PECB

CTS Customized Training Solutions

Biała Księga

Systemy Zarządzania Bezpieczeństwem Informacji

ISO 27001

TECHNOLOGIA INFORMACYJNA– TECHNIKI BEZPIECZEŃSTWA

BEZPIECZEŃSTWO INFORMACJI – SYSTEMY ZARZĄDZANIA - WYMAGANIA

szkolenia@cts.com.pl tel +48 22 208 28 61 www.cts.com.pl

SZANOWNI PAŃSTWO!

CTS Customized Training Solutions od 1989 roku prowadzi wysokospecjalistyczne szkolenia dla osób w branży IT. W CTS uczymy nie tylko technicznych umiejętności przydatnych w pracy programisty, administratora czy specjalisty IT, lecz także rozwijamy umiejętności analizowania, kreatywności, samodzielności i zaangażowania, które wzmacniają potencjał pracowników.

Dziś branża IT to wyzwanie – strategie i cele biznesowe organizacji opierają się na sprawnie funkcjonujących infrastrukturach IT i zespołach ludzi pracujących z nimi (specjaliści IT) i na nich (użytkownicy końcowi).

Wybór CTS na dostawcę rozwiązań szkoleniowych daje gwarancję otrzymania specjalistycznej wiedzy na najwyższym poziomie. Oferujemy:

- szkolenia autoryzowane (akredytowane), autorskie i certyfikowane, w tym m.in:
    - techniczne – Microsoft, IBM, Apple, VMware, Oracle, CompTIA, Docker, Jira, Linux/Unix, ElasticSearch, McAfee, UMTS/GSM
    - z bezpieczeństwa fizycznego oraz z norm i dobrych praktyk – zarządzania ciągłością działania, procesami odtwarzania po awarii, zarządzania ryzykiem (CISSP, ISACA)
    - z umiejętności analitycznych (IREB), testowych (ISTQB), metodyk zwinnych (Agile/Scrum), zarządzania projektami (Prince2, AgilePM), zarządzania korzyściami
- doświadczoną kadrę trenerską, szkolącą po polsku i angielsku
- elastyczne terminy i konkurencyjne ceny

Posiadamy także autoryzowane centra egzaminacyjne Pearson Vue, Certiport, Nextec, CastleWorld oraz PSI (egzaminy ISACA).

Prezes Zarządu
Rafał Maletko

CTS Customized Training Solutions
www.cts.com.pl
szkolenia@cts.com.pl
tel +48 22 208 28 61

Szkolenia z zarządzania – normy ISO

CTS prowadzi szkolenia akredytowane na mocy umowy certyfikacyjnej zawartej z Professional Evaluation And Certification Board (PECB), zgodnie ze standardami instytucji regulującej wdrażanie norm ISO - The American National Standards Institute (ANSI).

W akredytowanych instytucjach proces weryfikacji wiedzy zdobytej przez uczestników podczas szkolenia, jest dogłębniejszy i bardziej szczegółowy. Oznacza to, iż certyfikat zdobyty po pozytywnie zdanym egzaminie jest wartościowszy.

Egzamin, najczęściej w formie pisanego eseju, sprawdzany jest przez niezależnych egzaminatorów z PECB. Natomiast w instytucjach szkoleniowych nieposiadających akredytacji egzamin sprawdza zwykle trener, który prowadził szkolenie.

Dodatkowo po zdanym egzaminie, PECB weryfikuje doświadczenie zawodowe uczestnika szkolenia na potrzeby uzyskania danej certyfikacji. Wpływa to na zwiększenie wartości certyfikacji PECB i jej rozpoznawalność na rynkach międzynarodowych.

PROWADZIMY SZKOLENIA Z ZAKRESU:

Risk Management ISO 27005 i ISO 31000

Information Security ISO 27001

Business Continuity ISO 22301

Disaster Recovery ISO 24762

CTS Customized Training Solutions
www.cts.com.pl
szkolenia@cts.com.pl
tel +48 22 208 28 61

SPIS TREŚCI

GŁÓWNI AUTORZY
ERIC LACHAPELLE,
PECB MUSTAFE BISLIMI , PECB

Wprowadzenie

Wiele organizacji podejmuje kroki związane z bezpieczeństwem informacji lub podejmuje działania kontrolne w celu zapewnienia ochrony swoim informacjom, procesom biznesowym lub aktywom w postaci informacji. Jednak bez formalnie określonego Systemu Zarządzania Bezpieczeństwem Informacji te działania kontrolne są skazane na dezorganizację i chaos, ponieważ stanowią jedynie tymczasowe środki zaradcze wprowadzane w trybie ad hoc w zależności od konkretnej sytuacji. Prawdziwe wyzwanie dla małych i większych organizacji nie polega na wyjściu poza zakres posiadania scenariuszy rozwiązań dla konkretnych sytuacji zagrożenia bezpieczeństwa informacji. Wyzwanie to polega na zaangażowaniu się we wdrożenie kompleksowego podejścia do kwestii bezpieczeństwa informacji, a dla realizacji tego celu idealnym rozwiązaniem jest ISO/IEC 27001.

