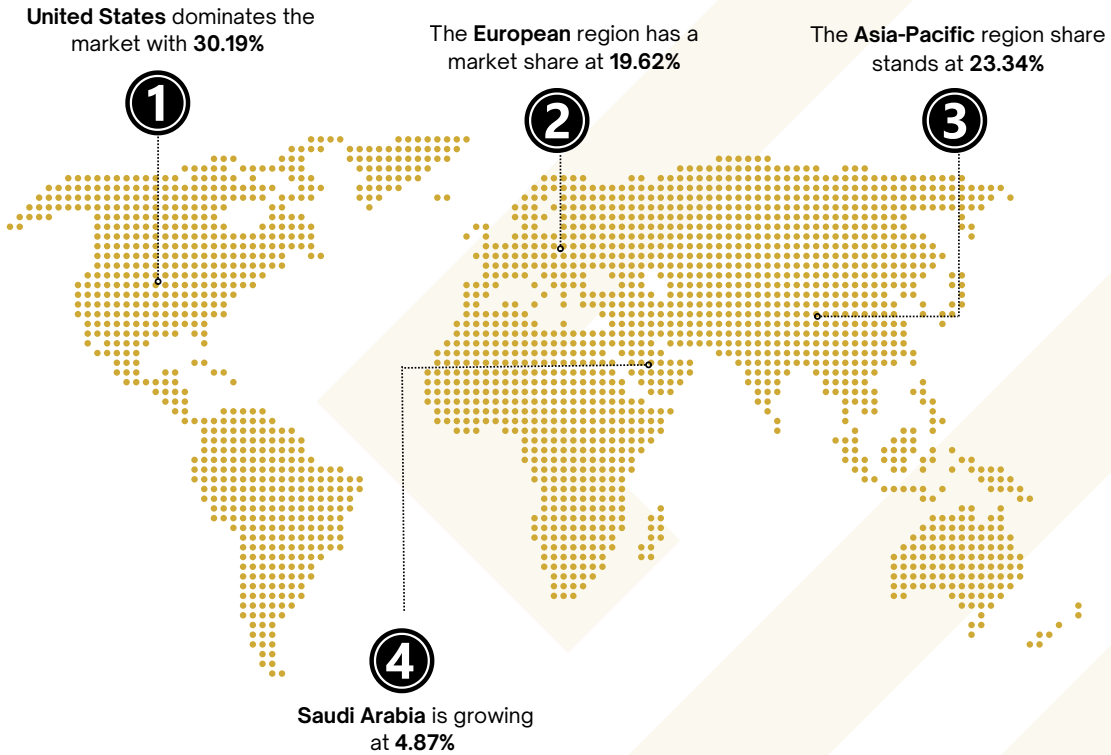


Figure 1: AI Global Market Share
Source: MarketsandMarkets

Copyright© 2026. All rights reserved

What is Next for AI?

As artificial intelligence continues to evolve, it is becoming more integrated, regulated, and embedded across modern enterprise systems. Advances in generative AI, retrieval-augmented generation, intelligent agents, cloud infrastructure, behavioural analytics, automated governance, and compliance monitoring help organizations assess risks, enforce policies, protect sensitive information, document decisions, and demonstrate adherence to regulatory requirements. For learners completing the AI+ Security Compliance certification, understanding these developments builds a strong foundation for managing AI security, privacy, governance, risk, and compliance across the system lifecycle.

Looking ahead, AI security compliance will increasingly emphasize secure-by-design development, continuous control monitoring, regulatory alignment, Zero Trust principles, access-aware data handling, model transparency, auditability, and responsible AI governance. Organizations will use AI-powered compliance assistants, automated assessment tools, policy enforcement systems, and real-time monitoring to identify data leakage, unauthorized access, model manipulation, privacy violations, control gaps, and regulatory risks. Human expertise will remain essential for interpreting regulations, validating compliance evidence, assessing business impact, protecting confidential information, overseeing AI decisions, and maintaining accountability. The certification prepares learners to manage AI compliance responsibly, strengthen enterprise controls, support informed risk decisions, and contribute confidently to secure and trustworthy AI adoption worldwide.

