Kod szkolenia: **HL949S**

Tytuł szkolenia: **Kompleksowe Przygotowanie do Egzaminu CISMP**

Certificate in Information Security Management Principals

Dni: 5

Authorized HP Training Reseller

Opis:

Ten akredytowany cykl kursów zawiera 3 dniowy kurs Information Security Essentials (HL945S) oraz 2 dniowy kurs Information Security Essentials Plus (HL946S). Szkolenie jest akredytowane przez Information Systems Examination Board (ISEB) reprezentowany przez British Computer Society (BCS) i przygotowuje Cię do cenionego i rozpoznawalnego na rynku IT egzaminu Certificate in Information Security Management Principles (CISMP).

Cel szkolenia

Kurs Information Security Essentials przygotuje Cię do spojrzenia na Twoją organizację i jej działanie poprzez pryzmat bezpieczeństwa informacji, a także przygotuje do wdrożenia kompleksowej strategii bezpieczeństwa informacji, która pozwoli Ci na bycie konkurencyjnym. Szkolenie prezentuje także praktyczne przykłady jak wdrożyć środki bezpieczeństwa i metody minimalizujące ryzyko w Twojej organizacji.

Niezależnie od tego czy odpowiadasz za kierowanie czy też za stronę techniczną bezpieczeństwa, ten kurs pozwoli Ci poznać, czym jest bezpieczeństwo informacji uwzględniając zarzadzanie ryzykiem, techniczne i administracyjne zabezpieczenia, przepisy prawa, fizyczne i osobowe zabezpieczenia, standardy bezpieczeństwa (np. ISO 27001/2), utrzymanie ciągłości działania i wiele innych.

Podczas kursu Information Security Essentials Plus poznasz element wdrożenia ISO 27001 i regulacje we wskazanych obszarach cyklu bezpieczeństwa informacji. Poznasz podstawy prawne i wymagania, które dotyczą Twojego programu bezpieczeństwa informacji oraz rozwoju oprogramowania, praktyk, które wspierają wymagania integracji bezpieczeństwa oraz

najlepszych praktyk w zakresie obsługi incydentów, przygotowania się do audytu, a także inne zagadnienia z tego zakresu.

Ten kurs prowadzi do kolejnych poziomów wiedzy oraz bardziej zaawansowanych certyfikatów zarówno w zakresie zarządzania, jak i technicznych elementów bezpieczeństwa, takich jak CISSP, Security+ i CCSK
oraz odpowiada aktualnym programom zarządzania projektami i utrzymaniem.

Adresaci szkolenia

Szkolenie dedykowane jest osobom, które chciałyby przystąpić do egzaminu BCS Certificate in Information Security Management Principles (CISMP), kierownictwu IT oraz członkom Zespołów Zarządzania Bezpieczeństwem informacji, szefom bezpieczeństwa i systemów IT, jak również osobom przygotowującym się do uzyskania certyfikatu z zakresu ISO/IEC 27001, ISO/IEC 27002, CISMP, CISSP, Security+ or CCSK.

Wymagania

Od osób chcących wziąć udział w szkoleniu wymagana jest podstawowa znajomość systemów operacyjnych i sieci IT.
Doświadczenie z zarządzania sieciami, zarządzaniu projektami oraz organizacją będzie pomocne, ale nie jest niezbędne.

Informacje dodatkowe

Szkolenie może być zrealizowane w języku polskim lub angielskim. Uczestnicy otrzymują akredytowane materiały szkoleniowe w języku angielskim.

Program szkolenia:

Moduł 1: Ustanowienie podstaw bezpieczeństwa.

- Przykłady jak ważne jest bezpieczeństwo informacji.
- Jak bezpieczeństwo może decydować o przewadze w businessie.
- Modele dojrzałości zapewnienie informacji.
- Identyfikacja właściwych źródeł wymogów zgodności prawnych, regulacyjnych, klienckich.

