Biała księga
ISO 31000

ZARZĄDZANIE RYZYKIEM – ZASADY I WSKAZÓWKI

CTS Customized Training Solutions

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 Managment 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
Besnik HUNDOZI, PECB

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

Wprowadzenie

ISO 31000 jest międzynarodowym standardem wprowadzonym w 2009 r. przez ISO (Międzynarodowa Organizacja Normalizacyjna), którego celem jest stworzenie przewodnika dla projektowania, wdrażania i utrzymania procesu zarządzania ryzykiem.

Organizacje każdego typu i rozmiaru stykają się z wewnętrznymi i zewnętrznymi czynnikami i wpływami, które powodują poczucie niepewność odnośnie tego, czy uda im się osiągnąć swoje cele. Efekt niepewności w stosunku do celów organizacji to właśnie ryzyko.

Ryzyko zawarte jest w każdej sferze aktywności danej organizacji. ISO 31000 opisuje systematyczny oraz logiczny proces, podczas którego organizacje zarządzają ryzykiem poprzez jego określenie, analizę oraz ocenę. Umożliwia to podjęcie decyzji odnośnie tego, czy dane ryzyko powinno być zmodyfikowane dzięki zastosowaniu odpowiedniego sposobu postępowania z ryzykiem poprzez określenie, czy dany rodzaj ryzyka wykracza poza przyjęte normy ryzyka.

Zarządzanie ryzykiem może być zastosowane na całej przestrzeni funkcjonowania organizacji, na jej wielu obszarach i poziomach, w dowolnym czasie oraz w stosunku do określonych funkcji, projektów oraz czynności.

RYZYKO – EFEKT NIEPEWNOŚCI W STOSUNKU DO CELÓW

PRZEGLĄD ISO 31000

ISO 31000 zapewnia zasady oraz generyczne wytyczne w celu zapewnienia pomocy danej organizacji w tworzeniu, wdrażaniu, zarządzaniu, utrzymaniu oraz ciągłemu polepszaniu ram zarządzania ryzykiem.

Ramy te nie są ściśle związane z żadną branżą czy sektorem, więc mogą być używane przez wszelkie przedsiębiorstwa publiczne, prywatne czy społeczne, stowarzyszenia, grupy oraz osoby fizyczne. Standard może być stosowany w trakcie całego cyklu rozwoju organizacji oraz w stosunku do szerokiego zakresu czynności, również w odniesieniu do strategii i decyzji, operacji, procesów, funkcji, projektów, produktów, usług czy różnego rodzaju aktywów.

