ISO/IEC 27001

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

KAŻDA ORGANIZACJA GROMADZI I PRZETWARZA INFORMACJE, KTÓRE STANOWIĄ TAEMINICĘ SŁUŻBOWĄ I HANDLOWĄ. DLATEGO NA PLACÓWKACH TYCH CIĄŻY ODPOWIEDZIALNOŚĆ ABY DANE TE BYŁY BEZPIECZNE, DOBRZE CHRONIONE I DOSTĘPNE WTEDY GDY JEST TAKA POTRZEBA. ABY WSPOMÓC ORGANIZACJE W BUDOWIE ZDROWEGO PODEJŚCIA DO ZAPEWNIENIA SPEŁNIENIA TEGO WYMAGANIA CORAZ WIĘCEJ ORGANIZACJI DECYDUJE SIĘ NA WDROŻENIE I CERTYFIKACJĘ TEGO SYSTEMU.

WPROWADZENIE

Istnieją różne formy przechowywania informacji. W każdej organizacji mają one formę cyfrową, papierową, lub stanowią wiedzę pracowników. Historia kontraktu i dokumenty związane - raporty, protokoły, wyniki, wypisy, etc. mają status co najmniej tajemnicy służbowej, tak więc powinny być dostępne tylko dla osób upoważnionych. Dlatego dostęp do nich musi być z jednej strony szybki dla osób upoważnionych i niemożliwy dla osób postronnych.

Systemy informacyjne i ich informatyzacja w organizacjach pozwala należycie zadbać o bezpieczeństwo gromadzonych danych. System zarządzania oparty o standard ISO 27001 - kompatybilny z rodziną norm ISO, jest obecnie najpopularniejszym standardem w odniesieniu dla tego typu kontekstu.
Dzięki wdrożeniu systemu zarządzania bezpieczeństwem danych zgodnego z normą ISO/ IEC 27001 organizacja deklaruje, że identyfikuje i obniża ryzyka związane z przechowywaniem poufnych i istotnych danych. Proces certyfikacji daje pewność wszystkim interesariuszom: klientom, zarządzającym i innym stronom, że z należytą dbałością organizacja podchodzi do bezpieczeństwa informacji.

KORZYŚCI DLA BIZNESU

Zawsze ilekroć mamy zaangażowaną stronę trzecią to wiadomo, że certyfikowany system zarządzania bezpieczeństwem informacji będzie strażnikiem i gwarantem zaangażowania organizacji w ochronę informacji, i daje pewność, że wszystkie dane są właściwie chronione - niezależnie od tego czy są przechowywane na papierze, czy też w formie cyfrowej. A świadomość pracowników w tym temacie pozwala zachować także należytą dbałość o te dane, które pozostają wiedzą specjalistów.

Ten efekt otrzymuje się poprzez metody i narzędzia systematycznego podejścia do zminimalizowania zagrożeń i zapewnienia zgodności z wymogami m.in. prawnymi.

A przybliżając ten temat, w kontekście wsparcia – pomaga w:

- Zarządzaniu informacjami będącymi w posiadaniu organizacji
- Aktywnym podejściu do zarządzania danymi i ochrony ważnych informacji poprzez identyfikowanie i zmniejszanie zagrożeń związanych z ich posiadaniem.
- Pozostawaniu w zgodności z ważnymi przepisami krajowymi i międzynarodowymi.
- Zapewnieniu ciągłości działania w przypadku incydentów związanych z ochroną danych.
- Przekonaniu i zapewnieniu wszystkich interesariuszy, że informacje poufne są bezpieczne.

ŚCIEŻKA DO CERTYFIKACJI

Jest kilka podejść do wdrożenia systemu zarządzania. W czasach tak dużego obciążenia pracowników obowiązkami zawodowymi i pracą multidyscyplinarną, obciążanie ich dodatkowym projektem bez wsparcia ze strony kierownictwa może okazać się mało efektywne.

Dlatego jako praktycy zalecamy aby organizacja prowadziła projekt wdrożenia w ujęciu hybrydowym, tj. praca własna + konsultacje z dobrymi praktykami branżowymi w systemach zarządzania, które można zakończyć audytem przedcertyfikacyjnym dla sprawdzenia gotowości organizacji do certyfikacji.

Najważniejszym jednak gwarantem sukcesu wdrożenia dowolnego systemu jest zaangażowanie najwyższego kierownictwa, tak by każdy pracownik organizacji był świadom determinacji organizacji aby osiągnąć ten sukces. Zwieńczenie procesu wdrożenia systemu zarządzania stanowi jego certyfikacja, prowadzona przez akredytowaną jednostkę certyfikacyjną jak QSCert.

PRZEBIEG AUDYTU

Usługa certyfikacji - zarówno audyt certyfikacyjny, jak i okresowe, jest zestandaryzowana. I tak naprawdę kompetencje audytorów decydują o jakości audytu, o wartości dodanej. Audyt certyfikacyjny składa się z dwóch etapów.

Pierwszy etap to przegląd dokumentacji podczas wizyty wstępnej, na której dokonuje się formalnej oceny przygotowania organizacji do audytu certyfikacyjnego. Weryfikuje się wyniki audytów wewnętrznych, przeglądu zarządzania, jakość dokumentacji - szczególnie tej obligatoryjnej, itp. Jeżeli organizacja jest do tego przygotowana można odnieść się do analizy ryzyk w odniesieniu do aktywów informacyjnych. Pozwoli to wypracować realną wartość dodaną do audytu.

Kolejny etap to audyt certyfikacyjny, który ocenia zrozumienie i skuteczność systemu, w wyniku którego organizacja otrzymuje rekomendację do wydania certyfikatu. W ciągu 3 lat współpracy certyfikacyjnej organizacja corocznie poddaje się audytom nadzoru.

PARTNERSTWO Z QSCERT

Jeżli za definicję partnerstwa przyjmiemy sformułowania: współpraca, wzajemność, zaufanie, pomoc, to QSCert jest jednostką, która ma to zapisane nie tylko w swoich wartościach, ale i tak działa. Dlatego też w ciągu 14 lat wydała ponad 8600 certyfikatów, działając w ponad 20 krajach świata, na 4 kontynentach. Młodość i sprawność w działaniu, pasja tworzenia i elastyczność jest dodatkowym atutem, co pozwala dopasować usługi certyfikacyjne do potrzeb klienta, zawsze poszanowaniu zasad akredytacyjnych.

Dobór kadry audytorskiej odbywa się w oparciu o uznane kompetencje, doświadczenie i doskonałą komunikację, tak by klient czuł się partnerem i podmiotem certyfikacji, i nie miał poczucia kontroli. Aduytorzy są czynnymi na rynku ekspertami, menedżerami, specjalistami w różnych organizacjach.

Polskie przedstawicielstwo QSCert, tworzą osoby aktywnie działający na rynku usług certyfikacyjnych od ponad 17 lat, będący jednocześnie członkami branżowych stowarzyszeń.

Zapraszamy do współpracy.

CoE
CENTRE of EXCELLENCE

QSCert-Poland (Centrum Certyfikacji w strukturze Centre of Excellence Sp. z o.o.),
Śląski Park Technologiczno-Przemysłowy, ul.Szyb Walenty 26a, 41-700 Ruda Śląska, Tel/Fax. +48 32 789-50-70, GSM: +48 601 448883, +48 664 413 776, e-mail: office@coe.biz.pl , Poland@qscert.pl ,
WEB: www.qscert.pl , www.coe.biz.pl KRS: 0000541672, NIP: 6412532186