How AI Can Transform Practices in Security Compliance

AI is poised to transform cybersecurity compliance by enhancing its efficiency and effectiveness. It paves the way for the development of innovative compliance frameworks and automated solutions, expanding the possibilities within the field.

Here's how AI is set to revolutionize cybersecurity compliance:

Copyright© 2026. All rights reserved



Fig. 2: How AI Can Transform Security Compliance Operations

How AI Can Address the Current Challenges in Security Compliance Practices

AI technologies are transforming how security and compliance teams monitor controls, assess risks, analyse regulatory data, protect AI applications, prepare audit evidence, and respond to emerging compliance concerns. The AI+ Security Compliance certification introduces practical ways AI-powered tools, intelligent automation, governance frameworks, secure design practices, and continuous monitoring help organizations overcome modern challenges across generative AI, RAG systems, cloud environments, data pipelines, models, and machine learning workflows. These capabilities improve compliance visibility, assessment speed, control coverage, consistency, audit readiness, and decision-making.

Copyright© 2026. All rights reserved

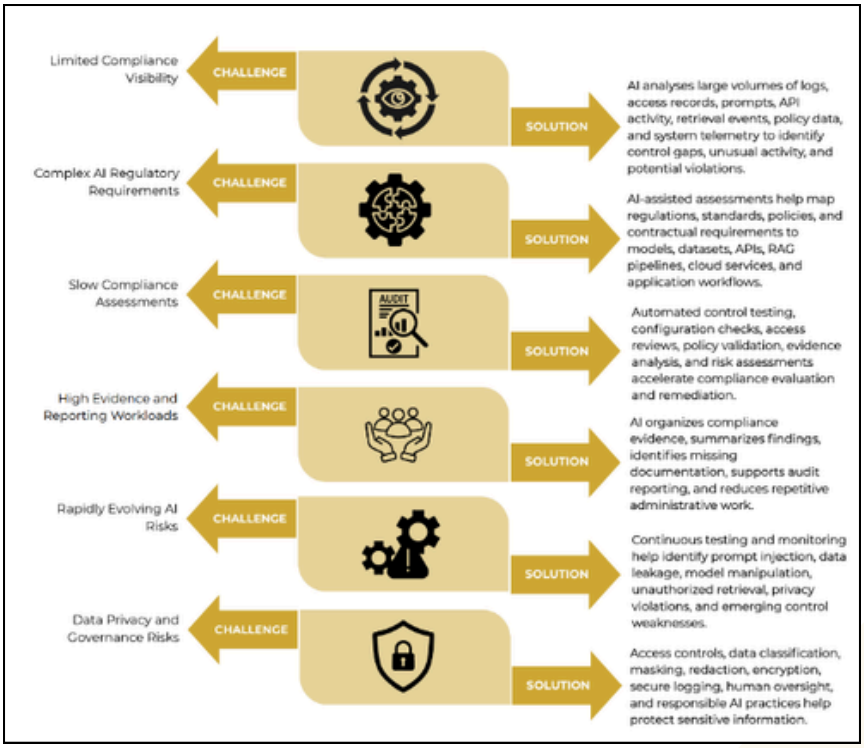


Fig. 3: How AI Addresses Common AI Security Compliance Challenges

How Industries Are Adopting AI to Transform Security Compliance Practices

Organizations across industries are increasingly adopting AI to strengthen compliance monitoring, regulatory assessments, control testing, audit readiness, risk management, and the governance of AI-enabled systems. By using AI-powered compliance tools, businesses can analyse large volumes of logs, policies, access records, regulatory requirements, and control evidence, automate repetitive compliance checks, identify control gaps, detect unusual activity, assess emerging risks, and support continuous monitoring. Security and compliance teams are applying AI across finance, healthcare, banking, retail, manufacturing, technology, government, and enterprise operations. These capabilities help professionals map regulatory requirements, prioritize high-risk findings, identify unauthorized access and data exposure, assess privacy and model risks, validate compliance evidence, prepare reports, and respond to control deficiencies more efficiently.

