Sudhara International
+48 32 724 35 86
info@sudharapolska.com
www.sudharapolska.com

PEŁNOMOCNIK DS. CYBERBEZPIECZEŃSTWA

PROGRAM SZKOLENIA

🎯 **Cel szkolenia**

Celem szkolenia jest kompleksowe przygotowanie uczestników do pełnienia funkcji Pełnomocnika ds. cyberbezpieczeństwa w organizacji poprzez rozwinięcie wiedzy i umiejętności z zakresu zarządzania bezpieczeństwem informacji, cyberodporności, analizy ryzyka, reagowania na incydenty oraz nadzorowania zgodności z wymaganiami prawnymi i normatywnymi:

- Zrozumienie wymagań prawnych (NIS 2, ustawa o KSC, RODO), normatywnych (ISO/IEC 27001, ISO/IEC 27005, ISO 31000, ISO 22301) oraz najlepszych praktyk (NIST CSF).
- Nabycie umiejętności budowania i nadzorowania systemu zarządzania bezpieczeństwem informacji (ISMS), prowadzenia analizy ryzyka, tworzenia polityk i procedur, zarządzania incydentami i ciągłością działania.
- Rozwijanie kompetencji w zakresie zarządzania dostawcami, kultury bezpieczeństwa oraz planowania audytów i ciągłego doskonalenia.
- Poznanie specyfiki zarządzania ryzykiem AI w kontekście nowych technologii.

Program szkolenia:

1. **Zakres roli i regulacje**:
   - omówienie obowiązków pełnomocnika, przepisów prawa, roli CSO/CISO w organizacji, wymogów raportowania do zarządu i organów nadzoru.
2. **System zarządzania bezpieczeństwem informacji**:
   - budowa ISMS zgodnie z ISO/IEC 27001,
   - integracja z innymi systemami (ISO 22301, ISO 31000),
   - znaczenie auditu zgodności.
3. **Metodyka analizy ryzyka**:
   - szczegółowe stosowanie ISO/IEC 27005 i ISO 31000 w identyfikacji, analizie i ocenie ryzyka,
   - wykorzystanie IEC 31010 do doboru technik (np. analiza FMEA, drzewa błędów),
   - prowadzenie „risk register"; ocena ryzyk łańcucha dostaw,
   - ***Ćwiczenie*: opracowanie macierzy ryzyka dla kluczowego procesu biznesowego.**
4. **Polityki i procedury**:
   - tworzenie i utrzymywanie polityki bezpieczeństwa, standardów, wytycznych i procedur operacyjnych (kontrola dostępu, zarządzanie hasłami, klasyfikacja informacji, wymogi zasobów ludzkich),
   - zgodność z RODO i NIS 2.
5. **Techniczne środki ochrony**:
   - przegląd technologii (firewalle, IDS/IPS, SIEM, EDR, DLP, szyfrowanie, segmentacja sieci, zarządzanie lukami), bezpieczeństwo chmury i usług SaaS,
   - konfiguracja i monitorowanie narzędzi.
6. **Zarządzanie incydentami i ciągłość działania**:
   - opracowanie procedur IR (Incident Response), definiowanie ról i odpowiedzialności, klasyfikacja incydentów, komunikacja wewnętrzna i zewnętrzna,
   - planowanie i testowanie planów ciągłości działania zgodnie z ISO 22301,

- integracja z ISO/IEC 27005.

7. **Zarządzanie dostawcami i łańcuchem dostaw**:
   - planowanie i prowadzenie due diligence dostawców, wymagania umowne, ocena ryzyka outsourcingu, monitorowanie umów i SLA,
   - podejście do NIS 2 w kontekście dostawców usług kluczowych.
8. **Kultura bezpieczeństwa i szkolenia**:
   - budowanie świadomości cyberbezpieczeństwa wśród pracowników, programy szkoleń, kampanie edukacyjne, phishing simulations, system nagród.
9. **Audit i ciągłe doskonalenie**:
   - planowanie auditów wewnętrznych, zbieranie i analiza danych, monitorowanie KPI, przeglądy zarządzania; reagowanie na niezgodności, działania korygujące i prewencyjne,
   - wykorzystywanie wyników analizy ryzyka do planowania inwestycji i budżetu.
10. **Nowe technologie i ryzyka AI**:
    - przegląd trendów (AI, IoT, 5G), zarządzanie ryzykiem AI zgodnie z NIST AI RMF i ISO/IEC 42001,
    - ocena wpływu AI na systemy bezpieczeństwa.
11. **Projekt:**
    - **uczestnicy przygotowują kompleksowy program cyberbezpieczeństwa dla przykładowej organizacji, obejmujący polityki, analizę ryzyka, procedury IR i szkolenia,**
    - **prezentacja i omówienie projektu.**

