Przygotowanie do egzaminu na certyfikat CISM (Certified Information Security Manager)

Szkolenie 8 dniowe (8 spotkań 1 dniowych) 64 godzin zajęć –

możliwość uzyskania 64 CPE)

zajęcia szkoleniowo-warsztatowe, środa lub czwartek (do ustalenia z grupą)

Termin zajęć: do ustalenia

Miejsce: Warszawa lub okolice

Cena netto 5600 PLN + 22% VAT (brutto 6832,00 PLN) +280 USD cena materiałów ISACA

Odbiorcy:

Warsztaty kierowane są w szczególności do:

- osób odpowiedzialnych za wszelkie aspekty bezpieczeństwa w organizacji
- osób odpowiedzialnych za zarządzanie ryzykiem
- osób pełniących funkcje Pełnomocników Ochrony Informacji Niejawnych,
- osób będących Koordynatorami Bezpieczeństwa w Pionach,
- osób zainteresowanych maksymalizacją efektu synergii w zarządzaniu

Program:

W programie stosownie do wymogów egzaminacyjnych ISACA poruszone zostaną zagadnienia z obszaru:

- Zarządzania bezpieczeństwem Informacji,
- Zarządzanie Ryzykiem,
- Rozwój programu bezpieczeństwa informacji,

- Zarządzanie programem bezpieczeństwa informacji,
- Zarządzanie reakcjami na incydenty.

Zajęcia będą prowadzone metodą warsztatową

KONSPEKT SZKOLENIA – część 1.

Co osiągniesz poprzez udział w szkoleniu?
(cele szkoleniowe)

- Przygotujesz się do egzaminu testowego do uzyskania certyfikatu CISM zapewniającego uznanie na całym świecie kompetencji zawodowych w obszarze zarządzania bezpieczeństwem informacji (więcej informacji www.isaca.org oraz www.isaca.org.pl).
- Zdobędziesz lub usystematyzujesz sobie wiedzę z obszaru:
  - Zarządzanie bezpieczeństwem Informacji ,
  - Zarządzania ryzykiem
  - Zarządzania programem bezpieczeństwa informacji,
  - Zarządzania bezpieczeństwem IT
  - Zarządzania odpowiedzią na incydent

UWAGA! Egzamin nie odbywa się w języku polskim.

Komu polecamy szkolenie?
(grupa celowa, wymagania wstępne)

- Doświadczonym menadżerom bezpieczeństwa informacji,
- Osobom nadzorującym ,planującym, nadzorującym i oceniającym obszar bezpieczeństwa informacji w skali firmy
- Kadrze kierowniczej i analitykom odpowiedzialnym za bezpieczeństwo informatyczne,
- Menadżerom odpowiedzialnym za operacyjne zarządzanie obszarem bezpieczeństwa informacji,
- Osobom zaangażowanym w zapewnienie bezpieczeństwa informacji i ciągłości działania biznesu

Certyfikat

Wymagania wstępne:
Podstawowa wiedza z zakresu technologii informatycznej, zarządzania i bezpieczeństwa.
Znajomość (w stopniu umożliwiającym czytanie i rozumienie tekstów technicznych) jednego z języków w których jest przeprowadzany egzamin np. język angielski, hiszpański, włoski, francuski

Jak długo trwa?
(liczba dni, godzin dydaktycznych)

8 dni (64 godz. dydaktycznych)

Jak przebiegają zajęcia?
(opis metodyki)

Zajęcia mają formę warsztatowo- szkoleniową. Odbywają się one w oparciu o oficjalny program ramowy certyfikatu CISM. Będą prowadzone w języku polskim. Zajęcia będą poświęcone usystematyzowaniu wiedzy (część szkoleniowo-wykładowa) oraz rozpatrywaniu poszczególnym „case study" i przedyskutowaniu w grupie poszczególnych zagadnień. Ponieważ sam egzamin nie odbywa się w języku polskim, celem lepszego przygotowania się do egzaminu, uczestnicy otrzymają podręcznik ISACA „CISM Review Manual 2010 English Edition" wydany w języku angielskim lub ich odpowiedniki w językach francuskim, włoskim lub hiszpańskim. Celem właściwego przygotowania się do certyfikatu uczestnicy będą proszeni o wcześniejsze zapoznanie się z daną partią materiału z w/w podręcznika. Każdy dzień zajęć będzie składał się z 6 godzin wykładów połączonych z dyskusją oraz z 2 godzin zajęć warsztatowych w podgrupach, na zakończenie których omówione będą przykłady pytań związanych z daną partią materiału występujących w testach egzaminacyjnych.

