TÜVNORD

Passion for Safety

Akademia Kompetencji TUV NORD

CyberSecurity Ekspert

TÜV NORD Polska

Rew.29/11/23, 09:44

CyberSecurity Ekspert

Akademia Kompetencji TUV NORD to programy edukacyjne rozwijające umiejętności na wielu płaszczyznach. Jedną z nich jest cyberbezpieczeństwo i proponowany tu cykl CyberSecurity Ekspert. Jest to kompleksowy program pozwalający na uzyskanie wiedzy niezbędnej dla osób zajmujących się ochroną zasobów firmy, odpowiedzialnych za jej ciągłość działania czy też skuteczną reakcje na incydenty. Ten program to kompendium wiedzy dla wszystkich organizacji wyznaczonych jako podmioty kluczowe lub ważne, a zdobyta wiedza pomoże spełnić wymagania NIS 2. W ramach programu istnieje możliwość uzyskania dwóch certyfikatów akredytowanych w PCA a więc tych które znajdują się na wykazie Ministra Cyfryzacji (Rozp. z dnia 12.10.2018, poz. 1999).

Dla kogo?

Akademia Kompetencji CyberSecurity Ekspert dedykowana jest osobom odpowiedzialnym za bezpieczeństwo informacji w firmie, za jej ciągłość działania oraz zapobieganie i zarządzanie incydentami. Będzie szczególnie przydatna w firmach objętych ustawą o KSC oraz dla osób realizujących audyty w zakresie cyberbezpieczeństwa. Wszystkie moduły zawierają w sobie elementy warsztatowe co pozwala na przekucie nowej wiedzy w praktykę.

Pełny cykl szkoleń: CyberSecurity Ekspert składa się z 3 modułów:

- Audytor wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg ISO 27001 (PCA)
- Audytor wiodący Systemu Zarządzania Ciągłością Działania wg ISO 22301 (PCA)
- Incident Response Manager.

Każdy z modułów zakończony jest egzaminem i w przypadku pozytywnego wyniku wydaniem certyfikatu (w tym dwóch akredytowanych w PCA). Cały cykl również jest zakończony egzaminem obejmującym program wszystkich 3 modułów.

Audytor wiodący systemu zarządzania bezpieczeństwem informacji wg ISO 27001

AKREDTACJA PCA

Czas trwania: 5 dni (40h)

Szkolenie przeznaczone jest dla

osób, które chcą zajmować się certyfikacją systemów zarządzania bezpieczeństwem informacji lub które z racji pełnionej funkcji (administrator, pełnomocnik, konsultant) zajmują się bezpieczeństwem i chcą poszerzyć swoją wiedzę w zakresie zarządzania bezpieczeństwem informacji. Kurs jest świetną propozycją dla tych wszystkich, którzy inwestują w swój rozwój zawodowy i chcą funkcjonować na dynamicznie rozwijającym się rynku usług związanych z bezpieczeństwem informacji.

Celem szkolenia jest

nabycie wiedzy w zakresie zarządzania bezpieczeństwem informacji oraz nabycie umiejętności praktycznego zastosowania wymagań zawartych w normie ISO/IEC 27001.

Tematyka szkolenia

- Wprowadzenie do bezpieczeństwa informacji
  - Systemowe zarządzanie bezpieczeństwem informacji.
  - Korzyści / wartości dodane dla organizacji
- Omówienie wymagań normy PN-EN ISO/IEC 27001 (w zakresie 1-10)
  - Identyfikacja wymagań dokumentacyjnych (w zakresie 1-10)
- Omówienie zabezpieczeń z załącznika A PN-EN ISO/IEC 27001
  - Identyfikacja wymagań dokumentacyjnych (w zakresie załącznika A)
- Wprowadzenie do procesu audytu – wytyczne ISO 19001: 2018
  - Kryteria audytów
  - Rodzaje audytów
  - Wytyczne dot. audytowania systemów zarządzania
  - Terminy i definicje
- Zasady audytowania – 7 zasad audytowania
- Zarządzanie programem audytów
  - Ustalenie celów programu audytu
  - Identyfikacja i ocena ryzyk i szans programu audytów
  - Role i odpowiedzialności osób zarządzających programem audytów
  - Kompetencje osób zarządzających programem audytów
  - Ustalenie zakresu programu audytów
  - Określenie zasobów dla programu audytów

