PDC

NUST-PNEC

NATIONAL UNIVERSITY OF SCIENCES & TECHNOLOGY ✦ PAKISTAN ✦

DISCOUNTS ARE AVAILABLE

CERTIFIED INFORMATION SECURITY MANAGER

CPD COURSE (PEC)

FIVE DAYS TRINING

20-NOV-2023

MONDAY-FRIDAY

TOTAL CONTACT HOURS 30

NUST CERTIFIED COURSE

MAKE THE MOVE FROM TEAM PLAYER TO LEADER

Take your expertise in Information Security to the next level with CISM certification

Data breaches, ransomware attacks and other constantly evolving security threats are top-of-mind for today's IT professionals. With a Certified Information Security Manager® (CISM®) certification, you'll learn how to assess risks, implement effective governance and proactively respond to incidents.

COURSE OUTLINE

- ☑ 17% DOMAIN 1 – INFORMATION SECURITY GOVERNANCE
- ☑ 20% DOMAIN 2 – INFORMATION SECURITY RISK MANAGEMENT
- ☑ 30% DOMAIN 4 – INCIDENT MANAGEMENT
- ☑ 33% DOMAIN 3 – INFORMATION SECURITY PROGRAM

LEARNING INVESTMENT

RS: 35,000/-

Scan For Registration

Contact:

☎ 03305988928

✉ dirpdc@pnec.nust.edu.pk

WEEKLY PLAN

PNS JAUHAR, Habib Ibrahim Rehmatullah Road, Karachi, Pakistan

NUST KARACHI CAMPUS

NUST CERTIFIED COURSE

WORKSHOP CONTENTS:

DAY-1

17% DOMAIN 1 – INFORMATION SECURITY GOVERNANCE

This domain will provide you with a thorough insight into the culture, regulations and structure involved in enterprise governance, as well as enabling you to analyze, plan and develop information security strategies. Together, this will affirm high-level credibility in information security governance to stakeholders.

A–ENTERPRISE GOVERNANCE

1. Organizational Culture
2. Legal, Regulatory and Contractual Requirements
3. Organizational Structures, Roles and Responsibilities

B–INFORMATION SECURITY STRATEGY

1. Information Security Strategy Development
2. Information Governance Frameworks and Standards
3. Strategic Planning (e.g., Budgets, Resources, Business Case)

DAY-2

20% DOMAIN 2 – INFORMATION SECURITY RISK MANAGEMENT

This domain empowers you to analyze and identify potential information security risks, threats and vulnerabilities as well as giving you all the information about identifying and countering information security risks you will require to perform at management level.

A–INFORMATION SECURITY RISK ASSESSMENT

1. Emerging Risk and Threat Landscape
2. Vulnerability and Control Deficiency Analysis
3. Risk Assessment and Analysis

B–INFORMATION SECURITY RISK RESPONSE

1. Risk Treatment / Risk Response Options
2. Risk and Control Ownership
3. Risk Monitoring and Reporting

DAY-3

33% DOMAIN 3 – INFORMATION SECURITY PROGRAM

This domain covers the resources, asset classifications and frameworks for information security as well as empowering you to manage information security programs, including security control, testing, comms and reporting and implementation.

A–INFORMATION SECURITY PROGRAM DEVELOPMENT

1. Information Security Program Resources (e.g., People, Tools, Technologies)
2. Information Asset Identification and Classification
3. Industry Standards and Frameworks for Information Security
4. Information Security Policies, Procedures and Guidelines
5. Information Security Program Metrics

B–INFORMATION SECURITY PROGRAM MANAGEMENT

1. Information Security Control Design and Selection
2. Information Security Control Implementation and Integrations
3. Information Security Control Testing and Evaluation
4. Information Security Awareness and Training
5. Management of External Services (e.g., Providers, Suppliers, Third Parties, Fourth Parties)
6. Information Security Program Communications and Reporting

DAY-3

30% DOMAIN 4 – INCIDENT MANAGEMENT

This domain provides in-depth training in risk management and preparedness, including how to prepare a business to respond to incidents and guiding recovery. The second module covers the tools, evaluation and containment methods for incident management.

A–INCIDENT MANAGEMENT READINESS

1. Incident Response Plan
2. Business Impact Analysis (BIA)
3. Business Continuity Plan (BCP)
4. Disaster Recovery Plan (DRP)
5. Incident Classification/Categorization
6. Incident Management Training, Testing and Evaluation

B–INCIDENT MANAGEMENT OPERATIONS

1. Incident Management Tools and Techniques
2. Incident Investigation and Evaluation
3. Incident Containment Methods
4. Incident Response Communications (e.g., Reporting, Notification, Escalation)
5. Incident Eradication and Recovery

Post-Incident Review Practices

PNS JAUHAR, Habib Ibrahim Rehmatullah Road,
Karachi, Pakistan

NUST KARACHI CAMPUS