Organizacje wszelkiego typu i rozmiaru niezależnie od tego, czy są zaangażowane bezposrednıo lub pośrednio w Technologię Informacyjną powinny teraz przystąpić do realizacji całościowego, usystematyzowanego, prewencyjnego, ochronnego, przygotowawczego oraz ograniczającego ryzyko procesu. Nie wystarczy już proste zaprojektowanie planu reagowania, który przewiduje lub minimalizuje konsekwencje zdarzeń mających wpływ na utratę bezpieczeństwa informacji. Organizacje potrzebują również podejmować działania adaptacyjne i proaktywne w celu ograniczenia prawdopodobieństwa tego typu zdarzeń.

Bezpieczeństwo Informacji w zakresie standardu ISO 27001 jest bardzo ważne, ponieważ wnosi dodatkową wartość do obecnie stosowanych systemów zarządzania jakością we wszelkiego typu organizacjach. Umożliwia ponadto określenie zagrożeń i odpowiednich sposobów postępowania w stosunku do aktywów w postaci priorytetyzowania informacji. Dzięki zaangażowaniu zainteresowanych stron w procesy bezpieczeństwa zwiększa się poziom wzajemnego zaufania. Umożliwia również prowadzenie niezależnych audytów bądź przeglądów w stosunku do tych procesów.

ISO/IEC 27001 zostało zaprojektowane w ten sposób, żeby udzielić wsparcia organizacjom oraz zminimalizować ryzyko zakłóceń w prowadzeniu przez nie działalności. Przedmiotowy standard jest zwieńczeniem wcześniejszych prób osiągnięcia tego celu o charakterze częściowym, a które to próby, takie jak BS 7799, COBIT, ITIL, PCI-DSS, SOX, COSO, HIPAA, FISMA oraz FIPS przyczyniły się do stworzenia systemu Zarządzania Bezpieczeństwem Informacji.

Koszt naruszenia bezpieczeństwa Informacji
Według badania przeprowadzonego w Wielkiej Brytanii w roku 2013 dotyczącego naruszeń bezpieczeństwa informacji około 90% organizacji zmagało się z tego typu problemem w zeszłym roku. Z 14% dużych organizacji wykradziono własność intelektualną lub informacje poufne.

Spośród wyżej opisanych sytuacji dotyczących naruszenia bezpieczeństwa informacji małe firmy poniosły koszt naprawy wynikłych z tego szkód wahający się w najgorszych przypadkach na poziomie od 35 tys. do 65 tys. funtów brytyjskich. W przypadku dużych organizacji koszt ten wzrósł do poziomu 850 tys. funtów. Czynniki składające się na wyżej opisane straty finansowe zawierały konieczność przerwania prowadzenia działalności przez okres kilku dni, konieczność oddelegowania dużej ilości osób do prowadzenia działań naprawczych, wymierne straty finansowe rzędu setek tysięcy funtów, konieczność przeznaczenia środków na prowadzenie bezpośrednich działań naprawczych, kary nakładane przez organy nadzoru, koszty z tytułu rekompensat oraz nadszarpniętą reputację.

CTS Customized Training Solutions
www.cts.com.pl
szkolenia@cts.com.pl
tel +48 22 208 28 61

Przegląd ISO 27001

ISO 27001 określa wymagania niezbędne do zaplanowania, wdrożenia, zarządzania, monitorowania, prowadzenia przeglądu, systematycznego ulepszania systemu zarządzania oraz do przygotowania planu i określenia sposobu reagowania na zdarzenia związane z bezpieczeństwem informacji, które mogą się zdarzyć.

ISO/IEC 27001 zostało zaprojektowane w celu ujęcia bezpieczeństwa informacji w odpowiednie ramy kontrolne. Zawiera ponad 100 konkretnych wymagań.

Zbiór wymogów ISO 27001 jest generyczny, elastyczny i przydatny we wszelkiego typu organizacjach. Z tego powodu przedmiotowy standard ISO będący Systemem Zarządzania może być połączony z innymi Systemami Zarządzania takimi jak Zarządzanie Jakością (ISO 9001), Zarządzanie Trwałością Biznesową (ISO 22301) oraz z innymi systemami zarządzania dzięki ich podobnej strukturze.

Czym jest System Zarządzania Bezpieczeństwem Informacji?

System Zarządzania bezpieczeństwem informacji jest częścią całościowego systemu zarządzenia opartym na podejściu do ryzyka biznesowego w celu wdrożenia, zarządzania, monitorowania, prowadzenia przeglądu oraz wzmacniania bezpieczeństwa informacji.