- Wdrożenie programu audytów
  - Określenie celów, kryteriów i zakresu dla każdego audytu
  - Wybór i ustalenie metod audytu
  - Wybór członków zespołu audytu
  - Przydzielenie odpowiedzialności za dany audyt audytorowi wiodącemu
  - Zarządzanie wynikami programu audytów
  - Zarządzanie i utrzymanie zapisów dotyczących programu audytów
  - Monitorowanie programu audytów
  - Przegląd i doskonalenie programu audytów
- Przeprowadzenie audytu
  - Przegląd czynności wykonywanych w ramach typowego audytu
  - Inicjacja audytu – nawiązanie pierwszego kontaktu z audytowanym
  - Określenie wykonalności audytu
- Przygotowanie działań audytowych
  - Przygotowanie przeglądu udokumentowanych informacji
  - Przygotowanie planu audytu
  - Przydzielenie pracy zespołowi audytowemu
  - Przygotowanie dokumentów roboczych
- Przeprowadzenie działań audytowych
  - Przypisanie ról i obowiązków przewodników i obserwatorów
  - Przeprowadzenie spotkania otwierającego
- Komunikacja podczas audytu
  - Dostęp do dowodów audytowych
  - Zbieranie i weryfikowanie informacji
  - Generowanie wyników audytu - rejestrowanie niezgodności i innych obserwacji (dowodów)
- Opracowanie ustaleń z audytu
  - Przygotowanie spotkania zamykającego
  - Wnioski z audytu
  - Przeprowadzenie spotkania zamykającego
  - Przygotowanie i rozpowszechnianie raportu z audytu
- Przygotowanie i rozpowszechnianie raportu z audytu
  - Przygotowanie raportu z audytu
  - Rozpowszechnianie raportu z audytu
- Zakończenie audytu
- Przeprowadzenie działań po audytowych
- Kompetencje i ocena audytorów
  - Określenie kompetencji audytora
  - Postawy i zachowania
  - Wiedza i umiejętności audytorów systemu zarządzania
  - Specyficzne kompetencje audytorów
  - Kompetencje audytora wiodącego
  - Nabywanie kompetencji audytora
  - Nabywanie kompetencji lidera zespołu audytowego
  - Ocena audytorów – przeprowadzenie oceny
  - Utrzymanie i ewaluacja kompetencji audytorów
- Ćwiczenia – scenki audytowe

Audytor wiodący systemu zarządzania wg ISO 22301

AKREDTACJA PCA

Czas trwania: 5 dni (40h)

Szkolenie przeznaczone jest dla

osób, które chcą zajmować się certyfikacją systemu opartego na ISO 22301 lub które z racji pełnionej funkcji (pełnomocnik, konsultant) zajmują się ciągłością działania i chcą poszerzyć wiedzę w tym zakresie. Kurs jest świetną propozycją dla tych, którzy inwestują w swój rozwój zawodowy i chcą funkcjonować na dynamicznie rozwijającym się rynku usług związanych z ciągłością działania.

Celem szkolenia jest:

- poznanie wymagań normy ISO 22301:2020
- poznanie procesu audytu wg 19011:2018
- poznanie zadań Audytora Wiodącego
- zdobycie umiejętności przygotowania do audytu 1, 2, i 3-ciej strony w roli Audytora Wiodącego
- zdobycie umiejętności przeprowadzenia audytu 1, 2, i 3-ciej strony
- zdobycie umiejętności dokumentowania wyników audytu

Program:

- System zarządzania ciągłością biznesu wg 22301 – BCMS
- Norma ISO 22301 jako nowe podejście do zarządzania ciągłością. Inne przydatne standardy
- Projektowanie systemu zarządzania ciągłością biznesu wg 22301 – BCMS
  - Określenie zakresu, celów
  - Wymagania organizacyjne, mechanizmy ciągłego doskonalenia
  - Polityki, procedury – dokumentacja BCMS
  - Zasady prowadzenia analizy BIA
  - Analiza ryzyk
  - Strategia zarządzania ciągłością – elementy składowe
  - Zarządzanie incydentami - elementy składowe
  - Projektowanie planów ciągłości działania wg ISO 22301.
- Mini BCMS'. Zajęcia o parte o przypadek studyjny. Zadaniem uczestników jest zaprojektowanie najważniejszych elementów zarządzania ciągłością działania:
  - Zakres, cele, określenie wymagań
  - Analiza BIA
  - Prosta analiza ryzyka
  - Zaprojektowanie strategii zarządzania ciągłością
  - Przygotowanie planu ciągłości działania
  - Prezentacja wyników
- Audytowanie
  - Zadania audytora
  - Wprowadzenie do audytowania
  - Rodzaje audytów
  - Opis pełnego proesu audytu
- Warsztat audytora – ćwiczenia
  - Inicjowanie audytu
  - Przygotowanie działań audytowych
  - Przeprowadzenie działań audytowych
  - Prowadzenie audytu
  - Ustalenia z audytu
  - Spotkanie zamykające
  - Raport
  - Zakończeniue audytu
  - Działania poaudytowe

Incident Response Manager

Czas trwania: 2 dni (16h)

Szkolenie przeznaczone jest dla

osób, które z racji pełnionych funkcji będą zaangażowane w postępowanie z potencjalnymi incydentami bezpieczeństwa informacji.

Celem szkolenia jest nabranie praktycznych umiejętności w zakresie zarządzania incydentem bezpieczeństwa informacji

Tematyka szkolenia:

- Informatyka śledcza, definicja, znaczenie
- Cele informatyki śledczej
- Dowód elektroniczny
- Co nam wolno, a na co powinniśmy uważać
- Założenia informatyki śledczej
- Polskie i światowe praktyki wykorzystywane w informatyce śledczej
- Procesy analizy śledczej
- Sposób zabezpieczania i gromadzenia danych
- Reguły i zasady przeprowadzania analizy śledczej
- Opis i przedstawienie narzędzi wykorzystywanych przez śledczych
- Opis i przedstawienie programów wykorzystywanych przez śledczych
- Proces zabezpieczenia materiału dowodowego
- Co to jest kopia binarna i po co jest nam w ogóle potrzebna
- Jak przechowywać dowód elektroniczny
- Zabezpieczanie dysków, poczty elektronicznej, strony internetowej, innych nośników
- Zabezpieczanie informacji ulotnych
- Wstępne analizy
- Przekazanie materiału dowodowego
- Informatyka śledcza w świecie aplikacji mobilnych
- Zarządzanie incydentami wg najlepszych praktyk ISO
- Przegląd wymagań ISO 27001 oraz ISO 27035
- Planowanie procesów: wykrywania, raportowania, reakcji na incydenty

Warunki uczestnictwa

Cena: 9 900 zł + 23% VAT

Koszt udziału w Akademii obejmuje:

- udział we wszystkich modułach tematycznych
- udział w procesach egzaminacyjnych (również akredytowanych) po każdym z modułów
- egzamin końcowy
- wydanie certyfikatu ukończenia Akademii Kompetencji CyberSecurity Expert

Istnieje możliwość uczestnictwa w pojedynczych modułach lub podejścia do samego egzaminu jeśli osoba zainteresowana uczestniczyła już w danym szkoleniu. Szczegółowy opis warunków znajduje się w Regulaminie

TÜVNORD

Passion for Safety

Masz pytania ?

Skontaktuj się z nami

TÜV NORD Polska

Mickiewicza 29
40-085 Katowice

bi@tuv-nord.pl
tuv-nord.pl

Magdalena Brudzyńska
tel.: 781 700 029
m.brudzynska@tuv-nord.pl

Kinga Szczygieł
tel.: 601 458 830
k.szczygiel@tuv-nord.pl