AICERTs™

AI+ Security Compliance™ (5 Days)

Program Detailed Curriculum

Executive Summary

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.

Course Prerequisites

- Basic understanding of cybersecurity principles.
- Knowledge of networking fundamentals.
- Familiarity with programming concepts and languages (Python recommended)
- An introductory course on AI or machine learning is beneficial but not required.

Module 1

Introduction to Cybersecurity Compliance and AI

1.1 Overview of Cybersecurity Compliance

- **Key Concepts and Principles:** This course covers foundational principles and essential concepts in AI, focusing on ethical considerations, risk management, and the strategic application of AI technologies.
- **Major Compliance Frameworks:** Learn the essentials of major compliance frameworks like GDPR, HIPAA, PCI-DSS, and NIST, focusing on regulatory requirements, best practices, and implementation strategies.

1.2 International Compliance Standards

- **International Organization for Standardization (ISO):** Explore key ISO standards, their role in quality management, risk assessment, and global best practices across industries for ensuring compliance and operational excellence.
- **European Union Cybersecurity Act:** This course provides an overview of the EU Cybersecurity Act, detailing its impact on security certification, risk management, and compliance within the European digital market.

1.3 Developing Compliance Programs

- **Key Components of an Effective Compliance Program:** Understand the critical elements of a robust compliance program, including risk assessments, internal controls, monitoring, and continuous improvement to ensure regulatory adherence.

- **Compliance Policies and Procedures:** Learn to develop and implement comprehensive compliance policies and procedures, ensuring clear guidelines and frameworks for organizational conduct and regulatory compliance.
- **Employee Training and Awareness:** This course emphasizes the importance of employee training in compliance, focusing on building awareness, understanding legal requirements, and promoting a culture of ethical behavior.

1.4 Implementing Compliance Programs

- **Roles and Responsibilities:** Explore the roles and responsibilities within compliance programs, detailing the functions of compliance officers, management, and employees in maintaining regulatory adherence.
- **Documentation and Record-Keeping:** Learn the importance of thorough documentation and effective record-keeping in compliance, ensuring accurate tracking, legal protection, and readiness for audits.
- **Compliance Audits and Assessments:** This course covers the processes and best practices for conducting compliance audits and assessments, focusing on identifying gaps, ensuring adherence, and continuous improvement.

1.5 AI in Cybersecurity Compliance

- **Basics of AI and Types of ML:** Gain a foundational understanding of AI concepts and explore the different types of machine learning, including supervised, unsupervised, and reinforcement learning.
- **Key Algorithms and Models:** Discover essential AI algorithms and models, such as decision trees, neural networks, and clustering techniques, and their applications in various industries.
- **Benefits of Integrating AI:** Learn about the strategic advantages of incorporating AI into business operations, including efficiency gains, improved decision-making, and enhanced customer experiences.
- **Challenges and Limitations:** Explore the challenges and limitations of AI, such as data quality issues, ethical concerns, and the need for specialized skills to effectively implement AI solutions.

1.6 Case Studies and Applications

- **Real-World Examples:** Explore practical applications of AI through real-world examples across various sectors, illustrating how AI solutions solve complex problems and drive innovation.
- **Industry Adoption:** Examine how different industries are adopting AI technologies, highlighting trends, best practices, and the transformative impact of AI on traditional business models.

Module 2

Security and Risk Management with AI

2.1 Risk Management Frameworks

- **Identifying and Assessing Risks:** Understand the process of identifying and evaluating potential risks, focusing on risk assessment techniques to prioritize and manage threats effectively.
- **Risk Mitigation Strategies:** Explore practical strategies for mitigating risks, including contingency planning, risk transfer, and controls implementation to minimize potential impacts.
- **NIST Risk Management Framework (RMF):** Dive into the NIST RMF, understanding its step-by-step approach for managing information security risks, emphasizing federal and organizational compliance.
- **ISO 31000 Risk Management:** Study the ISO 31000 standard, focusing on its principles, framework, and process for effective risk management, applicable across diverse industries and sectors.

2.2 Conducting Risk Assessments

- **Identifying and Evaluating Risks:** Learn techniques for identifying potential risks within projects and organizations, and methods for evaluating their significance and potential impact.