KLUCZOWE CZĘŚCI ISO 27001

ISO 27001 PODZIELONE JEST NA NASTĘPUJĄCE GŁÓWNE CZĘŚCI:

Cześć 4: Kontekst organizacji
Część 5: Przywództwo
Część 6: Planowanie
Część 7: Wsparcie
Część 8: Działanie
Część 9: Ewaluacja działania
Część 10: Rozwój

Każdy z tych kluczowych elementów został opisany poniżej:

CTS Customized Training Solutions
www.cts.com.pl
szkolenia@cts.com.pl
tel +48 22 208 28 61

CZĘŚĆ 4: KONTEKST ORGANIZACJI
ZROZUMIENIE ORGANIZACJI I JEJ KONTEKSTU

Określenie zewnętrznych i wewnętrznych kwestii, które wywierają wpływ na możliwość osiągnięcia zamierzonych celów przez organizację w zakresie realizacji Systemu Zarządzania Bezpieczeństwem Informacji (System Zarządzania Bezpieczeństwem Informacji)

ZROZUMIENIE POTRZEB I OCZEKIWAŃ ZAINTERESOWANYCH STRON

Organizacje powinny określić:

- zainteresowane strony w odniesieniu do Systemu Zarządzania Bezpieczeństwem Informacji;
- wymagania zainteresowanych stron odnośnie bezpieczeństwa informacji.

OKREŚLENIE ZAKRESU DZIAŁANIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Organizacja powinna określić granice oraz zakres stosowania Systemu Zarządzania Bezpieczeństwem Informacji w celu określenia:

- kwestii zewnętrznych i wewnętrznych, jakie się do niego odnoszą;
- wymagań, jakie się do niego odnoszą;
- wspólnych płaszczyzn oraz wzajemnych zależności w zakresie działań realizowanych przez organizację oraz zakresu działań realizowanych przez inne organizacje.

Ten zakres powinien być dostępny w postaci informacji w formie dokumentu.

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Organizacja powinna stworzyć, wdrożyć, utrzymywać i systematycznie ulepszać System Zarządzania Bezpieczeństwem Informacji zgodnie z wymogami przedmiotowego standardu.

CZĘŚĆ 5: PRZYWÓDZTWO
PRZYWÓDZTWO I ZAANGAŻOWANIE:

W celu zrealizowania sprawnego Systemu Zarządzania Bezpieczeństwem Informacji kierownictwo najwyższego szczebla powinno wykazać zaangażowanie i pokierować realizacją tworzenia systemu zarządzania informacją poprzez:

- odpowiedniej polityki dla Systemu Zarządzania Bezpieczeństwem Informacji, który będzie zgodny ze strategicznym kierunkiem obranym przez organizację;
- zapewnienie integracji Systemu Zarządzania Bezpieczeństwem Informacji z procesami organizacji;
- zapewnienie dostępności zasobów niezbędnych do realizacji Systemu Zarządzania Bezpieczeństwem Informacji;
- prowadzenie odpowiedniej komunikacji;
- wyznaczenie osób odpowiedzialnych za kierowanie i wspieranie Systemu Zarządzania Bezpieczeństwem Informacji;
- promowanie trwałego rozwoju.

POLITYKA: Kierownictwo najwyższego szczebla powinno stworzyć politykę bezpieczeństwa, która:

- spełnia cele organizacji;
- uwzględnia cele bezpieczeństwa informacji oraz gwarantuje odpowiedni udział w realizacji jej wymagań;
- gwarantuje systematyczne zaangażowanie w jej ustawiczny rozwój;
- powinna być dostępna jako informacja w formie dokumentu oraz być komunikowana wewnętrznie.

ROLE ORGANIZACYJNE, ZAKRESY ODPOWIEDZIALNOŚCI I UPOWAŻNIENIA: Kierownictwo najwyższego szczebla powinno zagwarantować, że odpowiednie zakresy odpowiedzialności oraz upoważnień są odpowiednio przypisane i zakomunikowane:

- zapewnienie, że System Zarządzania Bezpieczeństwem Informacji jest zgodny z wymaganiami przedmiotowego Standardu Międzynarodowego;
- przygotowywanie sprawozdań dla kierownictwa najwyższego szczebla na temat działania Systemu Zarządzania Bezpieczeństwem Informacji.

CZĘŚĆ 6: PLANOWANIE

ZAPEWNIENIE ODPOWIEDNIEGO DZIAŁANIA W STOSUNKU DO RYZYKA I MOŻLIWOŚCI:

- zagwarantowanie, że System Zarządzania Bezpieczeństwem Informacji może osiągnąć przewidziane dla siebie cel lub cele;
- zapobieganie lub redukcja niepożądanych efektów oraz osiąganie trwałego postępu;
- planowanie działań w celu zapewnienia odpowiedniego działania w stosunku do ryzyka i możliwości;
- przygotowanie sprawozdań na temat działania Systemu Zarządzania Bezpieczeństwem Informacji dla kierownictwa najwyższego szczebla.