At the same time, responsible adoption requires organizations to protect datasets, models, prompts, APIs, vector stores, compliance records, and ML pipelines, validate AI-generated findings, maintain human oversight, and implement effective access controls, documentation, and governance. Through practical and responsible implementation, AI is helping security compliance teams improve regulatory alignment, expand control visibility, strengthen audit readiness, maintain operational resilience, and adapt to increasingly complex AI-driven environments.

Copyright© 2026. All rights reserved

How to Integrate AI into Security Compliance Practices

To successfully integrate AI into security compliance operations, a structured and responsible approach is essential. Security and compliance teams need to identify suitable use cases, prepare reliable compliance data, select appropriate AI tools, implement secure governance frameworks, monitor AI performance, and maintain human oversight throughout the AI lifecycle. This ensures that AI-powered compliance solutions improve control monitoring, strengthen risk assessment, accelerate audit activities, and protect AI systems while maintaining confidentiality, integrity, transparency, accountability, regulatory alignment, and operational resilience.

Below are the key steps to integrate AI into security compliance practices:



Figure 4: Key Steps to Integrate AI into AI Security Compliance Practices

By following these steps, AI can be integrated effectively into modern security compliance functions. The AI+ Security Compliance Practitioner certification helps learners build the knowledge and practical skills required to govern AI applications, protect sensitive data, monitor controls, evaluate AI-related compliance risks, support informed decisions, maintain audit readiness, and adapt confidently to increasingly complex regulatory and AI-enabled environments.

Copyright© 2026. All rights reserved

Module 1: Foundations of AI-Enabled Security Compliance

Understanding the foundations of AI-enabled security compliance is essential for connecting cybersecurity practices with governance, risk, controls, evidence, and regulatory obligations. It helps professionals use AI responsibly while maintaining accountability, confidentiality, and human oversight.

You will learn the fundamentals of security compliance, AI, generative AI, large language models, AI assistants, and AI agents. You will also explore prompting, requirement interpretation, risk identification, evidence review, monitoring, reporting, audit support, and the creation of an AI-assisted compliance baseline.

Module 2: Using AI to Interpret Security Standards and Requirements

Understanding security standards and requirements is essential for accurately identifying an organization's obligations and translating them into practical controls. AI can simplify complex documents, but its interpretations must remain traceable to authoritative sources and validated by experts.

You will learn to summarize requirements, extract obligations, determine applicability, generate assessment questions, and map requirements to controls, evidence, risks, and owners. You will also compare frameworks, identify missing or conflicting mappings, and create an AI-assisted compliance requirements matrix.

Module 3: AI-Assisted Security Risk and Compliance Gap Assessment

Understanding security risks and compliance gaps is essential for identifying what could harm an organization, why weaknesses exist, and which issues require immediate attention. It supports informed risk-treatment decisions and ensures remediation efforts focus on the most significant exposures.

You will learn to assess assets, threats, vulnerabilities, likelihood, impact, inherent risk, and residual risk using AI. You will also create risk statements, score risks, identify compliance gaps, analyze root causes, prioritize remediation, and develop risk registers, gap matrices, and heat maps.

Copyright© 2026. All rights reserved

Module 4: AI for Security Policy and Procedure Management

Understanding security policies and procedures is essential for converting organizational expectations and external obligations into clear, approved, and actionable instructions. Effective documentation strengthens accountability, consistent control implementation, employee awareness, and audit readiness.

You will learn to use AI to draft, review, update, and simplify security policies and procedures. You will also examine document hierarchy, ownership, lifecycle management, clause validation, version control, approval workflows, control translation, exception tracking, and compliance monitoring.

Module 5: AI for Control Implementation and Evidence Management

Understanding control implementation and evidence management is essential for proving that security requirements are operating effectively, not merely documented. Well-designed controls and reliable evidence reduce risk, strengthen assessments, and support successful audits.

You will learn to define control objectives, scope, ownership, frequency, procedures, maturity, and test criteria. You will also use AI to map risks to controls, review control effectiveness, classify evidence, assess evidence quality, identify deficiencies, and build control and evidence matrices.

