Co potrafi osoba posiadająca kwalifikację?

Posiadacz certyfikatu z zakresu zarządzania bezpieczeństwem informacji w organizacji:

- wskazuje i omawia sposoby ochrony informacji w tym: ochrony danych osobowych, cyberbezpieczeństwa oraz informacji niejawnych,
- definiuje ryzyka związane z ochroną informacji,
- omawia proces utrzymania i doskonalenia systemu bezpieczeństwa informacji w organizacji,
- interpretuje normy ISO 27001, 27002, 27005 oraz zapisy Ustawy KRI,
- analizuje zgodność procedur wewnętrznych organizacji z wymaganiami stawianymi przez przepisy na gruncie bezpieczeństwa informacji,
- ocenia skuteczność zabezpieczeń stosowanych w organizacji,
- opracowuje i aktualizuje dokumentację systemu zarządzania bezpieczeństwem informacji,
- klasyfikuje informacje i dobiera adekwatną formę ochrony,
- omawia zasady reakcji na incydenty związane z naruszeniem bezpieczeństwa informacji.

Cel szkolenia

Oferowane szkolenie „Bezpieczeństwo informacji" jest unikalną odpowiedzią na zapotrzebowanie rynkowe. Treści prezentowane są przez trenera reprezentującego odmienne doświadczenia i perspektywę dzięki czemu możliwe jest holistyczne ujęcie tematu. Celem szkolenia jest podniesienie kwalifikacji uczestników szkolenia poprzez zapoznanie ich z wymaganiami systemu zarządzania bezpieczeństwem informacji, istotnymi wymaganiami z zakresu ochrony danych osobowych oraz praktycznym sposobem zarządzania audytem wewnętrznym bezpieczeństwa informacji w organizacji.

Do kogo adresowana jest kwalifikacja?

Kwalifikacja adresowana jest przede wszystkim do osób:

- chcących potwierdzić nabyte w trakcie wykonywanych obowiązków zawodowych kwalifikacje,
- pełnomocników systemu zarządzania bezpieczeństwem informacji,
- audytorów wewnętrznych pragnących usystematyzować wiedzę na temat procesów bezpieczeństwa informacji,
- stanowiących średnią lub wyższą kadrę zarządzającą procesami zgodności w organizacji,

- stanowiących średnią i wyższą kadrę zarządzającą zespołami IT w obszarach bezpieczeństwa,
- pragnących posiąść przekrojową wiedzę dotyczącą podniesienia bezpieczeństwa organizacji,
- zajmujących się zarządzaniem bezpieczeństwem w organizacjach.

Gdzie można znaleźć zatrudnienie?

Posiadacz kwalifikacji może znaleźć zatrudnienie:

- w przedsiębiorstwach lub instytucjach publicznych posiadających zespoły zajmujące się bezpieczeństwem,
- w przedsiębiorstwach chcących zwiększyć swoją konkurencyjność na rynku dzięki wskazaniu działań zgodnie z bezpieczeństwem informacji,
- w instytucjach publicznych (podmiotach zobowiązanych) w ramach, których obowiązkowo muszą być stosowane przepisy Ustawy KRI,
- w organizacjach, które planują rozszerzyć swoje procesy bezpieczeństwa celem wsparcia biznesu.

Informacje o szkoleniu

Szkolenie zostało zaprojektowane, aby pomóc liderom organizacji i specjalistom ds. bezpieczeństwa lepiej zrozumieć, zarządzać i redukować zagrożenia bezpieczeństwa informacji. Szkolenie zapewnia pozyskanie wiedzy w stopniu wystarczającym do nadzorowania systemów bezpieczeństwa informacji w organizacjach. Umożliwia zapoznanie się z zasadami, technikami i metodami prowadzenia analiz, weryfikacji i monitoringu wdrożonych rozwiązań z tego obszaru.

Wymogi dla trenera

Posiada udokumentowaną wiedzę, w zakresie Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z ISO 27001 oraz doświadczenie zawodowe w obszarze kwalifikacji.

Egzamin

Egzamin praktyczny przeprowadzany jest z wykorzystaniem notatek i komputera, trwa 30 minut, Egzamin przeprowadzany w formie testu jednokrotnego wyboru (30 pytań: 7 pytań z prawa, 7 pytań z psychologii i 16 pytań z norm ISO 27001 i 27002).

Zasady przeprowadzania egzaminu (walidacja)

Walidacja dla kwalifikacji „Zarządzanie bezpieczeństwem informacji” przeprowadzana jest przez Stowarzyszenie Ekspertów Bezpieczeństwa RP oraz GMP Defence Sp. z o.o.

1. Metody stosowane w walidacji

Egzamin praktyczny przeprowadzany jest w pomieszczeniu wyposażonym w stoliki, krzesła i trwa 30 minut, polega na testu tj. przyporządkowania określonych korzyści z wdrożenia systemu bezpieczeństwa informacji względem podanych kategorii dla organizacji.

2. Certyfikaty i odznaki cyfrowe potwierdzające kwalifikacje

Certyfikaty i odznaki cyfrowe potwierdzające kwalifikację wydawane są na podstawie dostarczonych potwierdzeń wyników egzaminu. Certyfikat i odznaka cyfrowa są wystawiane dla uczestników, którzy uzyskali pozytywny wynik egzaminu. Certyfikaty i cyfrowe odznaki są wystawiane w terminie maksymalnie 30 dni roboczych od daty egzaminu.

3. **Uczestnicy mają prawo do złożenia odwołania od wyniku egzaminu** (patrz procedura odwoławcza).

4. Kryteria oceny

Ocena merytoryczna posiadanej wiedzy w zakresie wdrożenie systemu bezpieczeństwa informacji w organizacji

5. Proces zgłoszenia i obsługi egzaminu:

- Stowarzyszenie Ekspertów Bezpieczeństwa RP przygotowuje listę uczestników egzaminu na podstawie prawidłowo wypełnionych Formularzy Kandydata/ki,
- przed egzaminem uczestnikom przekazywane są zasady jego oceniania,
- potwierdzenie odbycia egzaminu jest podpisywane przez uczestników oraz egzaminatorów,
- wyniki egzaminu są protokołowane - egzaminatorzy przygotowują arkusze dla egzaminu wraz z dokumentacją,
- kompletną dokumentację egzaminu egzaminatorzy przesyłają w oryginałach do Stowarzyszenia,
- dokumentacja egzaminu jest przechowywana w Stowarzyszeniu Ekspertów Bezpieczeństwa RP.