- **Impact and Probability Assessment:** Understand how to assess the impact and likelihood of identified risks, using qualitative and quantitative tools to prioritize risk management efforts.
- **Mitigation Strategies:** Explore effective risk mitigation strategies, including avoidance, reduction, and transfer, to minimize the adverse effects of potential risks on organizational objectives.

2.3 AI in Risk Assessment

- **Automated Risk Identification:** Discover how automated tools and AI technologies can streamline the risk identification process, improving accuracy and efficiency in recognizing potential threats.
- **Predictive Risk Analytics:** Learn about predictive risk analytics, which leverages data and machine learning models to forecast future risks, enabling proactive decision-making and risk management.

2.4 Compliance and AI

- **Legal and Regulatory Considerations:** Explore the legal and regulatory landscape surrounding AI in cybersecurity, focusing on compliance requirements, data protection laws, and the evolving regulatory environment.
- **Ethical Implications of AI in Cybersecurity:** Examine the ethical challenges posed by AI in cybersecurity, including issues of privacy, bias, transparency, and the responsible use of AI technologies to protect sensitive information.

2.5 Incident Response and AI

- **Automated Incident Detection and Response:** Learn about AI-driven systems for automating the detection of security incidents and orchestrating responses, enhancing speed and efficiency in managing cyber threats.
- **AI in Forensic Analysis:** Explore the use of AI technologies in forensic analysis, focusing on how AI aids in investigating cyber incidents, uncovering evidence, and supporting legal proceedings.

Module 3

Asset Security and AI for Compliance

3.1 Data Classification and Protection

- **AI-Based Data Classification:** Understand how AI techniques can automate and enhance data classification processes, improving accuracy and efficiency in managing and organizing data.
- **Data Encryption and Protection:** Explore methods for encrypting and protecting data, focusing on best practices and technologies to safeguard sensitive information from unauthorized access.

3.2 AI in Privacy Protection

- **Privacy-Preserving AI Techniques:** Learn about AI techniques designed to preserve privacy, such as differential privacy and federated learning, ensuring data protection while enabling useful analytics.
- **AI and Data Anonymization:** Discover how AI can assist in data anonymization, reducing the risk of identifying individuals while maintaining the utility of data for analysis and research.

3.3 Asset Management with AI

- **Automated Asset Discovery:** Learn about automated tools and techniques for discovering and inventorying assets within an organization, enhancing visibility and management of IT resources.
- **AI-Driven Asset Monitoring:** Explore how AI technologies can continuously monitor assets for security and performance issues, providing real-time insights and proactive management.

3.4 Case Studies and Best Practices

- **Implementing AI in Asset Security for Compliance:** Understand how to integrate AI into asset security strategies to ensure compliance with regulatory requirements, improving protection and risk management for organizational assets.

Module 4

Security Architecture and Engineering with AI

4.1 Secure Design Principles

- **AI in Secure System Design:** Explore how AI can be leveraged in designing secure systems, focusing on predictive threat modeling, adaptive defenses, and resilience against emerging cyber threats.
- **AI-Driven Security Architecture:** Learn about AI-driven approaches to building security architectures, enhancing threat detection, response capabilities, and overall system robustness.

4.2 AI in Cryptography

- **AI-Enhanced Cryptographic Techniques:** Discover how AI can enhance cryptographic methods, including the development of more secure encryption algorithms and the automation of cryptographic operations.
- **Quantum Computing and AI:** Understand the intersection of quantum computing and AI, exploring how these technologies could revolutionize encryption, data processing, and cybersecurity.

4.3 AI in Vulnerability Assessment

- **Automated Vulnerability Scanning:** Learn about AI-powered tools for automated vulnerability scanning, providing efficient and accurate identification of security weaknesses in systems and applications.
- **AI in Penetration Testing:** Explore the role of AI in penetration testing, focusing on automated attack simulations, vulnerability assessments, and improving the effectiveness of security testing.