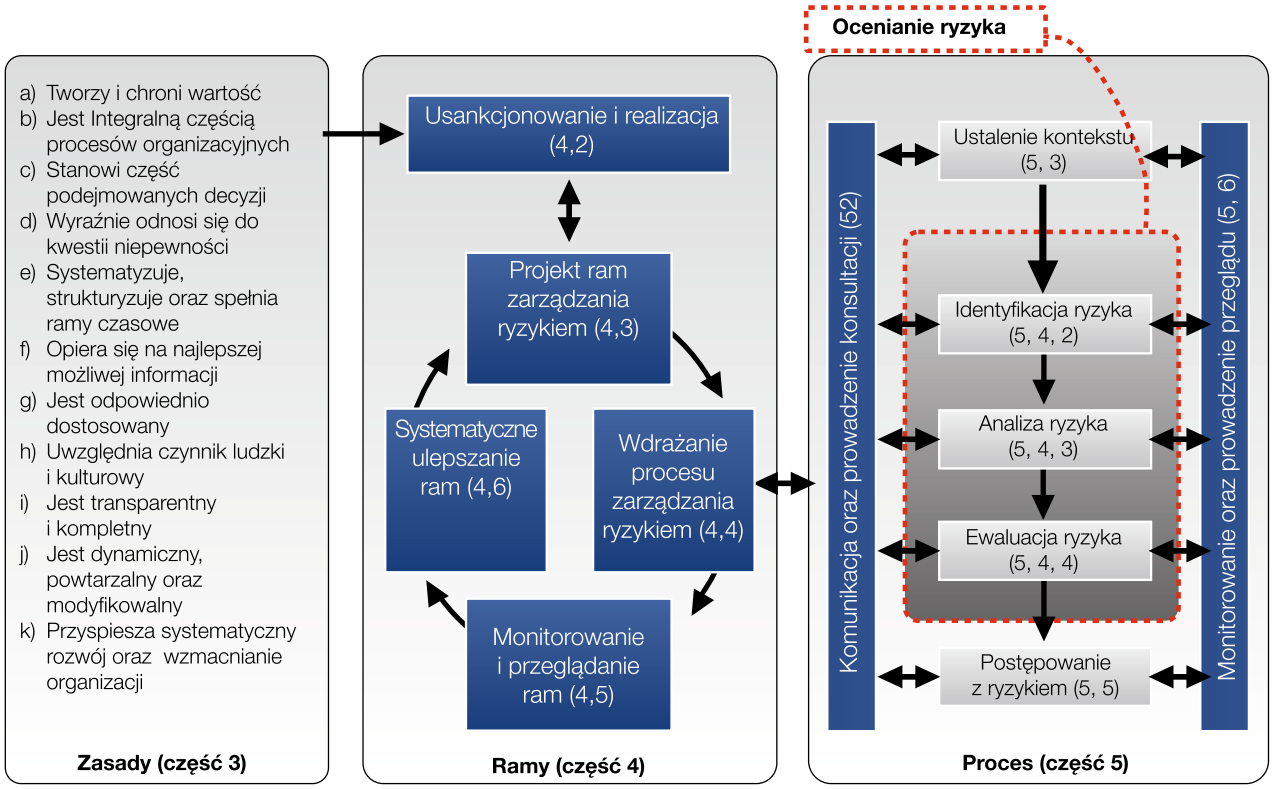
Standard ten nie ma na celu promowania jednolitości zarządzania ryzykiem w organizacjach. Projekt oraz implementacja planów oraz ram zarządzania ryzykiem będą musiały uwzględnić różne potrzeby określonych organizacji, ich szczególnych celów, kontekstu, operacji, procesów, funkcji, projektów, produktów, usług oraz aktywów i konkretnych wdrożonych praktyk.

CZYM JEST ZARZĄDZANIE RYZYKIEM?

Zarządzanie ryzykiem zostało zdefiniowane jako zbiór skoordynowanych czynności w celu odpowiedniego ukierunkowania organizacji oraz prowadzenia czynności kontrolnych w organizacji pod kątem ryzyka.

STRUKTURA ISO 31000

Poniższy obrazek pokazuje związki pomiędzy zasadami zarządzania ryzykiem, ramami oraz procesem.



Kluczowe elementy ISO 31000

Standard ISO 31000 składa się z następujących części:
Część 3: Zasady
Część 4: Ramy
Część 5: Proces

Podział każdej czynności kluczowej znajduje się poniżej.

CZEŚĆ 3: ZASADY ZARZĄDZANIA RYZYKIEM

W celu uzyskania skutecznego procesu zarządzania ryzykiem organizacja musi spełniać 11 wymogów.

1. Proces zarządzania ryzykiem tworzy i chroni wartość;
2. Proces zarządzania ryzykiem jest integralną częścią wszystkich procesów organizacyjnych;
3. Proces zarządzania ryzykiem jest częścią procesu podejmowania decyzji;
4. Proces zarządzania ryzykiem wyraźnie odnosi się do kwestii braku pewności;
5. Proces zarządzania ryzykiem jest procesem systematycznym, ustrukturyzowanym i realizującym ramy czasowe
6. Proces zarządzania ryzykiem oparty jest na możliwie najlepszej informacji;
7. Proces zarządzania ryzykiem jest dostosowany do konkretnych potrzeb;
8. Proces zarządzania ryzykiem uwzględnia czynnik ludzi i kulturowy;
9. Proces zarządzania ryzykiem jest transparentny i kompletny
10. Proces zarządzania ryzykiem jest dynamiczny, powtarzalny oraz modyfikowalny
11. Proces zarządzania ryzykiem przyspiesza systematyczny rozwój oraz ulepszanie organizacji