OCENA RYZYKA BEZPIECZEŃSTWA INFORMACJI:

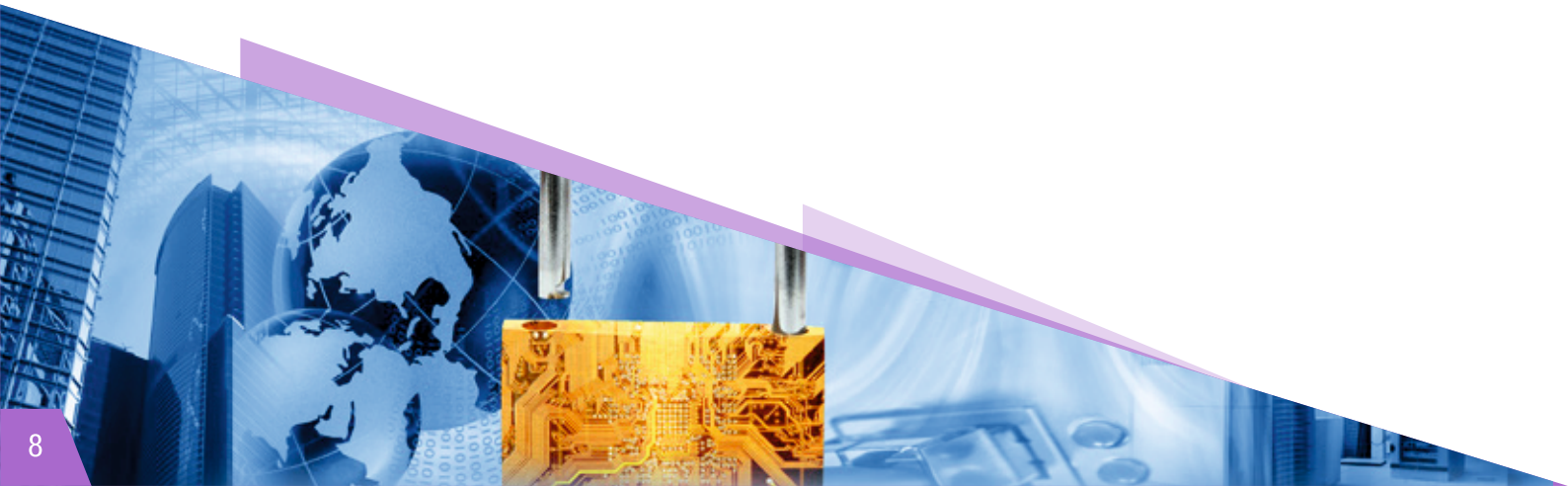
- ustanawia kryteria bezpieczeństwa informacji oraz ich realizacji;
- zapewnia, że powtarzalna ocena ryzyka bezpieczeństwa informacji generuje logiczne, wartościowe i porównywalne rezultaty;
- określa ryzyka bezpieczeństwa informacji;
- analizuje i ocenia ryzyko bezpieczeństwa informacji.

POSTĘPOWANIE Z RYZYKIEM UTRATY BEZPIECZEŃSTWA INFORMACJI:

- selekcja opcji postępowania z ryzykiem utraty bezpieczeństwa informacji, przygotowanie zestawienia zawierającego rezultaty oceny ryzyka;
- określenie wszystkich działań kontrolnych niezbędnych do wdrożenia systemu postępowania z ryzykiem utraty bezpieczeństwa informacji;
- stworzenie planu postępowania z ryzykiem utraty bezpieczeństwa informacji;
- uzyskanie akceptacji osoby odpowiedzialnej za dany zakres ryzyka odnośnie planu postępowania z ryzykiem utraty bezpieczeństwa informacji.

CELE BEZPIECZEŃSTWA INFORMACJI ORAZ PLANOWANIE ICH OSIĄGNIĘCIA:

- zgodność z polityką bezpieczeństwa informacji;
- mierzalność, informowanie oraz aktualizowanie stosowanie do sytuacji;
- wzięcie pod uwagę wymogów bezpieczeństwa informacji oraz rezultatów powstałych w rezultacie przeprowadzenia oceny ryzyka oraz analizy postępowania z ryzykiem;
- w trakcie planowania tego, jak osiągnąć swoje cele, organizacja powinna określić: co zostanie zrealizowane, jaki będzie zakres niezbędnych zasobów, kto będzie za to odpowiedzialny, kiedy zostanie to ukończone oraz zapewnić, że zostanie sporządzona odpowiednia ewaluacja.



CZĘŚĆ 7: WSPARCIE

ZASOBY:

Organizacja powinna określić zakres zasobów oraz zapewnić dostępność tych zasobów w zakresie niezbędnym do ustanowienia, wdrożenia, utrzymania oraz zapewnienia trwałego rozwoju Systemu Zarządzania Bezpieczeństwem Informacji.

