Sudhara International
+48 32 724 35 86
info@sudharapolska.com
www.sudharapolska.com

ANALIZA RYZYK W SYSTEMIE ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI NA ZGODNOŚĆ Z WYMAGANIEM NORMY ISO 27001

PROGRAM SZKOLENIA

🎯 **Cel szkolenia**

Celem szkolenia jest przygotowanie uczestników do samodzielnego i świadomego prowadzenia procesu analizy ryzyka w Systemie Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami ISO/IEC 27001, z uwzględnieniem wytycznych ISO/IEC 27005 oraz dobrych praktyk zarządzania ryzykiem.
Szkolenie rozwija kompetencje w zakresie identyfikacji aktywów, zagrożeń i podatności, oceny prawdopodobieństwa oraz skutków incydentów, budowy kryteriów oceny ryzyka, a także podejmowania decyzji dotyczących postępowania z ryzykiem. Uczestnicy poznają również sposób powiązania wyników analizy ryzyka z doborem zabezpieczeń, dokumentacją SZBI oraz wymaganiami prawnymi i organizacyjnymi.

- Zapoznanie z normą ISO/IEC 27001 jako fundamentem budowy systemu zarządzania bezpieczeństwem informacji (ISMS) i poznanie roli ISO/IEC 27005 w procesie identyfikacji, analizy, oceny i postępowania z ryzykami.
- Zdobycie umiejętności praktycznych w tworzeniu katalogu aktywów, analizie zagrożeń i podatności, budowie macierzy ryzyka oraz określaniu akceptowalnego poziomu ryzyka.
- Poznanie strategii postępowania z ryzykiem (redukcja, akceptacja, przeniesienie, unikanie) oraz wyboru zabezpieczeń z Załącznika A ISO/IEC 27001.
- Zapoznanie z normą ISO 31000 (ogólne zarządzanie ryzykiem) i IEC 31010 (techniki oceny ryzyka), a także z integracją z innymi przepisami (NIS 2, RODO, ISO 22301).

Program szkolenia

PRE – TEST

1. **Wprowadzenie do ISO/IEC 27001 i ISO/IEC 27005:**
   - Przegląd struktury ISMS (cykl PDCA), rola kontekstu organizacji, pojęcia aktywa, zagrożenia, podatność, ryzyko.
   - Różnice między normami ISO/IEC 27005 i ISO 31000 oraz ich wzajemne uzupełnianie.
2. **Identyfikacja i klasyfikacja aktywów**:
   - Tworzenie rejestru aktywów (informacyjnych, technologicznych, osobowych), określanie ich wartości i krytyczności.
   - Wykorzystanie technik oceny z IEC 31010, np. strukturalna analiza zagrożeń, scenariusze.
   - ***Ćwiczenie*: przygotowanie katalogu aktywów i identyfikacja zagrożeń.**
3. **Analiza i ocena ryzyka:**
   - Określanie kryteriów oceny (prawdopodobieństwo, skutek), budowa macierzy ryzyka, priorytetyzacja.

- Analiza wpływu i zależności; ustalenie apetytu na ryzyko i progów akceptacji.
- ***Ćwiczenie*: wypełnienie macierzy ryzyka i interpretacja wyników.**

4. **Postępowanie z ryzykiem:**
   - Dobór strategii (redukcja, akceptacja, przeniesienie, unikanie), wybór zabezpieczeń (kontrole z Załącznika A ISO/IEC 27001: zarządzanie tożsamościami, szyfrowanie, segmentacja sieci, kopie zapasowe, monitorowanie bezpieczeństwa), opracowanie planu postępowania z ryzykiem, dokument „Statement of Applicability".
   - ***Ćwiczenie*: opracowanie planu postępowania dla wybranych ryzyk.**
5. **Monitorowanie, przegląd i ciągłe doskonalenie:**
   - Wskaźniki KPI, audity wewnętrzne, przeglądy zarządzania; przetwarzanie informacji o incydentach i aktualizacja rejestru ryzyk.
   - Integracja z NIS 2, ISO 22301 i RODO.
6. **Integracja z przepisami:**
   - Omówienie, jak wyniki analizy ryzyka łączą się z obowiązkami prawnymi (NIS 2, ustawa o ochronie danych, prawa branżowe) oraz jak wdrożyć spójną dokumentację.

