W związku z obowiązkiem prowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji na podstawie przepisów Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12 kwietnia 2012 roku (Dz. U. nr 0, poz. 526)

zapraszamy do udziału w szkoleniu nt.

„Audyt i ocena bezpieczeństwa informacji w systemach IT".

Cel szkolenia:

1. Charakterystyka najistotniejszych zagadnień związanych z bezpieczeństwem systemów IT;
2. Przygotowanie do przeprowadzenia audytów bezpieczeństwa informacji w systemach IT i oceny bezpieczeństwa systemów IT - zgodnie z minimalnymi wymaganiami dla systemów teleinformatycznych zawartymi w Rozporządzeniu Rady Ministrów w sprawie Krajowych ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12 kwietnia 2012 roku (Dz. U. nr 0, poz. 526) oraz w ustawie o informatyzacji podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 roku (Dz.U. Nr 64, poz. 565, z późn. zm.);
3. Wskazanie i charakterystyka minimalnych wymagań zawartych w obowiązujących przepisach,
4. Nabycie umiejętności praktycznych z zakresu przeprowadzania audytów bezpieczeństwa informacji w systemach IT w jednostkach sektora finansów publicznych.
5. Podniesienie kompetencji zawodowych w zakresie działalności operacyjnej i organizacyjnej w obszarze związanym z zapewnianiem i oceną bezpieczeństwa informacji w systemach IT.

Adresaci szkolenia:

1. Managerowie IT.
2. Administratorzy bezpieczeństwa informacji (ABI).
3. Osoby odpowiedzialne za wdrażanie polityk bezpieczeństwa oraz zabezpieczeń w instytucjach.
4. Pracownicy działów IT.
5. Audytorzy i specjaliści ds. zarządzania systemami IT.
6. Osoby odpowiedzialne w JST za bezpieczeństwo informacji w systemach IT.

Prowadzący szkolenie:

Piotr Błaszczeć – specjalista ds. bezpieczeństwa IT, audytor systemów IT, Lead auditor ISO 27001 CIS, CICA, biegły sądowy z zakresu przestępstw przy użyciu sieci komputerowych, na co dzień główny specjalista bezpieczeństwa IT w jednej z Agencji Rządowych oraz właściciel firmy LOCOS zajmującej się wdrażaniem systemów bezpieczeństwa, szkoleniami, audytem i testami penetracyjnymi. Redaktor naczelny portalu dot. audytu i bezpieczeństwa IT – www.locos.pl.

Forma i program szkolenia:

Szkolenie prowadzone będzie w formie wykładów, warsztatów i konwersatorium. Uczestnikom szkolenia zapewni się laptopy z dostępem do Internetu, z uwagi na praktyczny charakter szkolenia.

Koszt szkolenia:

Istnieje możliwość wyboru dwóch opcji szkolenia:

1. **1080 zł (brutto)**- cena obejmuje uczestnictwo w szkoleniu, materiały szkoleniowe, serwis kawowy.
2. **1250 zł (brutto)**- cena obejmuje uczestnictwo w szkoleniu, materiały szkoleniowe, serwis kawowy oraz obiad w każdym dniu szkolenia.

Miejsce i termin szkolenia:

Szkolenie odbędzie się w Wyższej szkole Biznesu w Gorzowie Wlkp, przy ul. Myśliborskiej 30, 66-400 Gorzów Wlkp.

Termin realizacji szkolenia:
6-8 maja 2013r.

Zgłoszenia uczestnictwa należy dokonywać z wykorzystaniem formularza zgłoszeniowego pod adresem **a.swiercz@wsb.gorzow.pl**, do dnia **22.04.2013r**.
W celu uzyskania dodatkowych informacji oraz wyjaśnienia bieżących informacji dotyczących udziału w szkoleniu oraz przebiegu szkolenia prosimy o kontakt pod nr tel. **95 733 66 68** lub na adres **a.swiercz@wsb.gorzow.pl**.

Program szkolenia
„Audyt i ocena bezpieczeństwa informacji w systemach IT”

Dzień I (9.00-16.00)

Rozpoczęcie

Wprowadzenie do kontroli i audytu systemów teleinformatyczynych. Zasoby instytucji i proces ich kontroli. Rola kontroli w przeciwdziałaniu zagrożeniom IT.

Przerwa kawowa (11.00)

Analiza potencjalnych zagrożeń dotyczących systemów informacyjnych i teleinformatycznych.

Przerwa kawowa /obiadowa (13.30)

Zarządzanie ryzykiem jako sposób strategicznego podejścia do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych.

Dzień II (9.00-17.00)

Rozpoczęcie

Wsparcie dla audytu IT: normy i najlepsze praktyki z zakresu bezpieczeństwa IT. Powiązane przepisy prawne.

Przerwa kawowa (11.00)

Problemy outsourcingu. Prowadzenie kontroli z zakresu współpracy z firmami zewnętrznymi.

Przerwa kawowa /obiadowa (13.30)

Audyt legalności jako składowa audytu IT.

Dzień III (9.00-15.00)

Rozpoczęcie

Audyt bezpieczeństwa informacji krok po kroku. Utworzenie checklisty audytowej w zakresie:

- Analizy bezpieczeństwa fizycznego oraz infrastruktury sieciowej
- Analizy organizacji wewnętrznej
- Analizy dokumentacji związanej z bezpieczeństwem teleinformatycznym
- Kontrola procesu przetwarzania danych, rozwoju i utrzymania danych
- Analizy bezpieczeństwa sieci, systemów, aplikacji oraz baz danych
- Proces kontroli dostępu do zasobów
- Zapewnianie ciągłości działania

Przerwa kawowa (11.00)

Narzędzia pracy audytora.

Przerwa kawowa /obiadowa (13.30)

Podsumowanie i zakończenie