Verification Form
Certified Chief Information Security Officer (C|CISO)
DEAR VERIFIER, PLEASE TICK THE BOXES BELOW THAT MATCH THE APPLICANTS DOMAIN EXPERIENCE

EC-Council

Applicant's Name

Domain 1 - Governance (Policy, Legal & Compliance)

☒ Define, implement, manage and maintain an information security governance program that includes leadership, organizational structures and processes.

☒ Understand standards, procedures, directives, policies, regulations, and legal issues that affect the information security program.

☒ Understand the enterprise information security compliance program and manage the compliance team.

☐ Assess the major enterprise risk factors for compliance.

Domain 2 - IS Management Controls and Auditing Management (Projects, Technology & Operations)

☐ Identify and select the resources required to effectively implement and maintain information systems controls. Such resources can include human capital, information, infrastructure, and architecture (e.g., platforms, operating systems, networks, databases, applications).

☐ Monitor and document the information systems control performance in meeting organizational objectives by identifying and measuring metrics and key performance indicators (KPIs), and share with relevant stakeholders to support executive decision-making.

☐ Execute the audit process in accordance with established standards and interpret results against defined criteria to ensure that the information systems are protected, controlled and effective in supporting organization's objectives.

Domain 3 - Management - Projects and Operations

☐ Define activities needed to successfully execute the information systems program, estimate activity duration, and develop a schedule and staffing plan.

☐ Develop, manage and monitor the information systems program budget, estimate and control costs of individual projects.

☐ Identify, negotiate, acquire and manage the resources needed for successful design and implementation of the information systems program
(e.g., people, infrastructure, vendors and architecture).

☐ Assign clear information security personnel job functions and provide continuous training to ensure effective performance and accountability.

☐ Identify stakeholders, manage stakeholders' expectations and communicate effectively to report progress and performance.

Domain 4 - Information Security Core Competencies

☐ Design a systematic and structured risk assessment process and establish, in coordination with stakeholders, an information security risk management program based on standards and procedures and ensure alignment with organizational goals and objectives.

☐ Identify changes to risk management policies and processes and ensure the risk management program remains current with the emerging risk and threat environment and in alignment with the organizational goals and objectives.

☐ Define the scope of the enterprise continuity of operations program to address business continuity, business recovery, contingency planning, and disaster recovery/related activities.

☐ Develop a plan to identify a potential security violation and take appropriate action to report the incident.

Domain 5 - Strategic planning & finance

☐ Design, develop and maintain enterprise information security architecture (EISA) by aligning business processes, software and hardware, local and wide area networks, people, operations, and projects with the organization's overall security strategy.

☐ Define a forward-looking, visionary and innovative strategic plan for the role of the information security program with clear goals, objectives and targets that support the operational needs of the organization.

☐ Analyze, forecast and develop the operational budget of the information security department.

☐ Monitor and oversee cost management of information security projects, return on investment (ROI) of key purchases related to security infrastructure and security and ensure alignment with the strategic plan.

☐ Identify and report financial metrics to stakeholders.

TO BE COMPLETED BY THE VERIFIER

Please Print

Name _____

Title _____   Company _____

Address _____

_____

Email _____   Telephone _____

How long have you known the candidate and in what capacity?

_____

_____

Would you recommend the candidate for EC-Council's Certified Chief Information Security Officer (C|CISO) certification program?

☐ Yes, without reservation   ☐ Yes, with some reservation   ☐ Not at this time

If you checked "With some reservation" or "Not at this time" please address this in your statement.
In a brief statement, please decree the major strengths and weaknesses of the applicant as a Certified Chief Information Security Officer and attach it to this form.

_____

_____

_____

_____

_____

Verifier's Signature

May we contact you in the future?   ☐ Yes   ☐ No