4ITSECURITY

WDROŻENIE I CERTYFIKACJA ISO

WWW.4ITSECURITY.PL

WDROŻENIE I CERTYFIKACJA PN-ISO/IEC 27001:2014

Organizacja, która chce należycie zabezpieczyć swoje informacje powinna zastosować podejście systemowe, w ramach którego będzie zarządzać kompleksowo posiadanymi **aktywami informacyjnymi, infrastrukturą** przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji.

Dla organizacji, która chce świadomie chronić swoje aktywa na uwagę zasługuję System Zarządzania Bezpieczeństwem Informacji wg normy **PN-ISO/IEC 27001:2014.** Norma ta jest zbiorem wytycznych pozwalających na wdrożenie efektywnego Systemu Zarządzania Bezpieczeństwem Informacji w organizacji. Norma jest przeznaczona dla wszystkich rodzajów organizacji, zarówno dla podmiotów biznesowych jak i podmiotów administracji publicznej.

ZASTOSOWANIE W BRANŻACH:

Sektor publiczny | Ochrona Zdrowia | Infrastruktura krytyczna | Bankowość | Ubezpieczenia | Przemysł

Mamy przyjemność zaproponować Państwu naszą pomoc w zakresie przygotowania projektu, wdrożenia i doskonalenia **Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-ISO/IEC 27001:2014**

Duże doświadczenie naszych konsultantów gwarantuje skuteczne wdrożenie systemu zarządzania zgodnego z normą ISO. Kierując się naszym wieloletnim doświadczeniem proponujemy najkorzystniejszy, ramowy program wdrożenia systemu zarządzania, który za każdym razem dostosowujemy do potrzeb organizacji klienta.

Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji jest dużym przedsięwzięciem. Aby nim skutecznie zarządzać podzieliliśmy go na etapy, stanowiące jednocześnie punkty milowe projektu. Każdy z etapów jest zbiorem zadań prowadzących do uzyskania produktu w szacowanym czasie realizacji.

CZY JESTEŚ PEWIEN,
ŻE TWOJE DANE SĄ **BEZPIECZNE?**

ETAPY

ETAP 1 – AUDYT ISMS

Konsultanci przeprowadzają rozmowy z Kierownictwem i pracownikami, zapoznają się ze strukturą organizacyjną, dokumentacją stosowaną w organizacji, dokonują przeglądu dokumentów dotyczących systemu zarządzania w celu określenia w jakim stopniu organizacja jest zgodna z wymaganiami normy ISO a jakie elementy będą wymagały dostosowania do wymagań normy ISO. Informacje zebrane podczas audytu posłużą do opracowania szczegółowego zakresu prac i harmonogramu.

ETAP 2 – SZKOLENIA KIEROWNICTWA ORGANIZACJI

Zaangażowanie Kierownictwa jest podstawą dla prawidłowego funkcjonowania każdego systemu zarządzania. Podczas szkolenia zostają przedstawione zagregowane wyniki diagnozy z uwzględnieniem mocnych i słabych punktów ocenianych obszarów oraz zaprezentowane wymagania normy odnoszące się do najwyższego kierownictwa.

SZKOLENIE PEŁNOMOCNIKA SYSTEMU ZARZĄDZANIA I ZESPOŁU WDROŻENIOWEGO

Podczas którego omówione zostaną obowiązujące uregulowania wewnętrzne w zakresie systemu zarządzania bezpieczeństwem informacji.

SZKOLENIE PRACOWNIKÓW

Podczas którego omówione zostaną najważniejsze informacje dot. wdrażanej normy PN ISO/IEC 27001. Każdy z uczestników otrzyma materiał informacyjny.

ETAP 3 – SZKOLENIE Z METODYKI ANALIZY RYZYKA

Uczestnicy szkolenia zostaną zapoznani z zasadami zarządzania ryzykiem, z metodyką analizy ryzyka. Trener zapewni formularze oraz metodykę szacowania ryzyka, które ułatwią i przyspieszą proces tworzenia analizy.

ETAP 4 – KONSULTACJE PRZY OPRACOWANIU ANALIZY RYZYKA

Analiza ryzyka jest punktem wyjścia do projektowania systemu w organizacji. Na jej podstawie wdrażane są warianty postępowania z ryzykiem oraz opracowywane plany postępowania z ryzykiem. Konsultanci wraz z przedstawicielami organizacji przeprowadzą identyfikację źródeł ryzyka, wspólnie określą prawdopodobieństwo wystąpienia źródeł ryzyka i ich wpływ na funkcjonowanie organizacji.

