CPD POINTS

DISCOUNTS ARE AVAILABLE

CERTIFIED INFORMATION SYSTEMS AUDITOR

INTRODUCTION:

A Certified Information Systems Auditor (CISA) is a professional certification awarded to individuals who demonstrate expertise in auditing, control, and assurance of information systems. CISA certification is globally recognized and signifies a high level of competency in assessing and managing information technology systems within organizations. CISA professionals play a crucial role in ensuring the security, integrity, and efficiency of IT systems and data.

☑ INFORMATION SYSTEMS AUDITING PROCESS

PROVIDING INDUSTRY-STANDARD AUDIT SERVICES TO ASSIST ORGANIZATIONS IN PROTECTING AND CONTROLLING INFORMATION SYSTEMS, DOMAIN-1 AFFIRMS YOUR CREDIBILITY TO OFFER CONCLUSIONS ON THE STATE OF AN ORGANIZATION'S IS/IT SECURITY, RISK AND CONTROL SOLUTIONS.

☑ GOVERNANCE & MANAGEMENT OF IT

THIS DOMAIN CONFIRMS TO STAKEHOLDERS YOUR ABILITIES TO IDENTIFY CRITICAL ISSUES AND RECOMMEND ENTERPRISE-SPECIFIC PRACTICES TO SUPPORT AND SAFEGUARD THE GOVERNANCE OF INFORMATION AND RELATED TECHNOLOGIES.

START FROM

04-DEC-2023

Monday-Friday

☑ INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT & IMPLEMENTATION

DOMAINS 3 AND 4 OFFER PROOF NOT ONLY OF YOUR COMPETENCY IN IT CONTROLS, BUT ALSO YOUR UNDERSTANDING OF HOW IT RELATES TO BUSINESS

☑ INFORMATION SYSTEMS OPERATIONS & BUSINESS RESILIENCE

DOMAINS 3 AND 4 OFFER PROOF NOT ONLY OF YOUR COMPETENCY IN IT CONTROLS, BUT ALSO YOUR UNDERSTANDING OF HOW IT RELATES TO BUSINESS.

☑ PROTECTION OF INFORMATION ASSETS

CYBERSECURITY NOW TOUCHES VIRTUALLY EVERY INFORMATION SYSTEMS ROLE, AND UNDERSTANDING ITS PRINCIPLES, BEST PRACTICES AND PITFALLS IS A MAJOR FOCUS WITHIN DOMAIN 5.0 BUSINESS.

DURATION 48HOURS

LEARNING INVESTMENT

RS: 30,000/-

Scan For Registration

021-48503044/033-05988928
dirpdc@pnec.nust.edu.p

PNEC-NUST

START FROM

04-DEC-2023

Monday-Friday

PDC
NUST-KARACHI

Scan For Registration

SUPPORTING TASKS

1. Plan audit to determine whether information systems are protected, controlled and provide value to the organization.
2. Conduct audit in accordance with IS audit standards and a risk based IS audit strategy.
3. Communicate audit progress, findings, results and recommendations to stakeholders.
4. Conduct audit follow-up to evaluate whether risks have been sufficiently addressed.
5. Evaluate the IT strategy for alignment with the organization's strategies and objectives.
6. Evaluate the effectiveness of IT governance structure and IT organizational structure.
7. Evaluate the organization's management of IT policies and practices.
8. Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements.
9. Evaluate IT resource and portfolio management for alignment with the organization's strategies and objectives.
10. Evaluate the organization's risk management policies and practices.
11. Evaluate IT management and monitoring of controls.
12. Evaluate the monitoring and reporting of IT key performance indicators (KPIs).
13. Evaluate the organization's ability to continue business operations.
14. Evaluate whether the business case for proposed changes to information systems meet business objectives.
15. Evaluate whether IT supplier selection and contract management processes align with business requirements.
16. Evaluate the organization's project management policies and practices.
17. Evaluate controls at all stages of the information systems development lifecycle.
18. Evaluate the readiness of information systems for implementation and migration into production.
19. Conduct post-implementation review of systems to determine whether project deliverables, controls and requirements are met.
20. Evaluate whether IT service management practices align with business requirements.
21. Conduct periodic review of information systems and enterprise architecture.
22. Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization's objectives.
23. Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization's objectives.
24. Evaluate database management practices.
25. Evaluate data governance policies and practices.
26. Evaluate problem and incident management policies and practices.
27. Evaluate change, configuration, release and patch management policies and practices.
28. Evaluate end-user computing to determine whether the processes are effectively controlled.
29. Evaluate the organization's information security and privacy policies and practices.
30. Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded.
31. Evaluate logical security controls to verify the confidentiality, integrity and availability of information.
32. Evaluate data classification practices for alignment with the organization's policies and applicable external requirements.
33. Evaluate policies and practices related to asset lifecycle management.
34. Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.
35. Perform technical security testing to identify potential threats and vulnerabilities.
36. Utilize data analytics tools to streamline audit processes.
37. Provide consulting services and guidance to the organization in order to improve the quality and control of information systems.
38. Identify opportunities for process improvement in the organization's IT policies and practices.
39. Evaluate potential opportunities and threats associated with emerging technologies, regulations and industry practices.

021-48503044/033-05988928
dirpdc@pnec.nust.edu.p
PNEC-NUST