Programul de instruire curs "Digital Operational Resilience Act (DORA)"

I. Scopul și Obiectivele Instruirii

Xontech Systems își asumă livrarea unui curs care să asigure participanților o înțelegere clară și aplicabilă a **Regulamentului (UE) 2022/2554**, vizând direct:

- **Familiarizarea** cu cadrul normativ și cerințele-cheie DORA.
- **Înțelegerea obligațiilor** de gestionare a riscurilor TIC și reziliență digitală.
- **Clarificarea responsabilităților** de guvernanță, control și raportare la nivel instituțional.
- **Dezvoltarea capacității practice** de aplicare a cerințelor în procesele interne.
- **Identificarea măsurilor concrete** pentru alinierea politicilor și procedurilor interne.

II. Structura și Tematica Cursului

Programul este adaptat celor 4 subiecte majore solicitate, distribuite pe durata de **3 zile (6 sesiuni a câte 3,5 ore)**:

- **Subiectul 1: Cadrul general și domeniul de aplicare.**
  - *Abordare:* Analiza domeniului de aplicare și a termenelor de implementare.
- **Subiectul 2: Managementul riscurilor TIC și guvernanța.**
  - *Abordare:* Definirea rolului conducerii și a strategiilor de protecție și prevenție.
- **Subiectul 3: Gestionarea incidentelor TIC și raportarea.**
  - *Abordare:* Clasificarea incidentelor majore și fluxurile de notificare către autorități.
- **Subiectul 4: Testarea rezilienței și managementul terților.**

- *Abordare:* Programe de testare și cerințe contractuale obligatorii pentru furnizorii TIC.

III. Metodologia de Livrare și Rezultate Scontate

Instruirea se va desfășura **Online**, în limba **Română**, utilizând metode interactive pentru a garanta următoarele rezultate:

- Înțelegerea impactului DORA asupra activității instituției.
- Creșterea nivelului de conștientizare privind riscurile digitale.
- Capacitatea de a monitoriza implementarea cerințelor la nivel instituțional.
- Capacitatea de a identifica lacunele actuale față de standardele de conformare.

IV. Expertiza Trainerului: Lucian Chete

Implementarea acestor obiective va fi coordonată de **Lucian Chete**, a cărui experiență garantează calitatea instruirii:

- **Expertiză în Certificare:**, Lucian Chete deține o experiență vastă în auditarea sistemelor de management (ISO 27001, ISO 22301), fiind expert în evaluarea conformității pentru sectorul financiar și IT conform Regulamentului (UE) 2022/2554 DORA)
- **Trainer de Nivel Înalt:** A livrat programe complexe de instruire pentru entități precum Directoratul Național de Securitate Cibernetică (DNSC) și companii multinaționale si statale, având capacitatea de a traduce reglementări juridice complexe în pași tehnici și operaționali clari.
- **Specialist în Reziliență:** Expertiza sa acoperă întregul spectru al rezilienței digitale, oferind participanților nu doar teorie, ci soluții verificate în practică pentru alinierea la legislația europeană și națională (Legea 195/2024).

Programul de instruire curs „Specialist Cybersecurity ISO/IEC 27032”

I. Scopul și Obiectivele Instruirii

Scopul principal al acestui program este dezvoltarea competențelor tehnice și organizaționale necesare pentru protecția spațiului cibernetic, conform standardului internațional **ISO/IEC 27032**. Obiectivele urmărite sunt:

- **Fundamente ISO 27032:** Familiarizarea cu principiile și conceptele de bază ale standardului.
- **Cadrul de Cooperare:** Înțelegerea modului de colaborare între entitățile interne și externe pentru securitate cibernetică.
- **Managementul Amenințărilor:** Dezvoltarea abilităților de identificare, analiză și tratare a riscurilor cyber.
- **Măsuri de Protecție:** Aplicarea soluțiilor tehnice și organizaționale pentru securizarea infrastructurilor IT.
- **Răspuns la Incidente:** Consolidarea capacității de prevenire, detectare și reacție rapidă la incidente.

II. Structura și Tematica Cursului

Programul este structurat pe durata de **5 zile** (10 sesiuni a câte 3,5 ore), acoperind subiectele cheie:

- **Subiectul 1: Introducere în ISO/IEC 27032.** Cadrul general de securitate cibernetică și terminologia specifică.
- **Subiectul 2: Peisajul Amenințărilor.** Analiza detaliată a riscurilor, vulnerabilităților și tipologiilor de atacuri cibernetice.
- **Subiectul 3: Managementul Incidentelor.** Proceduri de răspuns, investigare și recuperare în urma unui incident cyber.

- **Subiectul 4: Controale Tehnice și Organizaționale.** Implementarea măsurilor de protecție specifice standardului pentru date sensibile și infrastructură.

III. Metodologia și Rezultatele Scontate

- **Forma:** Online, interactivă.
- **Durata:** 5 zile (Perioada: Trimestrul II-III, 2026).
- **Participanți:** 3 angajați.

Așteptări post-instruire:

1. Dobândirea cunoștințelor aplicabile conform ISO/IEC 27032.
2. Capacitate sporită de gestionare a amenințărilor cibernetice.
3. Îmbunătățirea proceselor interne de cooperare și securitate.
4. Consolidarea protecției activelor informaționale ale instituției.

IV. Expertiza Trainerului: Lucian Chete

Instruirea va fi condusă de un expert cu o bază solidă în securitate defensivă și ofensivă:

- **Certificări de Elită:** Deține titlurile **C)PTE (Certified Penetration Testing Engineer)** și **CHA (Computer Hacking Auditor)**, esențiale pentru modulele de amenințări și managementul incidentelor din ISO 27032, ISO27001 si ISO22301
- **Trainer Recunoscut:** Experiență demonstrată în colaborări cu Directoratul Național de Securitate Cibernetică (DNSC) și operatori de infrastructură critică din UE si Moldova, oferind o perspectivă practică asupra securității cibernetice.