XONTECH

Agenda Detaliată: Digital Operational Resilience Act (DORA)

Durata: 3 zile | Total: 21 ore

Ziua 1: Guvernanță și Managementul Riscului

- Sesiunea 1 (09:00 - 12:30)
  - **09:00 - 10:00:** Contextul European și scopul DORA. Obiectivele și termenul limită.
  - **10:00 - 11:00:** Domeniul de aplicare și clasificarea entităților financiare.
  - **11:00 - 11:15:** *Pauză de cafea.*
  - **11:15 - 12:30:** Rolul organului de conducere. Guvernanță și politici de reziliență.
- Sesiunea 2 (13:30 - 17:00)
  - **13:30 - 15:00:** Cadrul de management al riscului TIC: Identificare, protecție și prevenție.
  - **15:00 - 15:15:** *Pauză.*
  - **15:15 - 16:30:** Detectarea activităților anormale și mecanisme de control.
  - **16:30 - 17:00:** Sesiune Q&A și exercițiu de mapare a activelor critice.

Ziua 2: Incidente TIC și Raportare

- Sesiunea 3 (09:00 - 12:30)
  - **09:00 - 10:30:** Procesul de gestionare a incidentelor. Clasificarea incidentelor majore.
  - **10:30 - 10:45:** *Pauză de cafea.*
  - **10:45 - 12:30:** Standarde tehnice (RTS) pentru criteriile de clasificare a incidentelor.
- Sesiunea 4 (13:30 - 17:00)
  - **13:30 - 15:00:** Obligații de raportare: Notificarea inițială, raportul intermediar și final.
  - **15:00 - 15:15:** *Pauză.*
  - **15:15 - 17:00:** Workshop practic: Completarea unui raport de incident conform formatului oficial.

Digitally signed by Vicol Irina
Date: 2026.03.09 12:53:18 EET
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Ziua 3: Testarea și Managementul Furnizorilor

- Sesiunea 5 (09:00 - 12:30)
    - **09:00 - 10:30:** Programul de testare a rezilienței. Tipuri de teste și frecvență.
    - **10:30 - 10:45:** *Pauză de cafea.*
    - **10:45 - 12:30:** Teste avansate bazate pe amenințări (TLPT). Cerințe pentru testeri.
- Sesiunea 6 (13:30 - 17:00)
    - **13:30 - 15:00:** Riscul TIC asociat terților. Strategia de ieșire (Exit Strategy).
    - **15:00 - 15:15:** *Pauză.*
    - **15:15 - 16:30:** Analiza Articolului 30: Clauze contractuale obligatorii cu furnizorii TIC.
    - **16:30 - 17:00:** Recapitulare finală și plan de aliniere.

    Închiderea cursului și eliberarea certificatelor.

Agenda Detaliată: curs Specialist Cybersecurity ISO/IEC 27032

Durata: 5 zile | Total: 35 ore

Zilele 1-2: Fundamente și Managementul Riscului

- Sesiunile 1 & 3 (09:00 - 12:30)
    - **09:00 - 10:30:** Introducere în ISO 27032. Ecosistemul cibernetic și actorii implicați.
    - **10:45 - 12:30:** Identificarea amenințărilor (Phishing, Ransomware, DDoS).
- Sesiunile 2 & 4 (13:30 - 17:00)
    - **13:30 - 15:00:** Metodologii de evaluare a riscului cibernetic.
    - **15:15 - 17:00:** Workshop: Analiza vulnerabilităților și tratarea riscurilor.

Zilele 3-4: Controale Tehnice și Incident Management

- Sesiunile 5 & 7 (09:00 - 12:30)
    - **09:00 - 10:30:** Securitatea rețelelor și a sistemelor. Hardening și criptografie.
    - **10:45 - 12:30:** Ciclul de viață al incidentului: Pregătire și Detectare
- Sesiunile 6 & 8 (13:30 - 17:00)
    - **13:30 - 15:00:** Răspunsul la incidente: Contenire, Eradicare, Recuperare.
    - **15:15 - 17:00:** Exercițiu practic: Simulare de atac și răspuns defensiv

Ziua 5: Reziliență și Guvernanță Finală

- Sesiunea 9 (09:00 - 12:30)
    - **09:00 - 10:30:** Strategii de continuitate în spațiul cibernetic.
    - **10:45 - 12:30:** Schimbul de informații și parteneriatele de securitate (Sharing Communities).
- Sesiunea 10 (13:30 - 17:00)
    - **13:30 - 15:00:** Auditarea programului de securitate cibernetică.
    - **15:15 - 16:30:** Examen recapitulativ și evaluarea finală a cunoștințelor.

      Închiderea cursului și eliberarea certificatelor.