AI CERTs™

AI+ Security™ Compliance

Certification

Introduction to AI CERTs

AI CERTs™ leads the way in AI and blockchain certification, delivering top-tier programs that equip individuals to excel in these fast-evolving fields. Our certifications are tailored to bridge the gap between theory and real-world practice, ensuring learners are prepared to make an immediate impact on their careers.

AI CERTs™ was founded to offer high-quality, accessible certifications that empower individuals to thrive in the digital age. We aim to develop a new generation of tech leaders who are not just participants but innovators in the industry.

Acknowledgements

We would like to extend our sincere gratitude to all the Subject Matter Experts (SMEs), industry professionals, and teams who contributed their valuable time, expertise, and insights in developing the AI CERTs™ Certification Scheme. The collaborative efforts of individuals from diverse fields, including cybersecurity, artificial intelligence, education, and professional training, have played a crucial role in ensuring the relevance, rigor, and industry alignment of this certification program.

AI CERTs™

Contributors

- Cybersecurity Professionals: Individuals with expertise in cybersecurity practices, risk management, and compliance frameworks.

- AI Specialists: Experts in artificial intelligence, machine learning, and data science who understand how these technologies interact with security compliance.

- Regulatory and Compliance Experts: Professionals familiar with regulatory requirements (e.g., GDPR, HIPAA) and how they apply to AI technologies.

- IT Professionals: Those with experience in IT governance, risk, and compliance (GRC) who understand the implications of AI in IT environments.

- Academics and Researchers: Scholars with a focus on AI, cybersecurity, and compliance can contribute their insights and research findings.

- Industry Practitioners: Individuals working in sectors heavily influenced by AI and compliance, such as finance, healthcare, or government, can provide practical perspectives.

- Consultants: Professionals who specialize in advising organizations on AI implementation and compliance best practices

Exam Information

- The AI+ Security Compliance is an advanced course that merges the fundamental principles of cybersecurity compliance with the transformative power of artificial intelligence (AI). Building on the CISSP framework, this course focuses on how AI can enhance compliance processes, improve risk management, and ensure robust security measures in alignment with regulatory standards.

- This course introduces you to the core principles of cyber security compliances while exploring the potential of AI to enhance your security posture. This course structure integrates comprehensive cybersecurity compliance principles with advanced AI applications, providing learners with the necessary skills to ensure compliance and enhance security through AI technologies.

Exam Prerequisites

- **Basic Understanding of Cybersecurity Principles:** Familiarity with key concepts such as confidentiality, integrity, and availability (CIA triad), Awareness of common cybersecurity threats and vulnerabilities (e.g., malware, phishing, social engineering), Understanding of security controls and frameworks (e.g., NIST, ISO 27001).
- **Familiarity with Programming Concepts and Languages:** Basic understanding of programming concepts such as variables, data types, loops, and functions, Knowledge of object-oriented programming principles. Python is recommended due to its popularity in both cybersecurity and AI/ML applications. Familiarity with libraries like Pandas, NumPy, and scikit-learn can be advantageous.
- **Introductory Knowledge of AI or Machine Learning:** Awareness of fundamental AI concepts, including supervised and unsupervised learning. Understanding of basic machine learning algorithms (e.g., regression, classification, clustering), Familiarity with AI applications in cybersecurity, such as threat detection and response.

Exam Specifications

Number of Questions

50

Passing Score

35/50 or 70%

Duration

90 Minutes

Exam Options

Online, Remotely Proctored

Question Type

Multiple Choice/Multiple Response

Item Format Details

- **The exam will primarily consist of multiple-choice questions with single-response options.**
- **Additional item types may be included as necessary, such as:**
  - Manipulating snippets of code (e.g., SQL)
  - Interpreting data visualizations
- The exam will be administered using Proctoring 365, AI CERTs' proprietary remote proctoring solution, ensuring a secure and reliable testing environment for all candidates.
- (**Note:** exam time includes 5 minutes for reading and signing the Candidate Agreement and 5 minutes for the testing system tutorial.)

Exam Description

TARGET CANDIDATE	
CYBERSECURITY PROFESSIONALS	• Security Engineers • Incident Response Teams
AI AND MACHINE LEARNING PRACTITIONERS	• IT Personnel • Network Administrators
COMPLIANCE OFFICERS	• IT Governance and Risk Management Experts
DATA SCIENTISTS AND ANALYSTS	• Software Developers
CONSULTANTS	• Business Leaders and Managers • Regulatory Bodies
ACADEMICS AND RESEARCHERS	

Exam Objective Statement

The AI + Security Compliance certification is designed to equip professionals with the knowledge and skills to integrate artificial intelligence (AI) with cybersecurity compliance frameworks. The exam **objectives include:**

- **Introduction to Cybersecurity Compliance and AI:** Understanding the basics of cybersecurity compliance and how AI can be leveraged to enhance compliance.
- **Security and Risk Management with AI:** Using AI to conduct risk assessments and manage cybersecurity risks.
- **Asset Security and AI for Compliance:** Protecting and managing assets through AI-based solutions.
- **Security Architecture and Engineering with AI:** Applying AI to secure design principles and vulnerability assessments.
- **Communication and Network Security with AI:** Leveraging AI for network monitoring and defense.

