C|AIGA
Certified AI Governance Auditor

EC-Council
Building A Culture Of Security

Certified AI Governance Auditor

EXAM BLUEPRINT v1

Domain	Sub Domain	Description	Number of Questions	Weightage (%)
Domain 1 — AI Governance Foundations, Regulatory Landscape & Technical Literacy	Foundations of AI Governance Auditing	• Why AI Governance Auditing Is Now a Distinct Discipline • Core Vocabulary: AI System, Model, Agent, and Autonomy • Categories of AI Harm an Audit Must Test For • Auditing AI vs. Auditing Traditional IT: What Changes and What Doesn't	6	**18%**
	The Global AI Governance Framework Landscape	• Standards vs. Regulations: What's Binding and What's Voluntary • The NIST AI RMF: The Four Functions • ISO/IEC 42001: The Certifiable AI Management System Standard • The EU AI Act: Risk Tiers and Phased Obligations • Regional Regulatory Overview I: Americas & Europe • Regional Regulatory Overview II: India, Middle East & APAC • Industry Security Baselines and Using Multiple Frameworks Together	8	
	AI/ML & MLOps Fundamentals for Auditors	• What Is AI/ML: A Map of System Types • How Models Are Trained • Key Generative-AI Concepts • Retrieval-Augmented Generation and Vector Databases • Agentic AI: What Makes a System 'Agentic' • The MLOps Pipeline: From Data to Production • Reading Technical Evidence as an Auditor • Model Lifecycle Management and CI/CD for ML • Cloud and Infrastructure Basics for AI Systems • MLOps-to-Audit-Domain Crosswalk	8	
Domain 2 — AI System Design, Data Governance & Build-Time Assurance	AI System Design & Requirements Governance	• Design-Stage Governance: Why It Exists and What It Prevents • Documented Intended Use and System Requirements Specification • A Defensible Responsible-Design Process • Enforcing Autonomy and Agency Boundaries • The Pre-Build Impact Assessment and Prohibited-Practice Screening	6	**25%**

Certified AI Governance Auditor Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Domain	Sub Domain	Description	Number of Questions	Weightage (%)
	AI Data Governance & Protection	• Data Governance: Why It Exists and What It Prevents • Access Control and Personal-Information Protection for AI Data • Data Quality, Provenance, and Lifecycle Management • Cross-Border Transfer and Data-Subject Rights • Training-Data Bias and Intellectual-Property Controls • AI Sustainability and ESG Reporting Controls	8	
	AI Build, Integration & Secure Development	• Build-Time Governance: Why It Exists and What It Prevents • Identity and Access Management in AI Pipelines, Part 1 • Identity and Access Management in AI Pipelines, Part 2 • Model Lifecycle Management I: Supply Chain, Poisoning, and Value Alignment • Model Lifecycle Management II: Integrity, Versioning, and Baselining • Adversarial and Platform Security: Model Theft, Prompt Leaking, and RAG/Vector-Database Security • Deployment and Operational Security Architecture • Secure API and Endpoint Management, and Attack-Surface Reduction • Human-in-the-Loop Testing and Build-Time Separation of Duties • Secure Model Serialization and Safe-Loading Formats	12	
	AI Deployment & Change Management	• Deployment & Change Governance: Why It Exists and What It Prevents • The Release Gate: Criteria, Staged Rollout, and Rollback • Platform Security Hygiene: Configuration and Patch Management • Regulated and Jurisdictional Deployment Gates	4	
Domain 3 — AI Evaluation, Runtime Security & Incident Response	AI Evaluation, Testing & Red Teaming	• Evaluation, Testing & Red Teaming Governance: Why It Exists and What It Prevents • Evaluation Foundations: Regression, Coverage, and Metric Discipline • Model Risk Evaluation, Red Teaming, Robustness, and Performance	9	**20%**

Certified AI Governance Auditor Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Domain	Sub Domain	Description	Number of Questions	Weightage (%)
		• Fairness, Bias, and Explainability Evaluation • Frontier-Capability Evaluation, Containment, and Safety Assurance • Functional Safety and Independent Backstop Assurance		
	AI Runtime Security, Defense & Monitoring	• Runtime Security & Defense Governance: Why It Exists and What It Prevents • Context Trust, Output Handling & Resource Protection • Agentic Attack Surface I: Goal Hijacking, Tool Misuse & Inter-Agent Security • Agentic Attack Surface II: Human Trust Exploitation & Memory Integrity • Model Integrity: Toxic Output, Hallucination & Harmful Code Generation • Injection, Jailbreaking, PII & Output Filtering Defenses • Drift, Anomaly Detection & Alert Correlation • Observability Backbone: Logging, Consumption, Audit Retention & Performance • Agentic Governance: Tool Trust Tiers, Human Handoff & Secure Code Generation	11	
	AI Incident Response & Forensics	• Incident Response & Forensics Governance: Why It Exists and What It Prevents • Agentic Containment: Code Execution, Cascading Failure, and the Kill-Switch • Response, Recovery, and Reporting Across the Incident Lifecycle • Root Cause Analysis and the Post-Incident Learning Loop • Forensic Evidence and External Notification Obligations	4	
Domain 4 — AI Accountability, Risk, Transparency, Oversight & Supply Chain	AI Accountability, Roles & Organizational Governance	• Accountability & Organizational Governance: Why It Exists and What It Prevents • Individual Competence and System-Level Accountability • The Governance & Accountability Backbone • Ethics Policy, Defense-in-Depth, and Governance Composition	4	**20%**