KOMPETENCJE:

- określenie niezbędnych kompetencji osoby lub osób, które pracują pod kontrolą organizacji, a ich praca ma wpływ na działanie Systemu Zarządzania Bezpieczeństwem Informacji
- podejmowanie decyzji (w zależności od sytuacji) odnośnie niezbędnych kompetencji oraz dokonanie ewaluacji podjętych działań;
- gromadzenie odpowiednio udokumentowanych informacji, które ilustrują odpowiednie kompetencje.

BUDOWANIE ŚWIADOMOŚCI

Osoby wykonujące pracę pod kontrolą organizacji powinny być świadome: polityki, wkładu, jaki wnoszą do efektywności Systemu Zarządzania Bezpieczeństwem Informacji oraz efektów, jakie powoduje niespełnianie kryteriów Systemu Zarządzania Bezpieczeństwem Informacji.

KOMUNIKOWANIE:

Organizacje powinny określić potrzebę prowadzenia komunikacji wewnętrznej i zewnętrznej w związku z Systemem Zarządzania Bezpieczeństwem Informacji w szczególności tego, co komunikować, kiedy i kto powinien być adresatem takich komunikatów oraz kto powinien prowadzić tego typu komunikację.

PROWADZENIE DOKUMENTACJI INFORMACJI:

System Zarządzania Bezpieczeństwem Informacji organizacji powinien zawierać prowadzenie dokumentacji informacji zgodnie z wymogami standardu ISO 27001, tworzenie oraz aktualizowanie stworzonej dokumentacji na temat informacji oraz odpowiednie prowadzenie dokumentowanej informacji. System Zarządzania Bezpieczeństwem Informacji danej organizacji powinien być ponadto odpowiednio chroniony, a informacje w niej zgromadzone powinny być możliwe do wykorzystania.

CZĘŚĆ 8: DZIAŁANIE

PLANOWANIE DZIAŁANIA ORAZ KONTROLI. OCENA BEZPIECZEŃSTWA INFORMACJI ORAZ ODPOWIEDNIEGO SPOSOBU POSTĘPOWANIA:

Organizacja powinna planować, wdrażać oraz kontrolować procesy niezbędne do spełnienia wymogów bezpieczeństwa informacji.

Organizacja powinna przeprowadzać oceny bezpieczeństwa informacji w regularnych odstępach czasu lub w przypadku propozycji wdrożenia istotnych zmian lub też w przypadku zachodzenia istotnych zmian.

Organizacja powinna wdrożyć plan postępowania w stosunku do ryzyka utraty bezpieczeństwa informacji.

CZĘŚĆ 9: EWALUACJA DZIAŁANIA

MONITOROWANIE, KRYTERIA OCENY, ANALIZY ORAZ EWALUACJA:

Organizacja powinna dokonywać ewaluacji działania bezpieczeństwa informacji oraz efektywności Systemu Zarządzania Bezpieczeństwem Informacji

- co powinno być monitorowane i mierzone z uwzględnieniem procesów związanych z bezpieczeństwem informacji oraz działań kontrolnych
- jakie metody monitorowania, mierzenia, analizowania i oceniania zależnie od sytuacji w celu zagwarantowania otrzymania prawidłowych rezultatów powinny być zastosowane;

AUDYT WEWNĘTRZENY:

- organizacja powinna przeprowadzać audyty wewnętrzne w regularnych odstępach czasu w celu przedstawienia informacji odnośnie tego, czy System Zarządzania Bezpieczeństwem Informacji spełnia wymogi organizacji oraz czy System Zarządzania Bezpieczeństwem Informacji jest odpowiednio wdrożony i prowadzony.
  Organizacja powinna:
- planować, ustanawiać, wdrażać i utrzymywać programy audytowe, uwzględniając przy tym częstotliwość, metody, zakresy odpowiedzialności, wymogi odnośnie planowania oraz przygotowywanie sprawozdań. W programach audytu powinno być wzięte pod uwagę to, jak ważne są dane procesy oraz rezultaty poprzednich audytów;
- określać kryteria audytu oraz zakres każdego audytu;
- dokonać selekcji audytorów oraz przeprowadzać audyty w celu zapewnienia obiektywności oraz w stosunku do procesu audytowego;
- zagwarantować, że rezultaty audytów są przekazywane w formie raportu do odpowiedniego kierownictwa
- gromadzić informacje w formie dokumentu, tak aby móc zaprezentować programy audytowe oraz rezultaty tych audytów.

PRZEGLĄD ZE STRONY KIEROWNICTWA NAJWYŻSZEGO SZCZEBLA:

Kierownictwo najwyższego szczebla powinno prowadzić przegląd Systemu Zarządzania Bezpieczeństwem Informacji w zaplanowanych odstępach czasu w celu zapewnienia jego trwałości, odpowiedniości, adekwatności oraz efektywności.