To ensure that exam candidates demonstrate the necessary skills, the AI+ Security Level 1 exam (Exam Code: AIC-SEC-301) will assess their knowledge across the following domains, along with their respective weightings:

Module	% of Examination
Introduction to Cybersecurity Compliance and AI	10%
Security and Risk Management with AI	10%
Asset Security and AI for Compliance	10%
Security Architecture and Engineering with AI	10%
Communication and Network Security with AI	10%
Identity and Access Management (IAM) with AI	10%
Security Assessment and Incident Response with AI	10%
Security Operations with AI	10%
Software Development Security and Audit with AI	10%
Future Trends in AI and Cybersecurity Compliance	10%
Total	100%

AI CERTs™

AI+ Security Compliance™

Objectives

The information provided below is designed to assist you in preparing for your certification exam with AI CERTs. While this information serves as a valuable resource, it does not encompass every concept and skill that may be tested during your exam. The exam domains, previously identified and outlined in the objectives listing, represent the key content areas covered in the exam. Each objective within those domains reflects the specific tasks associated with the job role(s) being assessed. Additional information beyond the domains and objectives illustrates examples of concepts, tools, skills, and abilities relevant to the corresponding domains and objectives. This content is based on industry expert analysis related to the certification job role(s) and may not directly correlate with every aspect of the training program or exam content. We strongly encourage you to engage in independent study to familiarize yourself with any concepts highlighted here that were not explicitly addressed in your training program or materials.

Module 1

Module 1: Introduction to Cybersecurity Compliance and AI (10%)

1.1 Overview of Cybersecurity Compliance

1.2 International Compliance Standards

1.3 Developing Compliance Programs

1.4 Implementing Compliance Programs

1.5 AI in Cybersecurity Compliance

1.6 Case Studies and Applications

Module 2

Module 2: Security and Risk Management with AI (10%)

2.1 Risk Management Frameworks

2.2 Conducting Risk Assessments

2.3 AI in Risk Assessment

2.4 Compliance and AI

2.5 Incident Response and AI

Module 3

Module 3: Asset Security and AI for Compliance (10%)

3.1 Data Classification and Protection

3.2 AI in Privacy Protection

3.3 Asset Management with AI

3.4 Case Studies and Best Practices

Module 4

Module 4: Security Architecture and Engineering with AI (10%)

4.1 Secure Design Principles

4.2 AI in Cryptography

4.3 AI in Vulnerability Assessment

4.4 Security Models and AI

Module 5

Module 5: Communication and Network Security with AI (10%)

5.1 Network Security Fundamentals

5.2 AI in Network Monitoring

5.3 AI-driven Network Defense

5.4 Compliance in Network Security

Module 6

Module 6: Identity and Access Management (IAM) with AI (10%)

6.1 IAM Fundamentals

6.2 AI in Identity Verification

6.3 Access Control and AI

6.4 Threats to IAM and AI Solutions

Module 7

Module 7: Security Assessment and Incident Response with AI (10%)

7.1 Security Testing Techniques

7.2 AI in Security Testing

7.3 Continuous Monitoring and AI

7.4 Incident Response Planning

7.5 Managing Cybersecurity Incidents

7.6 Legal and Regulatory Considerations

Module 8

Module 8: Security Operations with AI (10%)

8.1 Security Operations Center (SOC)

8.2 Data Classification and Protection

8.3 Privacy Compliance

8.4 Disaster Recovery and AI

8.5 AI in Security Orchestration

Module 9

Module 9: Software Development Security and Audit with AI (10%)

9.1 Secure Software Development Life Cycle (SDLC)

9.2 AI in Application Security Testing

9.3 AI in Secure DevOps

9.4 Threat Modeling and AI

9.5 Internal and External Audits

Module 10

Module 10: Future Trends in AI and Cybersecurity Compliance (10%)

10.1 Emerging AI Technologies

10.2 AI in Cyber Threat Intelligence

10.3 Quantum Computing and AI

10.4 Ethical Considerations and AI Governance

10.5 Practical Applications

Recertification Requirements

To maintain your certification status, AI CERTs require recertification every 1 year. Candidates will be notified 3 months before their recertification due date. Candidates need to apply for recertification following the guidelines provided in the candidate handbook.

Contact Us for Recertification Inquiries

For any questions or to initiate the recertification process, please reach out to our support team. We are here to assist you with your recertification needs. Email: support@aicerts.io

Code of Conduct

All AI CERTs-certified professionals must adhere to the AI CERTs Code of Conduct, which emphasizes integrity, confidentiality, continuous competence development, fairness, and compliance with applicable laws and regulations. Certified individuals are expected to avoid conflicts of interest, respect intellectual property rights, and uphold ethical behavior in all professional activities. Any violation of this code may result in suspension or revocation of certification. Certified professionals agree to these terms as a requirement for maintaining their certification.

Acronyms

Acronym Expanded Form

- SDLC Secure Software Development Life Cycle
- AI - Artificial Intelligence
- SME - Subject Matter Expert
- GRC - Governance, Risk, and Compliance
- GDPR - General Data Protection Regulation
- HIPAA - Health Insurance Portability and Accountability Act
- NIST - National Institute of Standards and Technology
- CISSP - Certified Information Systems Security Professional
- CIA - Confidentiality, Integrity, Availability (CIA Triad)
- SDLC - Secure Software Development Life Cycle
- IAM - Identity and Access Management
- SOC - Security Operations Center
- ML - Machine Learning

AI CERTs™

www.aicerts.io

Contact

252 West 37th St., Suite 1200W

New York, NY 10018