4.4 Security Models and AI

- **AI in Access Control Models:** Discover how AI can enhance access control models by enabling dynamic, context-aware authorization, and improving security while reducing administrative overhead.
- **Trust Models with AI Integration:** Learn about integrating AI into trust models, focusing on building and maintaining trust in digital systems through advanced authentication, anomaly detection, and continuous monitoring.

Module 5

Communication and Network Security with AI

5.1 Network Security Fundamentals

- **Network Protocols and Architecture:** Understand the fundamentals of network protocols and architecture, focusing on how they enable communication and secure data exchange across networks.
- **Network Threats and Vulnerabilities:** Explore common network threats and vulnerabilities, learning how attackers exploit weaknesses and how to implement effective defenses.

5.2 AI in Network Monitoring

- **Network Traffic Analysis:** Learn techniques for analyzing network traffic, using AI tools to detect anomalies, monitor performance, and identify potential security threats.
- **AI in Intrusion Detection Systems (IDS):** Discover how AI enhances intrusion detection systems, improving their ability to identify, analyze, and respond to unauthorized network activities.

5.3 AI-driven Network Defense

- **AI in Firewalls and Intrusion Prevention Systems (IPS):** Explore the integration of AI in firewalls and intrusion prevention systems, enhancing their capability to block threats and adapt to evolving attack vectors.
- **Automated Threat Hunting:** Learn about automated threat hunting powered by AI, focusing on proactive identification of advanced persistent threats and real-time network security monitoring.

5.4 Compliance in Network Security

- **Ensuring Network Security Compliance with AI:** Understand how AI can assist in maintaining network security compliance, ensuring adherence to regulatory standards and best practices.
- **Reporting and Audit Trails:** Explore the role of reporting and audit trails in network security, focusing on how AI can automate these processes for accurate and efficient compliance tracking.

Module 6

Identity and Access Management (IAM) with AI

6.1 IAM Fundamentals

- **Authentication and Authorization:** Learn about the principles and practices of authentication and authorization, focusing on verifying user identities and managing access to resources.
- **Identity Management Lifecycle:** Explore the identity management lifecycle, including creation, maintenance, and deactivation of user identities, with a focus on security and compliance.

6.2 AI in Identity Verification

- **Biometric Authentication Using AI:** Discover how AI enhances biometric authentication methods, such as facial recognition and fingerprint scanning, to improve accuracy and security.
- **AI-Enhanced Multi-Factor Authentication:** Learn about AI-driven advancements in multi-factor authentication, combining multiple verification methods to strengthen security and reduce fraud.

6.3 Access Control and AI

- **Role-Based Access Control with AI:** Explore how AI can optimize role-based access control (RBAC) by automating access decisions based on user roles and context.
- **Dynamic Access Control Models:** Understand dynamic access control models powered by AI, which adjust permissions in real-time based on user behavior and environmental conditions.

6.4 Threats to IAM and AI Solutions

- **Identity Theft and AI Defenses:** Learn about strategies for protecting against identity theft using AI, including detection of fraudulent activities and prevention measures.
- **AI in Managing Insider Threats:** Discover how AI can help identify and manage insider threats, using behavioral analysis and anomaly detection to prevent security breaches.

Module 7

Security Assessment and Incident Response with AI

7.1 Security Testing Techniques

- **Penetration Testing:** Explore the process of penetration testing, including planning, executing, and analyzing tests to identify and exploit security weaknesses in systems and applications.
- **Vulnerability Assessment:** Learn about vulnerability assessment techniques, focusing on identifying, evaluating, and prioritizing security vulnerabilities to enhance the overall security posture.

7.2 AI in Security Testing

- **Automated Testing Tools:** Discover automated testing tools used for evaluating software and systems, focusing on their ability to identify issues and streamline the testing process.
- **AI-Driven Security Assessments:** Explore how AI technologies enhance security assessments by automating vulnerability detection and providing deeper insights into potential threats.

7.3 Continuous Monitoring and AI

- **Real-Time Security Monitoring:** Learn about real-time security monitoring techniques, including how AI can continuously analyze data and detect threats as they occur.
- **AI in Threat Intelligence:** Understand how AI improves threat intelligence by analyzing vast amounts of data to identify emerging threats and provide actionable insights.