Module 6: AI for Third-Party Security Compliance

Understanding third-party security compliance is essential because vendors, cloud providers, contractors, and business partners can expose organizations to data, operational, contractual, and regulatory risks. Effective oversight helps organizations manage these risks throughout the vendor relationship.

You will learn to classify third parties, conduct risk-based assessments, generate questionnaires, review vendor responses, analyze assurance documents, and calculate risk scores using AI. You will also monitor certifications, contractual obligations, remediation actions, alerts, and vendor approval decisions

Copyright© 2026. All rights reserved

Module 7: AI for Compliance Monitoring, Incident Management, and Auditing

Understanding continuous compliance monitoring, incident management, and auditing is essential for detecting control failures before they become serious regulatory or security issues. AI provides timely visibility, reduces manual effort, and helps organizations remain prepared for incidents and audits.

You will learn to monitor compliance indicators and security controls, analyze trends, create dashboards, and generate intelligent alerts. You will also use AI for incident triage, compliance impact analysis, documentation, audit planning, evidence analysis, audit findings, reporting, and follow-up.

Module 8: AI-Powered Security Compliance Program and Capstone

Understanding how to build an AI-powered security compliance program is essential for moving from isolated AI activities to a coordinated, governed, and continuously monitored enterprise approach. It helps organizations improve regulatory adherence, operational efficiency, risk visibility, and audit readiness.

You will learn to establish an AI-enabled compliance program, define governance and responsibility models, select appropriate AI solutions, and develop a transformation roadmap. You will also explore compliance AI agents, output validation, auditability, performance measurement, control towers, and the development of an end-to-end AI-powered compliance program.

How Can AI CERTs Help Build an AI-Ready Culture?

AI technologies bring significant advantages, but companies often encounter challenges like skill shortages, data complexity, and integration hurdles during adoption. At AI CERTs, we recognize these challenges and have developed our certifications to assist organizations in successfully addressing these obstacles.

Copyright© 2026. All rights reserved

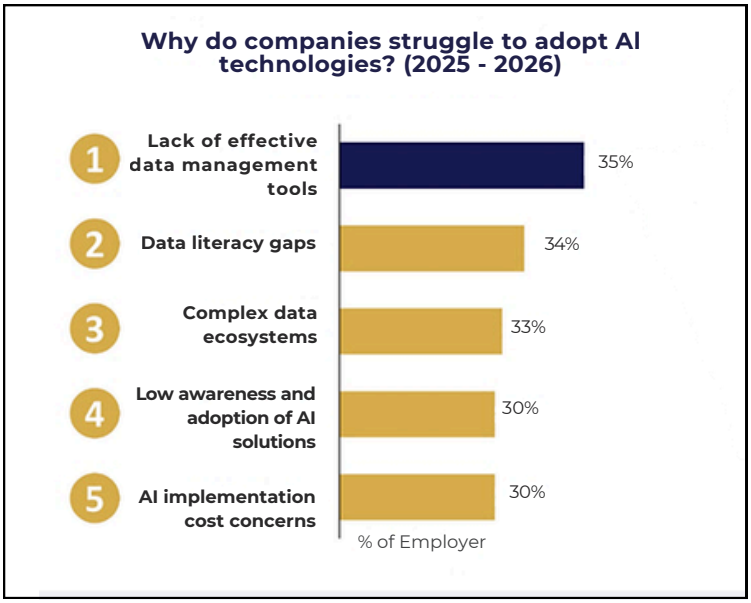


Figure 5: Factors Determining the Lack of Adopting AI Technologies
Source: Precisely, State of Data Integrity and AI Readiness Study 2026