ETAP 5 – KONSULTACJE PRZY OPRACOWANIU PLANU CIĄGŁOŚCI DZIAŁANIA

Na podstawie Planu postępowania z ryzykiem opracowany zostanie w drodze konsultacji Plan Ciągłości Działania, powołujący się na scenariusze postępowania w sytuacjach kryzysowych. Scenariusze sytuacyjne odwoływać się będą do procedur odtwarzania po awarii (DRP).

Wdrożenie planu ciągłości działania umożliwia kontynuacje kluczowych procesów biznesowych wykorzystujących elektroniczne przetwarzanie danych w sytuacji, gdy część infrastruktury informatycznej jest niedostępna – np. wskutek katastrofy. Plan ciągłości działania uruchamiany jest w sytuacji kryzysowej – gdy skutki zaistniałych incydentów zagrażają funkcjonowaniu organizacji.

ETAP 6 – KONSULTACJE PRZY TWORZENIU DOKUMENTACJI

Konsultanci przy wsparciu ze strony członków grupy wdrożeniowej dokonują uzupełniania dokumentacji systemowej o nowe elementy wymagane w systemie zarządzania. Wraz z oddelegowanymi do budowania systemu pracownikami organizacji zostanie sformułowana polityka systemu zarządzania. Dokumentację przygotowują pracownicy organizacji lub na życzenie klienta konsultanci, uzgadniając ją z osobami odpowiedzialnymi za poszczególne obszary.

ETAP 7 – SZKOLENIE AUDYTORÓW WEWNĘTRZNYCH

Po opracowaniu dokumentacji należy sprawdzić poprawność i stan wdrożenia opisanych w dokumentacji rozwiązań. Zadania te realizowane są przez przeszkolonych pracowników organizacji – audytorów wewnętrznych. Celem szkolenia jest przygotowanie audytorów do praktycznego przeprowadzenia audytów, stąd też zawiera ono szereg ćwiczeń i scenek audytowych. Audytorzy wewnętrzni zapoznawani są z widzą z w zakresie podejścia procesowego przy ocenie systemu zarządzania. Po ukończeniu szkolenia audytorzy otrzymują certyfikaty. Etap ten nie musi być realizowany, jeżeli klient nie dysponuje osobami mogącymi pełnić funkcję audytora wewnętrznego lub zakłada, że organizacja samodzielnie nie będzie przeprowadzała audytów wewnętrznych. Wówczas rolę audytora wewnętrznego przejmuje konsultant pomagający przy wdrożeniu systemu zarządzania, który zgodnie z planem audytów wewnętrznych przeprowadza audyty w fazie wdrożenia jak również i później, podczas utrzymywania systemu.

ETAP 8 – WDROŻENIE SYSTEMU ZARZĄDZANIA

Etap wdrożenia systemu zarządzania polega na przekazaniu wszystkim pracownikom opracowanej dokumentacji, polityki oraz zapewnieniu świadomości dotyczącej ich roli w funkcjonującym systemie. Forma przekazywania informacji dostosowywana jest do zasad panujących w organizacji (spotkania, szkolenia wewnętrzne, broszury, intranet). Wdrożenie systemu zarządzania jest to również etap dokonania oceny funkcjonowania systemu i sprawdzenia gotowości do certyfikacji, poprzez przeprowadzenie audytów wewnętrznych, wdrożenie działań korygujących i postępowania z ryzykiem.

ETAP 9 – ZGŁOSZENIE GOTOWOŚCI DO CERTYFIKACJI – PRZEGLĄD ZARZĄDZANIA

Ostatnim etapem wdrożenia jest przeprowadzenie Przeglądu zarządzania. Jest to spotkanie Pełnomocnika ds. systemu i kierownictwa pod przewodnictwem osoby zarządzającej organizacją. W spotkaniu przeważnie uczestniczy konsultant pomagając w sprawnym i zgodnym z wymaganiami normy jego przeprowadzeniu. Po zakończeniu konsultant pomaga w przygotowaniu Raportu z przeglądu zarządzania.

