Based on **CISSP Exam Outline** Effective April 15, 2024

As AI and machine learning (ML) become foundational to modern business operations, the CISSP certification has evolved to ensure that cybersecurity professionals can govern, design and defend these sophisticated systems. Rather than treating AI as a siloed topic, ISC2 continues to interweave AI-specific security tasks and subtasks across all eight domains of the CISSP Exam Outline. This ensures a holistic approach to security that addresses the unique risks of algorithmic bias, data poisoning and adversarial attacks while leveraging AI for defensive automation.

Domain 1: Security and Risk Management

Security leadership now requires a deep understanding of how AI assets shift the organizational risk posture. Within this domain, the CISSP Exam Outline emphasizes the integration of ML models and LLMs into existing risk management frameworks. This includes establishing governance for AI ethics and mitigating algorithmic bias, ensuring that automated decision-making processes align with legal, regulatory and privacy requirements.

Furthermore, AI integration touches upon third-party risk management. As organizations increasingly rely on external AI service providers, CISSPs must be equipped to evaluate the security of AI supply chains. This involves assessing the transparency of data sourcing and the resilience of provider-managed models against evolving threats, ensuring that AI adoption does not create unmanaged blind spots in the corporate security strategy.

Domain 2: Asset Security

In the realm of asset security, data is the lifeblood of AI, and its protection is paramount. This domain now covers the classification and handling of AI-specific assets, such as training datasets, pre-trained models and model weights. We focus on maintaining data integrity throughout the AI lifecycle, ensuring that the information used to “teach” these systems has not been tampered with or poisoned by malicious actors.

Privacy remains a cornerstone of this domain, specifically regarding how AI systems process Personally Identifiable Information (PII). Integration efforts focus on technical controls like differential privacy and data masking within AI environments. By treating ML models as high-value intellectual property, we provide a roadmap for managing the collection, storage and eventual destruction of data in a way that satisfies both security and privacy mandates.

Domain 3: Security Architecture and Engineering

The architecture and engineering domain addresses the structural defenses required to host and run AI safely. This includes the design of secure enclaves for high-performance AI compute and the implementation of robust input-validation mechanisms to defend against prompt injection and adversarial attacks. The CISSP Exam Outline integrates AI by looking at the shared responsibility models inherent in cloud-based AI services, ensuring the underlying infrastructure is resilient to the unique computational demands of neural networks.

Beyond physical and logical hosting, this domain includes the engineering of "Explainable AI" as a security requirement. By building systems that provide transparency into how they reached a specific output, security engineers can better audit AI behavior. This integration ensures that security architecture isn't just a perimeter around a system, but a transparent framework that supports the verification and validation of AI-driven security controls.

Domain 4: Communication and Network Security

As AI workloads move across the network, this domain focuses on securing the transit of massive datasets and the communication between distributed AI nodes. Integration involves implementing specialized micro-segmentation and Zero Trust Architecture (ZTA) to isolate AI training environments from the rest of the enterprise network. This prevents lateral movement in the event of a compromised AI interface.

Additionally, we address the role of AI in network defense. CISSPs are tasked with understanding how AI-driven Network Detection and Response (NDR) tools identify anomalous traffic patterns that traditional signature-based systems might miss. By securing the channels used for "inference at the edge," we ensure that the communication pathways supporting AI remain confidential and available.

Domain 5: Identity and Access Management (IAM)

Identity remains the primary perimeter in an AI-driven world. Within Domain 5, the CISSP Exam Outline focuses on managing identities for non-human entities, specifically AI agents and automated service accounts. This integration ensures that AI systems operate under the Principle of Least Privilege, preventing "privilege escalation" where an AI might gain unauthorized access to sensitive data repositories during its learning or execution phase.

The CISSP Exam Outline also incorporates the use of AI to enhance IAM through behavioral biometrics and adaptive authentication. By leveraging AI to analyze user login patterns and detect anomalies in real-time, CISSPs can implement more dynamic access controls. This dual focus ensures that while we secure the AI's identity, we also use AI to make the entire organization's identity infrastructure more resilient.

Domain 6: Security Assessment and Testing

Security testing must now evolve to include "Red Teaming" for AI systems. Within this domain, the CISSP Exam Outline integrates methodologies for testing model robustness against evasion and extraction attacks. Professionals audit AI systems not just for software bugs, but for "logic flaws" in the model's output that could be exploited by an adversary.

Furthermore, we address the use of AI to automate the vulnerability management lifecycle. By integrating AI-powered scanning tools, organizations can prioritize remediation efforts based on real-time threat intelligence. This ensures that security assessments are continuous rather than point-in-time, allowing for the rapid identification of vulnerabilities in both traditional code and complex ML architectures.

Domain 7: Security Operations

In the Security Operations Center (SOC), AI is a force multiplier. This domain focuses on the integration of AI and ML into Security Orchestration, Automation and Response (SOAR) platforms. The CISSP Exam Outline addresses how to manage "Alert Fatigue" by using AI to correlate disparate events and provide high-fidelity context to security analysts, allowing for faster incident response.

Operationally, we also cover the "Security of AI" during the production phase. This includes monitoring for "Model Drift"—where an AI's performance degrades over time—and responding to live adversarial attacks. By blending traditional incident response with AI-specific monitoring, CISSPs ensure that the organization's operational resilience keeps pace with the speed of automated threats.

Domain 8: Software Development Security

As AI transforms how code is written, Domain 8 has evolved to secure the modern development lifecycle. The CISSP Exam Outline incorporates the use of AI-assisted coding tools, focusing on the risks of "hallucinated" vulnerabilities or the accidental inclusion of insecure code snippets generated by LLMs. The focus is on integrating automated AI security testing into the CI/CD pipeline to catch these flaws before they reach production.

Additionally, this domain addresses the security of the software supply chain as it pertains to ML libraries and frameworks. Professionals are tasked with identifying and mitigating "Model Hijacking" or "Inference Attacks" that target the software layer. By embedding AI considerations into the Software Development Life Cycle (SDLC), we ensure that developers can leverage the efficiency of AI without compromising the integrity of the finished product.