Bridging the AI Skill Gap

- **Challenge:** As artificial intelligence becomes increasingly integrated into enterprise systems, cloud environments, business processes, security operations, and automated workflows, compliance professionals need a clear understanding of AI-related regulations, governance requirements, control obligations, privacy risks, audit expectations, and responsible AI practices. However, many professionals lack the practical knowledge required to interpret complex security standards, assess compliance gaps, manage AI-related risks, evaluate control effectiveness, maintain audit evidence, monitor third parties, and support continuous compliance across the AI lifecycle.
- **Solution:** The AI+ Security Compliance Practitioner certification provides practical knowledge of AI-enabled security compliance foundations, regulatory interpretation, risk and gap assessment, policy and procedure management, control implementation, evidence management, third-party compliance, continuous monitoring, incident management, and auditing. It enables professionals to use AI responsibly to analyse requirements, map controls, identifycompliance gaps, organize evidence, support audits, monitor risks, and strengthen governance using recognized frameworks, structured methodologies, and human oversight.
- **Benefit:** This certification equips security, risk, audit, governance, privacy, and compliance professionals with the skills and confidence to manage AI-related compliance requirements across applications, data, models, vendors, and enterprise processes. It strengthens regulatory interpretation, control assessment, evidence-based decision-making, audit readiness, risk monitoring, incident response, and cross-functional accountability. It helps bridge the gap between traditional security compliance and AI-enabled governance, preparing professionals to manage increasingly complex regulatory and technology environments responsibly.

Copyright© 2026. All rights reserved

Empowering Security Professionals with AI Skills

- **Challenge:** Organizations often find it difficult to adopt AI effectively while maintaining security, privacy, regulatory alignment, control effectiveness, audit readiness, and operational resilience. Many security and compliance professionals lack practical knowledge of AI governance, regulatory interpretation, risk assessment, control mapping, policy management, evidence validation, third-party oversight, and continuous compliance monitoring, limiting their ability to manage modern AI-enabled environments responsibly.
- **Solution:** The AI+ Security Compliance Practitioner certification provides practical training in AI-enabled compliance foundations, interpretation of security standards, risk and compliance gap assessment, policy and procedure management, control implementation, evidence management, third-party security compliance, incident management, continuous monitoring, and auditing. It helps learners use AI-powered tools responsibly to analyse requirements, evaluate controls, identify gaps, organize evidence, support audits, and strengthen compliance processes throughout the AI lifecycle.
- **Benefit:** With practical AI security compliance knowledge, learners can improve regulatory interpretation, strengthen control assessments, protect sensitive information, manage compliance evidence, evaluate third-party risks, support incident investigations, and maintain audit readiness. This empowers security, governance, risk, privacy, and compliance professionals to lead responsible AI initiatives, strengthen organizational accountability, and adapt confidently to increasingly complex regulatory and AI-enabled enterprise environments.

At AI CERTs, we offer a strategic solution, fostering a culture primed for AI integration and innovation. Our AI certification delivers in-depth training and industry-recognized credentials, equipping your workforce with the skills needed to drive your organization toward an AI-powered future.

AI CERTs Cultivate AI Culture in Several Ways:

- Our structured certification fosters a comprehensive understanding of AI concepts and applications, making the technology more approachable and less intimidating.
- We prioritize continuous learning, ensuring your workforce stays up to date with the latest AI advancements to keep your organization competitive.
- By promoting collaboration through cross-functional projects, AI CERTs facilitate knowledge sharing and bridges departmental divides, supporting effective AI implementation.

AI CERTs: Your Pathway to Becoming AI-Ready

The future of business belongs to those who harness the power of AI.

Tailored for Success: Our certifications are tailored to the specific needs of your organization, avoiding a one-size-fits-all approach. Developed by industry experts, our specialized training provides your workforce with the targeted skills and expertise required to thrive in essential AI roles.

Copyright© 2026. All rights reserved

Actionable Expertise: We prioritize practical experience over mere theory. By engaging in real-world projects and case studies, your team will gain the hands-on skills and confidence needed to successfully implement AI technologies, fostering innovation and achieving tangible results.

Become an AI Leader: Lead the AI revolution, don't just follow it. Collaborate with AI CERTs to create an AI-driven culture, empowering your workforce to unlock AI's potential and place your organization at the cutting edge of transformation.

Copyright© 2026. All rights reserved

AICERTs®

www.aicerts.ai

Contact

252 West 37th St., Suite 1200W
New York, NY 10018