Szkolenie

System Zarządzania Bezpieczeństwem Informacji wg normy ISO 27001:2022 – wymagania, wdrażanie i utrzymanie

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Szkolenie przedstawia pełny zakres wymagań normy ISO/IEC 27001:2022, obejmujący zasady projektowania, wdrażania, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Uczestnicy poznają definicje kluczowych pojęć, strukturę normy, wymagania dokumentacyjne oraz szczegółowe omówienie kontroli Załącznika A wraz z praktycznymi przykładami ich wdrożenia. Program szkolenia kończy moduł dotyczący audytowania SZBI zgodnie z ISO 19011, obejmujący techniki zbierania dowodów, raportowanie i działania poaudytowe.

Korzyści

Uczestnik po ukończeniu szkolenia:

- zrozumie wszystkie wymagania normy ISO/IEC 27001:2022 wraz z interpretacją i przykładami,
- pozna ponad 90 zabezpieczeń Załącznika A podzielonych na kontrole organizacyjne, ludzkie, fizyczne i technologiczne,
- zrozumie praktyczne sposoby analizy ryzyka, planowania działań i prowadzenia pełnego cyklu PDCA,
- będzie potrafił opracować kluczowe dokumenty SZBI: polityki, SoA, rejestry, procedury, plany reagowania,
- pozna wymagania związane z bezpieczeństwem usług chmurowych, dostawców, projektów, kryptografii, sieci i aplikacji,
- zrozumie, jak przygotować organizację do audytu, jakie dowody są wymagane i jak przebiega

audit SZBI zgodnie z ISO 19011,
- otrzyma pełną mapę wymagań dokumentacyjnych SZBI wynikających z ISO/IEC 27001:2022.

Wymagania

- podstawowa wiedza z zakresu cyberbezpieczeństwa lub procesów IT,
- brak konieczności wcześniejszego doświadczenia w pracy z normami ISO.

Harmonogram szkolenia

1. Wprowadzenie do ISO/IEC 27001

- Korzyści ze wdrożenia SZBI
- Zarządzanie ryzykiem
- Budowanie zaufania i odporności organizacji

2. Słownik kluczowych pojęć bezpieczeństwa informacji

- Aktywa, kontrola, poufność, integralność, dostępność
- Incydent i zdarzenie bezpieczeństwa
- Ryzyko, ocena ryzyka
- Tożsamość, uwierzytelnianie, uprawnienia
- Poufne / wrażliwe informacje
- Zarządzanie incydentami, PII, luka, zagrożenie
- Segregacja obowiązków, zarządzanie aktywami
- Klasyfikacja informacji, etykietowanie
- Kontrola dostępu
- Ochrona przed malware, praca zdalna, bezpieczeństwo fizyczne
- Bezpieczeństwo w łańcuchu dostaw ICT
- Kryptografia, chmura, monitorowanie, testy

3. Znaczenie i korzyści wdrożenia SZBI

- Ochrona aktywów
- Zgodność prawna i kontraktowa
- Budowanie reputacji i przewagi konkurencyjnej
- Minimalizacja ryzyk i kosztów
- Wsparcie ciągłości działania

4. Rodzina norm ISO/IEC 27000

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

- ISO 27000 – słownik
- ISO 27001 – wymagania certyfikacyjne
- ISO 27002 – wdrażanie zabezpieczeń
- ISO 27003 / 27004 / 27005 – wskazówki dot. wdrożeń, pomiaru, ryzyka
- Normy sektorowe (27017, 27018, 27701 itd.)

5. Struktura normy ISO/IEC 27001:2022

- Zakres
- Odniesienia normatywne
- Terminy i definicje
- Kontekst organizacji
- Przywództwo
- Planowanie
- Wsparcie
- Operacje
- Ocena efektów działania
- Doskonalenie

6. Cykl PDCA

- Plan → Do → Check → Act
- Rola w ciągłym doskonaleniu SZBI

7. Szczegółowe omówienie Załącznika A (kontrole A.5–A.8)

- A.5 – organizacyjne (polityki, role, segregacja obowiązków, kontakt z władzami, dostawcy, projekty)
- A.6 – ludzie (rekrutacja, szkolenia, dyscyplina, obowiązki po ustaniu zatrudnienia)
- A.7 – fizyczne (strefy, kontrola wejść, monitoring, ochrona przed zagrożeniami)
- A.8 – technologiczne (IAM, kryptografia, malware, DLP, backup, redundancja, monitoring, sieci, SDLC itd.)

8. Wymagania dokumentacyjne ISO/IEC 27001:2022

- Polityka bezpieczeństwa informacji
- Cele bezpieczeństwa
- Zakres SZBI
- Kryteria oceny ryzyka
- Proces postępowania z ryzykiem
- SoA – oświadczenie o stosowaniu
- Plany postępowania z ryzykiem
- Rejestry, dowody, zapisy audytów i przeglądów

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

9. Utrzymanie SZBI

- Ciągłe doskonalenie
- Reakcja na niezgodności
- Analiza przyczyn
- Przeglądy zarządzania

10. Audytowanie SZBI zgodnie z ISO 19011

- Definicja audytu
- Planowanie audytu
- Przegląd dokumentacji
- Zbieranie dowodów (wywiady, obserwacje, inspekcje, testy)
- Obserwacje audytowe
- Raportowanie
- Działania poaudytowe

Tagi:

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.