Przegląd ze strony kierownictwa organizacji powinien uwzględniać następujące czynniki:

- status działań od czasu poprzednich przeglądów ze strony kierownictwa firmy;
- zmiany w zewnętrznych i wewnętrznych kwestiach, które odnoszą się do Systemu Zarządzania Bezpieczeństwem Informacji;
- informacja zwrotna odnośnie działania bezpieczeństwa informacji.

CZĘŚĆ 10: ROZWÓJ

NIEZGODNOŚCI, DZIAŁANIA NAPRAWCZE ORAZ STAŁY ROZWÓJ

W przypadku wykrycia niezgodności organizacja powinna:

- reagować na niezgodności w zależności od sytuacji;
- ocenić potrzebę działania w celu wyeliminowania powodów, które powodują niezgodności w celu zapewnienia, że dana niezgodność nie powtórzy się bądź nie zdarzy się gdzie indziej;
- wdrożyć wszelkie potrzebne działania;
- prowadzić przegląd efektywności wszelkich podjętych działań naprawczych;
- w miarę potrzeby wprowadzać zmiany do Systemu Zarządzania Bezpieczeństwem Informacji.

Działania naprawcze powinny być dostosowane do napotkanych niezgodności.

Organizacja powinna gromadzić udokumentowane informacje w celu określenia:

- natury niezgodności oraz wszelkich później podejmowanych działań;
- rezultatów wszelkich działań naprawczych.

ZWIĄZEK Z INNYMI STANDARDAMI BEZPIECZEŃSTWA ORAZ WYTYCZNYMI

- istnieją inne dobrze znane standardy powiązane z ISO 27001:
- zasady OECD (2002)
- PCI-DSS - standard poziomu bezpieczeństwa we wszystkich środowiskach, w których przetwarzane są dane posiadaczy kart płatniczych, (ang. Payment Card Industry Data Security Standard) (2004)
- basel II (2004)
- COBIT – zbiór dobrych praktyk z zakresu IT (ang. Control Objectives for Business and related Technology) (1994+)
- ITIL – kodeks postępowania dla działów informatyki oraz zbiór zaleceń, jak efektywnie i skutecznie oferować usługi informatyczne (ang. Information Technology Infrastructure Library) (1980+)

ZWIĄZEK Z ISO 22301 – TRWAŁOŚĆ BIZNESOWA

ISO 27001 jest przydatne jako część procesu certyfikacyjnego prowadzącego do uzyskania certyfikatu ISO 22301 (trwałość biznesowa). Cele ISO 27001 w części A.14 (Zarządzanie Trwałością Biznesową) mogą być użyte w celu zapewnienia zgodności z ISO 22301. Ponadto w kwestii wdrożenia i realizacji oceny ryzyka organizacja może zawsze odnieść się do ISO/IEC 27005 lub w szerszym kontekście do ISO 31000 – Zarządzanie Ryzykiem – Zasady i Wytyczne lub, w celu przeprowadzenia samodzielnej oceny, może również odnieść się do ISO 31010 – Zarządzanie Ryzykiem – Techniki oceny ryzyka.

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI – KORZYŚCI DLA BIZNESU

W przypadku wszystkich większych przedsięwzięć w danej organizacji niezbędne jest uzyskanie poparcia i wsparcia finansowego ze strony zarządu danej organizacji. Niepodważalnie najlepszym sposobem na uzyskanie tego celu jest zilustrowanie korzyści posiadania działającego systemu zarządzania bezpieczeństwem informacji niż podkreślanie negatywnych aspektów scenariusza odwrotnego.

Obecnie efektywne zarządzanie bezpieczeństwem informacji nie polega na byciu zmuszonym do podejmowania działania w celu reagowania na zdarzenia zewnętrzne. Jego znaczenie opiera się na rozpoznaniu pozytywnej wartości Bezpieczeństwa Informacji, gdy określona dobra praktyka wdrożona jest w Państwa organizacji.

PRZEWIDYWALNE I EFEKTYWNE REAGOWANIE NA ZDARZENIA ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMACJI	**ZAPEWNIENIE OCHRONY PRACOWNIKOM**	**UTRZYMYWANIE NA OPTYMALNYM POZIOMIE STRATEGICZNYCH DZIAŁAŃ ORGANIZACJI**	**LEPSZE ZROZUMIENIE ORGANIZACJI**
REDUKCJA KOSZTÓW	**UWZGLĘDNIENIE INTERESÓW ZAINTERESOWANYCH STRON**	**OCHRONA REPUTACJI ORAZ MARKI**	**POCZUCIE BEZPIECZEŃSTWA ZE STRONY KLIENTÓW**
PRZEWAGA KONKURENCYJNA	**ZGODNOŚĆ Z PRZEPISAMI PRAWA**	**ZGODNOŚĆ Z REGULACJAMI**	**ZAPEWNIENIE ZGODNOŚCI Z ZAPISAMI W UMOWACH**

Wdrożenie efektywnego procesu zarządzania bezpieczeństwem informacji będzie miało korzyści w wielu dziedzinach, których przykłady są podane poniżej:

1. Ochrona wartości dla akcjonariuszy
2. Zwiększone poczucie bezpieczeństwa względem zainteresowanych stron w danej organizacji
3. Dobre zarządzanie
4. Zapewnienie zgodności i prawidłowości
5. Możliwość przeprowadzenia prawidłowej oceny określonych konsekwencji w stosunku do obowiązku dochowania staranności oraz przepisów prawa w stosunku do bezpieczeństwa informacji
6. Możliwość uniknięcia bycia pociąganym do odpowiedzialności
7. Redukcja kosztów
8. Zwiększenie całościowego bezpieczeństwa
9. Marketing

CERTYFIKOWANIE ORGANIZACJI

Typowa ścieżka wybierana przez organizacje, które chcą uzyskać certyfikat ISO 27001 została opisana poniżej:

1. Wdrażanie system zarządzania: Przed przeprowadzeniem audytu system zarządzania musi być wykorzystywany przez pewien czas. Zazwyczaj minimalny czas działania systemu wymagany przez jednostki certyfikacyjne wynosi 3 miesiące.

2. Audyt wewnętrzny i prowadzenie przeglądu przez kierownictwo najwyższego szczebla: Zanim będzie możliwe przeprowadzenie certyfikacji systemu, dany system powinien do tego czasu przejść audyt wewnętrzny oraz przegląd ze strony kierownictwa najwyższego szczebla.

3. Wybór jednostki certyfikacyjnej: Każda organizacja może wybrać jednostkę certyfikacyjną wedle własnego uznania.

4. Audyt wstępny (opcjonalny): Organizacja może zdecydować się na przeprowadzenie wstępnego audytu w celu określenia braków, jakie istnieją pomiędzy obecnym systemem zarządzania a wymogami dla określonego standardu.

5. Audyt poziomu 1: Przegląd zgodności projektu systemu zarządzania. Jego głównym celem jest zweryfikowanie, że system zarządzania jest zaprojektowany tak, aby spełniać wymogi standardów oraz cele organizacji. Zalecane jest, aby przynajmniej pewna część audytu poziomu 1 była przeprowadzona w danej organizacji na miejscu.

6. Audyt poziomu 2 (wizyta na miejscu): Celem audytu poziomu 2 jest określenie czy zadeklarowany system zarządzania odpowiada wszystkim wymaganiom standardu, czy ma faktyczne zastosowanie oraz czy może wspierać organizację w osiąganiu jej celów. Ten etap realizowany jest na miejscu w organizacji bądź w miejscach, w których organizacja prowadzi swoją działalność, gdzie system zarządzania jest wdrażany.

7. Audyt sprawdzający (opcjonalny): Jeżeli organizacja przechodząca audyt ma obszary niezgodności, które wymagają dodatkowego sprawdzenia przed przystąpieniem do procesu certyfikacyjnego, audytor przeprowadzi audyt sprawdzający na miejscu w celu określenia planu działań w odniesieniu jedynie do obszarów niezgodności (zazwyczaj zajmuje to jeden dzień).

8. Potwierdzenie rejestracji: Jeżeli organizacja spełnia wymogi określonego standardu, Organizacja Certyfikujące potwierdza rejestrację i wydaje certyfikat.

9. Systematyczna poprawa wydajności oraz audyty kontrolne: Po dokonaniu rejestracji organizacji czynności kontrolne są przeprowadzane przez Organizację Certyfikującą w celu zapewnienia, że system zarządzania w dalszym ciągu spełnia wymogi danego standardu. W skład czynności kontrolnych wchodzą wizyty na miejscu (min. raz na rok), które umożliwiają zweryfikowanie zgodności danego systemu zarządzania klienta. Ponadto w ich skład może wchodzić prowadzenie przeglądu strony internetowej, wyjaśnienie problemu po przekazaniu zgłoszenia, pisemna prośba o udzielenie wsparcia.

SZKOLENIA ORAZ CERTYFIKOWANIE SPECJALISTÓW

Organizacja PECB stworzyła rekomendowaną mapę drogową szkoleń oraz określone programy dedykowane osobom odpowiedzialnym za wdrożenia i nadzór w organizacji, które chcą uzyskać certyfikat ISO 27001. Mimo że certyfikowanie organizacji jest znaczącym elementem zagadnienia bezpieczeństwa informacji, gdyż stanowi dowód tego, że organizacje rozwinęły standaryzowane procesy oparte na najlepszych praktykach, to certyfikowanie osób również stanowi dowód na uzyskanie kompetencji zawodowych oraz doświadczenia przez osoby, który wcześniej brały udział w określonym szkoleniu bądź egzaminie.

Służy to również do wykazania, że osoba, która uzyskała certyfikat, posiada określone kompetencje oparte na najlepszych praktykach. Organizacje ponadto mogą przeprowadzać świadomą selekcję pracowników bądź usług na podstawie kompetencji, które są wykazane w danym certyfikacie. Szczególnie ważne jest to, że określona osoba otrzymuje dodatkową motywację do ciągłego rozwijania swoich umiejętności oraz poszerzania wiedzy, gdyż pracodawcy otrzymują narzędzie gwarantujące skuteczność szkolenia.