Certified AI Governance Auditor Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Domain	Sub Domain	Description	Number of Questions	Weightage (%)
	AI Risk Inventory & Classification	• Risk Inventory & Classification Governance: Why It Exists and What It Prevents • Inventory, Classification & Applicability Foundations • Aggregate Risk Visibility & Lifecycle Reassessment	3	
	AI Transparency, Explainability & Stakeholder Communication	• Transparency & Stakeholder Communication Governance: Why It Exists and What It Prevents • Disclosure, Reactive Reporting & Regulatory Duties • Ongoing Communication, Community Engagement & Aggregate Reporting • Data & Model Transparency Documentation • Decision Explainability, Justification & Agentic Traceability • Content Provenance, Accessibility & Emerging Safety Disclosure Mandates	6	
	AI Oversight, Continuous Assurance & Audit Management	• Oversight & Continuous Assurance Governance: Why It Exists and What It Prevents • Internal Assurance Mechanics: Concern Reporting, Exception Management & Internal Audit • Operational Oversight: Performance Metrics, Documentation & Regulatory Update Actioning • AI FinOps: Cost Governance Across the Spend Lifecycle • The Regulatory Compliance Chain: Alignment, Mapping, Validation & Gap Tracking • Governance Program Management: Target Operating Model, Value & ROI • Horizon Scanning, Regulatory Intelligence & Frontier Capability Monitoring • Independent Assurance of Continuous Monitoring	7	
	AI Third-Party & Supply Chain Risk Management	• Third-Party & Supply Chain Risk Governance: Why It Exists and What It Prevents • Responsibility Allocation: Deployment Classification & Downstream Use • Vendor Risk, Governance & Performance Management	4	

Certified AI Governance Auditor Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Domain	Sub Domain	Description	Number of Questions	Weightage (%)
		• Vendor Change Tracking & Continuous Compliance Validation		
Domain 5 — Multi-Standard Audit Methodology, Platforms, AI-BOM & Professional Ethics	Multi-Standard Audit Methodology, Evidence Management & Certification Practice	• General Audit Principles and the Audit Lifecycle • Scoping an Engagement: Domains, Standards, and Risk Tiers • A Weighted Maturity Scale in Practice • Prioritizing Findings: Risk-Weighted Rollups and Critical-Control Gating • Evidence Sufficiency, Sampling, and Evidence Management • Nonconformity Grading, Corrective-Action Timelines, and Reporting • Certification Decision-Making, Appeals, and Assessor Independence • Continuous Assurance: From Point-in-Time Audits to Ongoing Monitoring • Audit Quality Assurance and Multi-Auditor Engagement Management	8	**17%**
	AI Bill of Materials & Surveillance Audits	• What an AI Bill of Materials Is and Why It Exists • What a Complete AI-BOM Must Document • Testing AI-BOM Completeness and Currency • Surveillance Audits: Purpose and Position in the Certification Lifecycle • Scoping a Surveillance Audit • Triggers for Unscheduled Surveillance • Connecting the Two: AI-BOM Currency as Standing Surveillance Scope	4	
	AI-Assisted Auditing Techniques	• A Capability Model: Matching AI to Audit Tasks • The Error Profile: How AI Fails at Audit Work • The Verification Discipline • Auditing With AI Versus Auditing AI: Why This Is a Separate Discipline • Confidentiality, Data Handling, and Engagement Permission • Independence, Professional Judgment, and Accountability • Building Capability: Developing and Validating Your Own Techniques	4	

Certified AI Governance Auditor Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Domain	Sub Domain	Description	Number of Questions	Weightage (%)
	Converting An Operating Model Into An Operating System	• What Makes a Framework an Operating System Rather Than a Model • ADG's Structure as Evidence of Continuous, By-Design Operation • Logic and Substrate: Why a Continuous Design Still Needs Somewhere to Run • ADG's Control Taxonomy: A Named Example of How a Real Framework Organizes Governance • Certification Mechanics: How an ADG Audit Actually Concludes • Walking Through the Substrate: How ComplyX Executes ADG's Scoring • A Universal Framework for Evaluating Any Execution Substrate	2	
	Professional Ethics, Multi-Standard Certification & Exam Preparation	• Code of Professional Ethics for an AI Governance Auditor • Conflict-of-Interest Management and Independence • Continuing Professional Education (CPE) and Recertification • Exam Blueprint Walkthrough and Practice Questions	2	
Total			**120**	**100%**

Certified AI Governance Auditor Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.