Moduł 2: Definicja kluczowych założeń bezpieczeństwa informacji.

- Bezpieczeństwo informacji oraz kluczowe elementy: poufność, integralność, dostępność.
- Spełnienie wymagań w bezpieczeństwie informacji.
- Różnice pomiędzy zagrożeniami, podatnościami a atakami.
- Zastosowanie definicji w środowisku.
- Identyfikacja form zagrożeń.
- Wykaz typowych podatności w firmach.
- Omówienie, co jest przyczyną incydentów bezpieczeństwa.

Moduł 3: Zarządzanie bezpieczeństwem informacji w organizacji.

- Wskazanie przewagi stosowania istniejących wytycznych.
- Pokazanie cyklu zarządzania bezpieczeństwem.
- Wskazanie kluczowych ról, odpowiedzialności i interakcji.
- Różnice pomiędzy polityką, standardem, procedurą a wytycznymi.
- Charakterystyka dobrej polityki.
- Jak ważne jest ogłoszenie polityki.

Moduł 4: Wprowadzenie do zagrożeń IT, podatności i ataków.

- Omówienie podatności w komunikacji klient/serwer.
- Omówienie, dlaczego duże organizacje są zagrożone.
- Identyfikacja fizycznych, technicznych i socjotechnicznych zagrożeń.
- Identyfikacja i Omówienie najczęściej występujących ataków.
- Omówienie najczęściej występujących przykładów ataków socjotechnicznych.

Moduł 5: Ocena ryzyka.

- Role zarządzania ryzykiem w bezpieczeństwie informacji oraz ich powiązanie z cyklem zarządzania bezpieczeństwem.
- Szacowanie ryzyka szczątkowego dla Twojej organizacji w różnych kluczowych obszarach.
- Różnice pomiędzy analizą wpływu na działalność a ocena ryzyka.
- Różnice pomiędzy jakościowym a ilościowym analizowaniem ryzyka.
- Omówienie skanowania podatności.
- Przykładowe narzędzia do skanowanie portów komunikacyjnych oraz innych podatności.
- Wskazanie narzędzi kryteriów wyboru i porównania.
- Przygotowanie raportu ze skanowania.

Moduł 6: Kontrola dostępu.

- Omówienie wagi kontroli dostępu w implementacji bezpieczeństwa informacji.
- Wskazanie jak autoryzacja i weryfikacja działają razem w celu zapewnienia kontroli

dostępu.
- Zarys, dlaczego techniczne i fizyczne zabezpieczenia są wspólnie bardzo ważne.

Moduł 7: Wybór zabezpieczeń

- Wskazanie typowych zabezpieczenia dla każdej z kategorii zagrożenia.
- Wskazanie przeciwdziałania ze względu na strategię.
- Omówienie ważności zarządzania aktualizacją i patchowaniem.
- Kategoryzacja zabezpieczeń fizycznych.
- Omówienie przeciwdziałania technicznego.
- Identyfikacja pozycji firewall w architekturze sieciowej i w strefie DMZ.
- Wskazanie działania, jakie firewall może podjąć w celu rozpoznania ruchu sieciowego.
- Omówienie działania IPS (Intrusion Prevention Systems).
- Omówienie jak IPS wykrywa atak.
- Porównanie typów IPS-ów.
- Omówienie jak VPN (Virtual Private Networking) wspiera cele bezpieczeństwa.
- Omówienie jak szyfrowanie wspiera bezpieczeństwo.
- Omówienie jak można stosować szyfrowanie.
- Różnice pomiędzy szyfrowaniem symetrycznym a asymetrycznym.
- Omówienie pozycjonowania skanerów antywirusowych.

Moduł 8: Planowanie zabezpieczeń dla konsumeryzacji i rozwiązań Cloud (chmury obliczeniowej) w IT.