Kursy szkoleniowe organizacji PECB są ofertowane globalnie przez sieć autoryzowanych ośrodków szkoleniowych w wielu językach i zawierają zagadnienia z poziomów introduction, foundation, implementer i auditor. Poniższa tabela przedstawia krótki opis oficjalnych kursów szkoleniowych organizacji PECB dotyczących Systemu Zarządzania Bezpieczeństwem Informacji w oparciu o ISO 27001.

Nazwa szkolenia	Krótki opis	Kto powinien w nim uczestniczyć?
ISO 27001 Introduction	• Wprowadzenie do pojęć związanych z zarządzaniem i wdrażaniem Systemu Zarządzania Bezpieczeństwem Informacji • Nie kończy się uzyskaniem certyfikatu	• Specjaliści ds. IT • Osoby zaangażowane we wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji • Konsultanci ds. IT • Pracownicy szczebla kierowniczego odpowiedzialni za wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji
ISO 27001 Foundation	• Zaznajomienie się z najlepszymi praktykami dot. wdrażania i zarządzania Systemem Zarządzania Bezpieczeństwem Informacji • Godzinny egzamin	• Członkowie zespołu odpowiedzialnego za bezpieczeństwo informacji • Specjaliści ds. IT • Osoby zaangażowane w System Zarządzania Bezpieczeństwem Informacji • Technicy • Osoby sprawujące nadzór
ISO 27001 Lead Implementer	• Zarządzanie Systemem Zarządzania Bezpieczeństwem Informacji oraz zarządzanie wdrażaniem tego systemu • Trzygodzinny egzamin	• Project menedżerzy i/lub konsultanci • Osoby sprawujące nadzór nad bezpieczeństwem informacji • Członkowie zespołu ds. bezpieczeństwa informacji • Eksperci techniczni
ISO 27001 Lead Auditor	• Zarządzanie nadzorem nad • Systemem Zarządzania Bezpieczeństwem Informacji • Trzygodzinny egzamin	• Osoby odpowiedzialne za nadzór wewnętrzny • Osoby sprawujące nadzór • Project menedżerzy i/lub konsultanci • Członkowie zespołu ds. bezpieczeństwa informacji • Eksperci techniczni

Pomimo, iż określony zestaw kursów bądź zakres materiału nie jest wymagany w procesie certyfikacyjnym, to ukończenie uznawalnego kursu bądź cyklu zajęć organizacji PECB znacząco wzmocni szanse zdania egzaminu certyfikacyjnego organizacji PECB. Mogą Państwo sprawdzić autoryzowane ośrodki szkoleniowe realizujące oficjalne szkolenia organizacji PECB pod adresem www.pecb.org/en/eventlist.

WYBÓR ODPOWIEDNIEGO CERTYFIKATU

Certyfikat ISO 27001 Foundation jest certyfikatem zawodowym dla specjalistów chcących uzyskać całościowe zrozumienie standardu ISO 27001 i jego wymogów.

Certyfikaty The ISO 27001 Lead Implementer są certyfikatami zawodowymi dla specjalistów chcących wdrożyć System Zarządzania Bezpieczeństwem Informacji, a w przypadku certyfikatu ISO 27001 Lead Implementer certyfikat ten przeznaczony jest dla specjalistów chcących zarządzać projektem wdrożeniowym.

Certyfikaty ISO 27001 Auditor są certyfikatami dedykowanymi specjalistom, którzy chcą sprawować nadzór nad Systemem Zarządzania Bezpieczeństwem Informacji, a w przypadku certyfikatu ISO 27001 Lead Auditor certyfikat ten dedykowany jest specjalistom, którzy chcą zarządzać zespołem audytowym.
Certyfikat ISO 27001 Master jest certyfikatem zawodowym dedykowanym specjalistom, którzy chcą wdrożyć System Zarządzania Bezpieczeństwem Informacji, zgłębić techniki sprawowania nadzoru oraz zarządzać zespołami audytowymi lub też zarządzać programem nadzoru. Dotyczy to również osób, które chcą być częścią takich zespołów lub chcą być zaangażowane w taki program.

W zależności od całościowego doświadczenia i zdobytych kwalifikacji otrzymają Państwo jeden lub więcej z tych certyfikatów w oparciu o projekty lub zadania związane z nadzorem, które wykonywali Państwo w przeszłości lub w oparciu o zadania, nad którymi pracują Państwo obecnie.

Masz pytania?
Skontakuj się z nami!

CTS Customized Training Solutions Sp z o.o.
al. Jana Pawła II 25
00-854 Warszawa

tel./fax: **+48 22 208 28 61**
szkolenia@cts.com.pl

www.cts.com.pl