CZĘŚĆ 4: RAMY

Standard ISO 31000 stanowi, iż sukces zarządzania ryzykiem będzie zależał od efektywności ram zarządzania, które zapewnią podstawy oraz konkretne działania, co spowoduje wdrożenie tego standardu na wszystkich poziomach organizacji.
Ramy te:

- pomagają w zarządzaniu ryzykiem w sposób efektywny poprzez wdrażanie procesu zarządzania ryzykiem;
- gwarantują, że informacje na temat ryzyka pozyskane z procesu zarządzania ryzykiem są adekwatnie raportowane;
- gwarantują, że te informacje są używane jako podstawa do podejmowania decyzji oraz ustalania odpowiedzialności na wszystkich poziomach hierarchii w organizacji.

Ta część opisuje niezbędne elementy ram zarządzania ryzykiem oraz sposobu, w jaki te elementy wzajemnie na siebie w trybie cyklicznym.

Usankcjonowanie i realizacja: Zarządzanie potrzebami organizacji wymaga wykazania silnego i trwałego podejścia do kwestii zarządzania ryzykiem przez określenia polityki zarządzania ryzykiem, celów, zapewnienia zgodności z obowiązującymi przepisami prawa i regulacjami, zapewnienia niezbędnych zasobów dla procesu zarządzania ryzykiem, komunikowania korzyści wynikających z procesu zarządzania ryzykiem dla wszystkich udziałowców/akcjonariuszy.

Projekt ram zarządzania ryzykiem: Przed wdrożeniem organizacja musi przygotować projekt ramy zarządzania ryzykiem. W jego skład wchodzą następujące elementy:
Zrozumienie organizacji oraz kontekstu, w jakim dana organizacja funkcjonuje

- Stworzenie polityki zarządzania ryzykiem
- Ustanowienie struktur odpowiedzialności, hierarchii kierowniczej oraz zakresu posiadania wymaganych kompetencji do zarządzania ryzykiem
- Wdrażanie procesów zarządzania ryzykiem do procesów organizacyjnych
- Alokocia odpowiednich zasobów
- Ustanowienie wewnętrznych i zewnętrznych ścieżek komunikacyjnych oraz mechanizmów raportowania

Wdrażanie procesu zarządzania ryzykiem: Organizacja musi wdrożyć ramy zarządzania ryzykiem w celu zapewnienia, że zarządzanie ryzykiem oraz proces zarządzania ryzykiem są odpowiednio realizowane.

Monitorowanie oraz prowadzenie przeglądu ram: W celu zapewnienia efektywności procesu zarządzania ryzykiem organizacja powinna mierzyć efekty procesu zarządzania ryzykiem oraz osiągnięty postęp, nadzorować, czy ramy zarządzania ryzykiem, polityka i plan są w dalszym ciągu adekwatne oraz prowadzić przegląd efektywności ram zarządzania ryzykiem.

Systematyczne ulepszanie ram: Decyzje odnośnie tego, jak mogą być ulepszane ramy zarządzania ryzykiem, polityka oraz plan, powinny być podejmowane w oparciu o rezultaty monitorowania oraz w oparciu o rezultaty prowadzonego przeglądu.

CZĘŚĆ 5: PROCES

Zgodnie z ISO 31000 sukces zarządzania ryzykiem będzie zależał od efektywności zarządzania.

- Proces zarządzania ryzykiem powinien być:
  - integralną częścią zarządzania;
  - dostosowany do danej kultury i stosowanych tam praktyk;
  - dostosowany do procesów biznesowych tej organizacji.

- Proces zarządzania ryzykiem zawiera następujące czynności:

Komunikacja i prowadzenie konsultacji: Poprzez określenie kontekstu organizacja jasno definiuje swoje cele, określa zewnętrzne i wewnętrzne parametry, które powinny być wzięte pod uwagę w przypadku zarządzania ryzykiem oraz określa zakres oraz kryteria ryzyka dla pozostałej części procesu.

Określenie kontekstu: Poprzez określenie kontekstu organizacja jasno definiuje swoje cele, określa zewnętrzne i wewnętrzne parametry, które powinny być wzięte pod uwagę w przypadku zarządzania ryzykiem oraz określa zakres oraz kryteria ryzyka dla pozostałej części procesu.