7.4 Incident Response Planning

- **Incident Response Lifecycle:** Study the incident response lifecycle, including preparation, detection, containment, eradication, recovery, and lessons learned, to effectively manage security incidents.
- **Creating an Incident Response Plan:** Learn how to develop a comprehensive incident response plan, outlining roles, procedures, and communication strategies to handle security incidents efficiently.
- **AI in Incident Detection:** Explore how AI enhances incident detection by analyzing patterns and anomalies in data to identify potential security breaches more effectively.
- **Automated Incident Response:** Discover how automation can streamline incident response processes, from detection to resolution, improving response times and reducing manual effort.

7.5 Managing Cybersecurity Incidents

- **Detection and Analysis:** Learn how to detect and analyze security incidents, focusing on identifying indicators of compromise and assessing the impact and scope of threats.
- **Containment, Eradication, and Recovery:** Explore strategies for containing security incidents, removing threats from the environment, and recovering systems to normal operations while minimizing damage.
- **Post-Incident Activities:** Understand the importance of post-incident activities, including reviewing the incident response, documenting lessons learned, and implementing improvements to prevent future incidents.

7.6 Legal and Regulatory Considerations

- **Reporting Requirements:** Understand the essential reporting requirements for security incidents, including what information needs to be documented and communicated to regulatory bodies and stakeholders.
- **Cooperation with Law Enforcement:** Learn about best practices for cooperating with law enforcement during and after a security incident, ensuring effective collaboration and compliance with legal requirements.
- **Automated Compliance Checks:** Explore automated tools and techniques for performing compliance checks, enhancing efficiency in verifying adherence to regulatory standards and organizational policies.
- **AI in Audit Processes:** Discover how AI can enhance audit processes by automating data analysis, identifying discrepancies, and improving accuracy and efficiency in compliance monitoring.

Module 8

Security Operations with AI

8.1 Security Operations Center (SOC)

- **SOC Roles and Responsibilities:** Learn about the various roles and responsibilities within a Security Operations Center (SOC), including monitoring, incident response, and threat analysis.
- **AI in SOC Operations:** Explore how AI can enhance SOC operations by automating threat detection, streamlining incident management, and providing advanced analytics to support security efforts.

8.2 Data Classification and Protection

- **Data Sensitivity and Classification:** Learn how to assess and classify data based on sensitivity levels to ensure proper handling and protection in accordance with security policies and regulations.
- **Encryption and Data Masking:** Explore encryption and data masking techniques used to secure sensitive information, preventing unauthorized access and protecting data during storage and transmission.
- **Secure Data Disposal:** Understand methods for securely disposing of data, including data wiping and physical destruction, to prevent unauthorized recovery and ensure compliance with data protection standards.

8.3 Privacy Compliance

- **Principles of Data Privacy:** Study the fundamental principles of data privacy, including data protection rights, consent, and the ethical handling of personal information.
- **Privacy Impact Assessments (PIAs):** Learn how to conduct Privacy Impact Assessments (PIAs) to evaluate the effects of projects or systems on individual privacy and ensure compliance with privacy regulations.
- **Privacy by Design and Default:** Explore the concept of Privacy by Design and Default, focusing on integrating privacy considerations into the design of systems and processes from the outset.

8.4 Disaster Recovery and AI

- **AI in Disaster Recovery Planning:** Discover how AI can enhance disaster recovery planning by predicting potential disruptions, optimizing recovery strategies, and ensuring business continuity.
- **AI-Driven Business Continuity:** Learn about AI-driven approaches to business continuity, including risk assessment, incident response, and maintaining operations during disruptions.

8.5 AI in Security Orchestration

- **Security Automation:** Explore the role of security automation in improving efficiency and effectiveness in threat detection, response, and overall security management.
- **AI in Security Workflow Management:** Understand how AI can streamline and enhance security workflow management by automating routine tasks, optimizing processes, and improving overall incident handling.

Module 9

Software Development Security and Audit with AI

9.1 Secure Software Development Life Cycle (SDLC)

- **Secure Coding Practices:** Learn best practices for secure coding to prevent vulnerabilities, including techniques for writing robust code that withstands common security threats.
- **AI in Code Analysis:** Discover how AI technologies assist in code analysis by automatically identifying vulnerabilities, ensuring adherence to coding standards, and improving code quality.