- Omówienie wpływu konsumeryzacji IT.
- Omówienie zagrożenia i podatności dla rozwiązań mobilnych.
- Podsumowanie interwencji dla rozwiązań mobilnych.
- Identyfikacja zagrożeń ze strony mediów społecznościowych.
- Podsumuj zabezpieczenia dla mediów społecznościowych.
- Omówienie relacji pomiędzy konsumeryzacją a rozwiązaniami chmury obliczeniowej.
- Różnice pomiędzy rozwiązaniami chmury obliczeniowej i usługami.
- Identyfikacja ryzyka dla różnych przykładów wykorzystania chmury obliczeniowej.
- Przykłady zabezpieczeń dla chmury obliczeniowej.

Moduł 9: Planowanie utrzymania ciągłości działania oraz przywracanie po awarii

- Omówienie ważności ciągłości działania.
- Przykłady, dlaczego jest to takie ważne.
- Omówienie ciągłości działania i terminów z tym związanych.
- Omówienie relacji z zarządzaniem ryzykiem.
- Wskazanie elementów utrzymania ciągłości działania.
- Porównanie i różnice pomiędzy BCP a DRP.
- Omówienie kluczowych elementów oraz prawne zapisy dostępności usług.
- Omówienie weryfikacji rozwiązań redundantnych.
- Rozważania na temat redundancji.

Moduł 10: Strategie wdrożenia dla właściwego poziomu bezpieczeństwa.

- Wskazanie kilku najczęściej pomijanych zagrożeń dla bezpieczeństwa IT.
- Wskazanie najlepszych praktyk w zakresie zatrudniania i szkolenia użytkowników/pracowników.

Moduł 11: Zarządzanie bezpieczeństwem Informacji.

- Wskazanie równowagi pomiędzy wymogami organizacji a zarządzaniem bezpieczeństwem.
- Omówienie holistycznego podejścia do zarządzania w organizacji.
- Wskazanie, jak bardzo ważne jest wsparcie ze strony zarządu dla bezpieczeństwa informacji.
- Wskazanie jak wymagania bezpieczeństwa informacji przenikają przez poszczególne szczeble zarządzania.
- Wskazanie ról w organizacji powiązanych z bezpieczeństwem informacji.
- Omówienie procesu wdrażania polityki.

Moduł 12: Ramy prawne.

- Wskazanie odpowiednich podstaw prawnych w różnych regionach świata.
- Omówienie typowych elementów ochrony danych.
- Zidentyfikowanie typowych naruszeń ochrony danych.
- Omówienie jak organizacje z różnymi lokalizacjami mogą poradzić sobie z różnymi systemami prawnymi.
- Wskazanie odpowiedzialności organizacji w zakresie monitorowania użytkowników/pracowników.

Moduł 13: Standardy bezpieczeństwa.

- Wskazanie najważniejszych standardów dla różnych regionów.
- Omówienie standardów ISO i powiązania między nimi.
- Wskazanie kolejnych etapów w cyklu SZBI.
- Wskazanie elementów dokumentacji SZBI.
- Identyfikacja poziomów bezpieczeństwa.
- Rozpoznawanie certyfikowanych produktów.
- Wskazanie kluczowych elementów zaleceń NIST.
- Omówienie, dlaczego ważne są standardy szyfrowania.

Moduł 14: Programowanie aplikacji dla bezpieczeństwa.

- Omówienie najlepszych praktyk z zakresu programowania aplikacji w celu zachowanie bezpieczeństwa.

Moduł 15: Audyt bezpieczeństwa.

- Omówienie kluczowych terminów związanych z audytem.
- Opis procesów związanych z audytem.
- Wskazanie celu audytu.
- Wskazanie typów audytu.
- Omówienie zadania audytora.
- Omówienie elementów dokumentacji poaudytowej.

Moduł 16: Zarządzanie incydentami.

- Omówienie kolejnych kroków w przypadku wystąpienia incydentu.
- Wskazanie elementów raportu związanego z incydentem bezpieczeństwa.
- Omówienie procesów zbierania dowodów związanych z incydentem.