Ocenianie ryzyka: Ocenianie ryzyka jest procesem, za pomocą którego organizacja systematycznie precyzuje, analizuje oraz ewaluuje ryzyko.

– Określenie ryzyka: Na tym etapie organizacja określa źródła ryzyka, obszary wpływu, zdarzenia i ich powody oraz ich potencjalne konsekwencje.
– Analiza ryzyka: Po określeniu organizacja przystępuje do stworzenia oraz zrozumienia określonego ryzyka, analizuje przyczyny i powody danego typu ryzyka, jego pozytywne i negatywne konsekwencje oraz prawdopodobieństwo, że te konsekwencje mogą mieć konkretny efekt . Wynik przeprowadzonej analizy ryzyka stanowi podstawę ewaluacji ryzyka oraz podstawę do podjęcia decyzji, odnośnie tego, czy danym ryzykiem należy się zająć, a jeżeli tak, to jakie są najbardziej odpowiednie strategie i metody w postępowaniu z tym ryzykiem.
– Ewaluacja ryzyka: Celem tego kroku jest uzyskanie pomocnej informacji w kwestii podejmowania decyzji odnośnie tego, które ryzyko wymaga tego, aby się nim zająć się wraz z prowadzeniem odpowiedniej selekcji priorytetów.

Postępowanie z ryzykiem: Możliwe opcje powinny zostać wybrane w oparciu o rezultat oceny ryzyka, oczekiwanego kosztu wdrożenia konkretnych opcji oraz oczekiwanych korzyści wynikających z wdrożenia tych opcji.

Monitorowanie oraz prowadzenie przeglądu: Monitorowanie i prowadzenie przeglądu może odbywać się okresowo i powinno stanowić zaplanowaną część procesu zarządzania ryzykiem.

Prowadzenie rejestru procesu zarządzania ryzykiem: Czynności związane z zarządzaniem ryzykiem powinny umożliwiać ich łatwe mierzenie oraz sprawdzanie. W procesie zarządzania ryzykiem prowadzenie rejestru stanowi podstawę do ulepszania zarówno metod i konkretnych narzędzia oraz całościowego procesu.

ZWIĄZEK POMIĘDZY ISO 31000 I INNYMI STANDARDAMI

Standard ISO 31000 związany jest z innymi standardami zarządzania ryzykiem, np. ISO Guide 73 – Risk management vocabulary oraz ISO/IEC 31010 – Risk management – Risk assessment techniques. Standard ISO/IEC 31010 jest standardem wspierającym ISO 31000 i zapewnia wytyczne odnośnie wyboru oraz stosowania metodycznych technik oceny ryzyka.

ZWIĄZEK Z ISO 27005

Standard ISO 27005 oparty jest na ramach ISO 31000 i szczegółowo wyjaśnia, jak przeprowadzać ocenę ryzyka oraz jak należy reagować na ryzyko w kontekście bezpieczeństwa informacji.

ZARZĄDZANIE RYZYKIEM – KORZYŚCI BIZNESOWE

Każde większe przedsięwzięcie w jakiejkolwiek organizacji musi uprzednio uzyskać aprobatę oraz wsparcie finansowe szczebla kierowniczego. Najlepszym możliwym sposobem na osiągnięcie tego celu jest zilustrowanie korzyści posiadania efektywnych i działających ram zarządzania ryzykiem niż podkreślanie negatywnych aspektów nieposiadania procesu zarządzania ryzykiem w ogóle.

Zarządzanie ryzykiem umożliwia organizacji zagwarantowanie, że zna i rozumie ryzyko z odpowiednich zakresów. Wdrożenie sprawnego procesu zarządzania ryzykiem w organizacji przyniesie korzyści w wielu dziedzinach, np.:

- zwiększy prawdopodobieństwo osiągnięcia celów
- będzie promować zarządzanie proaktywne
- promuje świadomą potrzebę określenia oraz odpowiedniego reagowania na ryzyko na przestrzeni całej organizacji
- usprawni proces określania możliwości i zagrożeń
- zapewni zgodność z określonymi przepisami prawa, regulacjami i normami międzynarodowymi
- usprawni obowiązkowe i dobrowolne procesy sprawozdawcze
- usprawni zarządzanie
- zwiększy zaufanie oraz zadowolenie akcjonariuszy
- stworzy odpowiednie podstawy dla podejmowania decyzji oraz planowania
- ulepszy i usprawni procesy kontrolne
- zapewni efektywną alokację zasobów oraz wykorzystywanie zasobów w odniesieniu do danego typu ryzyka