EGZAMIN

👥 Grupa odbiorcza

Szkolenie przeznaczone jest dla osób odpowiedzialnych za zarządzanie cyberbezpieczeństwem, bezpieczeństwem informacji, zgodnością regulacyjną oraz ciągłością działania organizacji, w szczególności dla:

- kandydatów na Pełnomocników ds. cyberbezpieczeństwa,
- obecnych Pełnomocników ds. bezpieczeństwa informacji i cyberbezpieczeństwa,
- CISO, CSO oraz menedżerów IT,
- specjalistów ds. cyberbezpieczeństwa i bezpieczeństwa informacji,
- compliance managerów,
- auditorów wewnętrznych systemów zarządzania,
- osób odpowiedzialnych za zarządzanie ryzykiem, ciągłość działania i ochronę danych osobowych,
- kadry kierowniczej nadzorującej obszar IT, bezpieczeństwa, jakości, ryzyka lub compliance.

🚀 Korzyści po szkoleniu

Po ukończeniu szkolenia uczestnicy będą potrafili:

- Skutecznie pełnić rolę Pełnomocnika ds. cyberbezpieczeństwa w organizacji.
- Interpretować wymagania NIS 2, KSC, RODO oraz kluczowych norm ISO i standardów branżowych.
- Projektować, wdrażać i nadzorować system zarządzania bezpieczeństwem informacji.
- Identyfikować, analizować i oceniać ryzyka cyberbezpieczeństwa.
- Prowadzić i aktualizować rejestr ryzyk oraz dobierać odpowiednie działania zabezpieczające.
- Opracowywać polityki, procedury, instrukcje i standardy bezpieczeństwa.
- Zarządzać incydentami cyberbezpieczeństwa oraz organizować proces reagowania.
- Integrować cyberbezpieczeństwo z ciągłością działania organizacji.
- Oceniać ryzyka związane z dostawcami, outsourcingiem i łańcuchem dostaw.
- Budować świadomość i kulturę bezpieczeństwa wśród pracowników.
- Przygotowywać organizację do audytów, przeglądów zarządzania i działań doskonalących.
- Uwzględniać ryzyka wynikające z nowych technologii, w tym AI, IoT, chmury i usług SaaS.

+48 32 724 35 86
info@sudharapolska.com
www.sudharapolska.com

Metodyka szkolenia

Szkolenie prowadzone jest w formule warsztatowo-eksperckiej, łączącej przekazanie uporządkowanej wiedzy z praktycznym zastosowaniem wymagań prawnych, normatywnych i organizacyjnych.

Metodyka obejmuje:

- interaktywne wykłady eksperckie,
- analizę wymagań prawnych i normatywnych,
- studia przypadków z obszaru cyberbezpieczeństwa,
- ćwiczenia praktyczne z identyfikacji i oceny ryzyka,
- pracę na przykładach polityk, procedur i rejestrów,
- warsztaty dotyczące reagowania na incydenty,
- analizę scenariuszy naruszeń bezpieczeństwa,
- pracę zespołową nad programem cyberbezpieczeństwa dla przykładowej organizacji,
- dyskusje moderowane i wymianę doświadczeń uczestników,
- egzamin potwierdzający zrozumienie kluczowych zagadnień.

Szkolenie kładzie nacisk na praktyczne przygotowanie uczestników do samodzielnego działania w roli Pełnomocnika ds. cyberbezpieczeństwa oraz do współpracy z zarządem, IT, compliance, auditem, dostawcami i właścicielami procesów biznesowych.

Czas trwania szkolenia – 3 dni