9.2 AI in Application Security Testing

- **Automated Application Scanning:** Explore automated tools for scanning applications to detect security vulnerabilities, ensuring early identification and remediation of potential threats.
- **AI-Driven Vulnerability Discovery:** Understand how AI enhances vulnerability discovery by analyzing code, detecting potential security flaws, and prioritizing risks for more effective mitigation.

9.3 AI in Secure DevOps

- **Integrating AI in CI/CD Pipelines:** Learn how to integrate AI into Continuous Integration and Continuous Deployment (CI/CD) pipelines to enhance automation, improve code quality, and accelerate development processes.
- **AI in Continuous Security Testing:** Explore the role of AI in continuous security testing, focusing on automating vulnerability detection and risk assessment throughout the software development lifecycle.

9.4 Threat Modeling and AI

- **AI in Identifying Software Threats:** Discover how AI can enhance the identification of software threats by analyzing code and behavior patterns to detect vulnerabilities and potential attacks.
- **Mitigating Risks with AI:** Learn how to use AI to mitigate risks by implementing predictive analytics, automated threat detection, and proactive measures to address security vulnerabilities.

9.5 Internal and External Audits

- **Preparing for Audits:** Explore best practices for preparing for security audits, including documentation, policy reviews, and readiness assessments to ensure compliance and smooth audit processes.
- **Conducting Audits:** Understand the process of conducting security audits, focusing on evaluating controls, assessing compliance, and identifying areas for improvement.
- **Audit Reporting and Follow-Up:** Learn how to create comprehensive audit reports and conduct follow-up actions, including addressing findings, implementing recommendations, and ensuring continuous improvement.

9.6 Continuous Monitoring

- **Security Information and Event Management (SIEM):** Explore SIEM systems that aggregate, analyze, and respond to security events and information, enhancing visibility and incident response capabilities.
- **Continuous Diagnostics and Mitigation (CDM):** Understand CDM practices for continuously assessing and managing security risks, using real-time diagnostics and automated mitigation strategies to protect assets.
- **Compliance Monitoring Tools:** Discover tools and technologies for monitoring compliance, including automated solutions that track adherence to regulatory requirements and organizational policies.

Module 10

Future Trends in AI and Cybersecurity Compliance

10.1 Emerging AI Technologies

- **AI Advancements:** Explore recent advancements in AI technology, including breakthroughs in machine learning, natural language processing, and their implications for various industries.
- **Potential Impact on Cybersecurity Compliance:** Learn about how AI advancements can influence cybersecurity compliance, including changes to regulatory requirements and the impact on security practices.

10.2 AI in Cyber Threat Intelligence

- **Predictive Threat Intelligence:** Discover how AI enhances predictive threat intelligence by analyzing data patterns to forecast potential threats and improve proactive defense measures.
- **AI in Threat Hunting:** Understand the role of AI in threat hunting, focusing on how it can automate and refine the process of identifying and investigating potential security threats.

10.3 Quantum Computing and AI

- **Impact on Cryptography:** Examine the impact of AI on cryptography, including potential benefits and challenges for encryption techniques and data security.
- **Preparing for Post-Quantum Security:** Learn how to prepare for post-quantum security challenges, focusing on strategies and technologies to protect against quantum computing threats.

10.4 Ethical Considerations and AI Governance

- **Ethical AI in Cybersecurity Compliance:** Explore the ethical considerations of using AI in cybersecurity, including fairness, transparency, and ensuring that AI systems adhere to compliance standards.
- **Developing AI Governance Frameworks:** Understand the principles of developing AI governance frameworks, including policies and practices to ensure responsible and effective use of AI in cybersecurity.

10.5 Practical Applications

- **Hands-On Exercises and Simulations with AI Tools:** Engage in hands-on exercises and simulations using AI tools, applying theoretical knowledge to practical scenarios and enhancing skills in real-world applications.
- **Real-World Scenarios and Problem Solving:** Apply AI concepts to real-world scenarios, solving practical problems and gaining insights into effective solutions for complex cybersecurity challenges.