ETAP 10 – CERTYFIKACJA

Etap ten realizowany jest przez wybraną jednostkę certyfikującą. Pomagamy w wyborze firmy certyfikującej. Podczas audytu certyfikującego nie pozostawiamy Klientów bez opieki.

ETAP 11 – SERWISOWANIE SYSTEMU ZARZĄDZANIA

Po otrzymaniu certyfikatu nie zostawiamy naszych klientów samych. Na życzenie pomagamy w utrzymaniu systemu zarządzania: dokonujemy przeglądu analizy ryzyka, szkolimy, audytujemy, przeprowadzamy przegląd systemu przed audytami nadzoru.

Doświadczeni konsultanci i trenerzy czuwają nad prawidłowym przebiegiem wdrożenia. Posiadają kompetencje audytorów wewnętrznych i wiodących, współpracują z jednostkami certyfikującymi jako audytorzy i trenerzy. Współpraca z naszymi konsultantami zawsze kończy się sukcesem.

Dodatkowo na naszą korzyść przemawia:

- Znajomość specyfiki Klientów z różnych obszarów działalności gospodarczej
- Poparte referencjami doświadczenie w tworzeniu i wdrażaniu rozwiązań związanych z bezpieczeństwem systemów informatycznych dla instytucji z sektorów publicznego, infrastruktury krytycznej, medycznego, bankowego, finansowego i przemysłowego
- Doświadczenie w szeroko rozumianych pracach nad bezpieczeństwem u wielu Klientów, w zróżnicowanych i złożonych systemach
- Najlepsze standardy, sprawdzone rozwiązania i spójna metodologia pracy
- Przeszkolony zespół specjalistów na najwyższym poziomie
- Prestiżowe certyfikaty zawodowe z zakresu bezpieczeństwa informacji
- Bezpośrednia współpraca z ComCERT - niezależną firmą specjalizującą się w usługach typu CERT (Computer Emergency Response Team), tj. dostarczającą rozwiązania z dziedziny bezpieczeństwa sieci przedsiębiorstw i instytucji w zakresie ich obrony w sytuacji zagrożeń z publicznych sieci teleinformatycznych
- Dostęp do informacji o pojawiających się zagrożeniach
- Metodyka zgodna z przepisami polskiego prawa oraz obowiązującymi normami
- Zdolność do obsługi Klientów w rozumieniu Ustawy o Ochronie Informacji Niejawnej

O FIRMIE

Zachęcamy do nawiązania kontaktu z naszymi konsultantami, którzy udzielą dodatkowych informacji, poznają oczekiwania oraz przygotują ofertę spełniającą Państwa potrzeby i wymagania.

4 IT SECURITY jest polską firmą doradczą świadczącą usługi w zakresie bezpieczeństwa teleinformatycznego i ochrony danych w oparciu o zasoby i wsparcie technologiczne ComCERT SA. Jesteśmy zespołem profesjonalistów, którzy z pasją dostarczają najwyższej jakości usługi bezpieczeństwa teleinformatycznego wspierające realizację celów biznesowych Klientów. Oferowane przez nas usługi i realizowane projekty cechują się wysoką jakością wykonania, innowacyjnością technologiczną oraz szczególną troską o wysokie bezpieczeństwo danych.

Szerokie doświadczenie naszych ekspertów bezpieczeństwa informacji potwierdzone jest między innymi certyfikatami:

- CISSP, CISM, CISA, CRISC, OSCP, CEH
- Audytor wiodący systemu: ISO 27001, ISO 22301
- Audytor wiodący ISO 9001
- Audytor Systemu Zarządzania Usługami IT ISO 20000
- ITIL Foundation, ITIL Intermediate in Continual Service Improvement, ITIL Expert
- Togaf 8 Certified
- PRINCE2

Nasi konsultanci posiadają certyfikaty producentów rozwiązań sprzętowych czy programowych. Posiadamy także poświadczenia bezpieczeństwa w zakresie dostępu do informacji niejawnych oznaczonych klauzulą „POUFNE" a także „TAJNE".

4 IT SECURITY, Technopark Pomerania, ul. Cyfrowa 2, 71-441 Szczecin

www.4itsecurity.pl biuro@4itsecurity.pl (+48) 607 60 38 90 NIP: 6691408645