Kto prowadzi?
(imię i nazwisko trenera)

Marek Pióro, CGEIT, CISA, CISM

Jaki jest zakres tematyczny szkolenia?
(program w punktach)

CZĘŚĆ I - Zarządzanie bezpieczeństwem Informacji

- Definicja, cele, zadania,
- Efektywne zarządzanie bezpieczeństwem Informacji
  - Role i odpowiedzialności wyższej kadry kierowniczej,
  - Matryca przychodów i odpowiedzialności,
- Menadżer Bezpieczeństwa Informacji
  - Odpowiedzialność
  - Relacje z wyższą kadra kierowniczą,
- Miary zarządzania Bezpieczeństwem informacji
  - Strategiczne powiązanie,
  - Zarządzanie ryzykiem,
  - Zapewnienie określenia procesów biznesowych,
  - Dostarczanie wartości (dodanej),
  - Zarządzanie zasobami, zarządzanie wydajnością,
- Strategia Bezpieczeństwa Informacji,
- Wyzwania rozwoju strategii bezpieczeństwa informacji,
- Cele strategii bezpieczeństwa Informacji,
- Bieżący stan bezpieczeństwa,
- Rozwój strategii bezpieczeństwa informacji,
- zasoby strategii,
- ograniczenia strategii,
- implementowanie zarządzania bezpieczeństwem informacji

CZĘŚĆ II Zarządzania ryzykiem

- Definicja, cele, zadania,
- Efektywne zarządzanie bezpieczeństwem Informacji
    - Role i odpowiedzialności wyższej kadry kierowniczej,
- Koncepcje zarządzania ryzykami bezpieczeństwa,
- Implementacja zarządzania ryzykiem,
    - Proces zarządzania ryzykiem,
    - Zagrożenia, podatności,
    - Ryzyko, wpływ ryzyka,
    - Mechanizmy kontrolno-zabezpieczające i miary,
    - Klasyfikacja zasobów informacyjnych,
    - Cele czasu odtworzenia,
    - Zewnętrzni dostawcy usług,
    - Integracja w procesy biznesowe,
    - Monitorowanie i komunikowanie,
    - Dokumentowanie,

CZĘŚĆ III Zarządzanie programem bezpieczeństwa informacji

- Definicja, cele, zadania
- Zarządzanie programem bezpieczeństwa informacji
    - Przychody z zarządzanie programem bezpieczeństwa informacji,
    - Kluczowe elementy,
    - zadania
- planowanie
- podstawy bezpieczeństwa,
- procesy biznesowe,
- infrastruktura,
- cykl życia,
- wpływ na użytkownika końcowego,
- rozliczalność,
- miary bezpieczeństwa,
- zarządzanie wewnętrznymi i zewnętrznymi zasobami,

CZĘŚĆ IV Zarządzanie bezpieczeństwem IT

- Definicja, cele, zadania
- Zarządzanie bezpieczeństwem informacji
    - Zaangażowanie kadry kierowniczej,
    - Bezpieczeństwo IT, a bezpieczeństwo informacji,
    - Przychody z zarządzanie bezpieczeństwem informacji,
- Efektywne zarządzanie bezpieczeństwem informacji,
    - Obszar odpowiedzialności
    - Role i odpowiedzialności,
- Koncepcje zarządzania bezpieczeństwem informacji,
- Wdrażanie zarządzania bezpieczeństwem informacji,
    - Zintegrowane czynności zapewnienia,
    - Mechanizmy kontrolno- zabezpieczające,
    - Zasady bezpieczeństwa,

- Standardy bezpieczeństwa,
- Procedury bezpieczeństwa,
- Przypisanie ról i odpowiedzialności,
- Partnerzy biznesowi i bezpieczeństwo dostawców usług,
- Miary bezpieczeństwa i ich monitorowanie,
- Proces zarządzania zmianami,
- Ocena podatności,
- Należyta staranność,
- Rozwiązywanie kwestii niezgodności z zasadami i wymogami,
- Kultura, zwyczaje i świadomość bezpieczeństwa,

CZĘŚĆ V Zarządzanie odpowiedzią na incydent

- Definicja, cele, zadania, wiedza,
- Kluczowe elementy zarządzania odpowiedzią
- Analiza wpływu na biznes – BIA
- Rozwijanie planów odpowiedzi i odtworzenia,
- Proces odpowiedzi na incydent,
- Testowanie planu planów odpowiedzi i odtworzenia,
- Wykonywanie planów odpowiedzi i odtworzenia,
- Dokumentowanie zdarzeń,
- Przeglądy

Materiały, pomoce dydaktyczne, sprzęt

- Dla uczestników:
  - podręcznik w formie wydrukowanej prezentacji, pojedyncze kartki ze scenariuszami ćwiczeń,
  - CISM Review Manual 2010 English Edition - podręcznik w języku angielskim, wydany przez ISACA obejmujący całość materiału merytorycznego egzaminu testowego (cena 115USD),
  - CISM Practice Question Database v9 English Edition – oprogramowanie - baza pytań (w języku angielskim) z poprzednich testów kompetencyjnych pozwalająca na przetestowanie poprawności własnej wiedzy z komentarzami (cena 165USD)
- Używane przez trenera: prezentacja PP wyświetlana podczas zajęć
- Sprzęt: laptop, projektor LCD

Kiedy odbędzie się szkolenie?
(terminy na I i/lub II półrocze)

Do ustalenia z chętnymi środy lub czwartki (maks. 1 spotkanie w tygodniu)

Ceny wszystkich szkoleń są cenami Netto. W skład ceny szkolenia wchodzą materiały przygotowane przez prowadzących, serwis kawowy. Minimalna liczebność grupy 6 osób.
Istnieje możliwość zorganizowania w/w szkoleń zamkniętych dla zakładów pracy lub wybranych grup (np. wyłącznie dla członków Zarządów itp.) w dowolnej lokalizacji na terenie Polski.
Na życzenie uczestników organizatorzy pomogą uczestnikom w zakupie oryginalnych angielsko-językcznych materiałów wydawanych przez ISACA