POST - TEST

👥 Grupa odbiorcza

Szkolenie jest skierowane do:

- pełnomocników i koordynatorów ds. ISO 27001 oraz SZBI,
- menedżerów bezpieczeństwa informacji, compliance i ryzyka,
- auditorów wewnętrznych systemów zarządzania,
- specjalistów IT, cyberbezpieczeństwa i administratorów systemów,
- osób odpowiedzialnych za ochronę danych osobowych i zgodność regulacyjną,
- kierowników procesów i właścicieli aktywów informacyjnych,
- członków zespołów wdrażających lub doskonalących system zarządzania bezpieczeństwem informacji,
- kadry menedżerskiej odpowiedzialnej za podejmowanie decyzji dotyczących akceptacji ryzyka i nadzoru nad bezpieczeństwem organizacji.

Szkolenie będzie szczególnie wartościowe dla organizacji przygotowujących się do wdrożenia ISO/IEC 27001, certyfikacji, auditu klienta lub uporządkowania procesu analizy ryzyka w związku z wymaganiami NIS2, RODO oraz wewnętrznym ładem organizacyjnym.

✅ Korzyści po szkoleniu

Po szkoleniu uczestnicy:

- Rozumieją wymagania ISO/IEC 27001 dotyczące podejścia opartego na ryzyku oraz rolę ISO/IEC 27005 w praktycznym prowadzeniu analizy ryzyka.
- Potrafią zbudować i uporządkować rejestr aktywów oraz przypisać im właścicieli, wartość i krytyczność.
- Umieją identyfikować zagrożenia, podatności i potencjalne scenariusze naruszenia bezpieczeństwa informacji.
- Potrafią opracować kryteria oceny ryzyka oraz stosować macierz ryzyka w sposób spójny i powtarzalny.
- Potrafią określić poziomy akceptacji ryzyka oraz wspierać kierownictwo w podejmowaniu decyzji.
- Umieją dobrać właściwe sposoby postępowania z ryzykiem i powiązać je z zabezpieczeniami organizacyjnymi, technicznymi i proceduralnymi.
- Rozumieją, jak przygotować dokumentację wspierającą SZBI, w tym plan postępowania z ryzykiem oraz Statement of Applicability.
- Wiedzą, jak monitorować ryzyka, aktualizować ocenę oraz wykorzystywać wyniki w audytach, przeglądach zarządzania i działaniach doskonalących.

- Potrafią powiązać analizę ryzyka z wymaganiami prawnymi i biznesowymi organizacji.

Dodatkową korzyścią dla organizacji jest zwiększenie dojrzałości procesu zarządzania bezpieczeństwem informacji, lepsza przejrzystość decyzji dotyczących ryzyka oraz większa gotowość do audytów i wymagań klientów.

🛠️ Metodyka szkolenia

Szkolenie prowadzone jest w formule warsztatowo-praktycznej, ukierunkowanej na realne zastosowanie wymagań normy w środowisku organizacyjnym uczestników.
Metodyka obejmuje:

- krótkie, uporządkowane wprowadzenia teoretyczne do wymagań norm i dobrych praktyk,
- omówienie pojęć i zależności na przykładach z funkcjonowania organizacji,
- pracę na przykładach dotyczących aktywów, zagrożeń, podatności i scenariuszy ryzyka,
- ćwiczenia praktyczne związane z budową rejestru aktywów, macierzy ryzyka oraz planów postępowania,
- analizę przypadków i dyskusję nad typowymi błędami popełnianymi przy szacowaniu ryzyka,
- konsultowanie podejścia możliwego do zastosowania w organizacji uczestników,
- pytania kontrolne, wymianę doświadczeń i wspólne wypracowanie dobrych praktyk.
- Pre i post testy weryfikujące wiedzę.

Szkolenie nastawione jest na zrozumienie logiki podejścia do ryzyka, a nie wyłącznie na interpretację zapisów normy. Dzięki temu uczestnicy zdobywają nie tylko wiedzę formalną, ale również praktyczne umiejętności wdrożeniowe i decyzyjne.

Czas trwania szkolenia: 2 dni