IMPLEMENTACJA PROCESU ZARZĄDZANIA RYZYKIEM ZA POMOCĄ RAM ZARZĄDZANIA RYZYKIEM ORGANIZACJI PECB

Podjęcie decyzji o wdrożeniu ram zarządzania ryzykiem opartych na ISO 31000 jest decyzją, którą podejmuje się bardzo łatwo, gdyż korzyści z tego płynące są bardzo dobrze udokumentowane. Poprzez stosowanie ustrukturyzowanej i efektywnej metodologii organizacja ma pewność, że realizuje wszystkie absolutnie niezbędne praktyki wymagane do wdrożenia systemu zarządzania ryzykiem.

Nie istnieje jeden prosty schemat wdrożenia standardu ISO 31000, który będzie skuteczny w przypadku każdej firmy, ale istnieje kilka uniwersalnych kroków, które umożliwią Państwu pogodzenie ze sobą wiele często sprzecznych ze sobą wymogów oraz pomogą przejść pozytywnie przez proces certyfikacyjny.

Organizacja PECB stworzyła ramy zarządzania ryzykiem. Ich oficjalna nazwa to Ramy Zarządzania Ryzykiem organizacji PECB, które oparte są na najlepszych i stosowanych praktykach.

TRENING ORAZ CERTYFIKACJA

Organizacja PECB stworzyła rekomendowany projekt szkoleniowej mapy drogowej oraz szereg systemów certyfikacyjnych dla osób sprawujących stanowiska kierownicze w organizacji, które chcą wykazać zgodność z ISO 31000. Mimo że celem standardu ISO 31000 nie jest wykorzystywanie go do certyfikowania organizacji, wiele z nich stosuje go, gdyż stanowi to dowód na to, że dane organizacje wypracowały standaryzowane procesy oparte na najlepszych praktykach. Certyfikowanie pracowników stanowi dowód posiadania przez nich kompetencji zawodowych oraz doświadczenia dzięki temu, że wcześniej uczestniczyły w przedmiotowych kursach oraz egzaminach.

Również służy to do zademonstrowania, że certyfikowany specjalista posiada zdefiniowane kompetencje w oparciu o najlepsze praktyki. Umożliwia to organizacjom przeprowadzenie świadomej selekcji pracowników bądź zakupu usług w oparciu o kompetencje wykazane w określonym kierunku certyfikacyjnym. Ponadto stanowi to zachętę dla danego specjalisty do ciągłego rozwoju swoich umiejętności oraz wiedzy, gdyż pełni rolę narzędzia dla pracodawców chcących zagwarantować sobie, że szkolenie i pozyskane wiadomości były skuteczne.

Kursy szkoleniowe organizacji PECB są oferowane na całym świecie przez sieć autoryzowane jednostki szkoleniowe i są dostępne w kilku językach. Tabela poniżej stanowi krótki opis oficjalnych kursów szkoleniowych organizacji PECB dotyczących zarządzania ryzykiem w oparciu o ISO 31000.

Nazwa szkolenia	Krótki opis	Kto powinien uczestniczyć?
Wprowadzenie do ISO 31000	• Wprowadzenie do pojęć związanych z zarządzeniem ryzykiem • Nie kończy się uzyskaniem certyfikatu	• Pracownicy chcący zrozumieć ISO 31000 oraz pozyskać większą wiedzę na temat procesów dot. zarządzania ryzykiem zgodnie z międzynarodowym standardem • Pracownicy zaangażowani w jakikolwiek etap programu zarządzania ryzykiem
Manager ds. ryzyka ISO 31000	• Zarządzanie implementacją oraz ramami zarządzania ryzykiem • Dwugodzinny egzamin	• Menedżerzy ds. ryzyka • Dyrektorzy procesów • Dyrektorzy finansowi • Menedżerzy ds. ryzyka biznesowego • Dyrektorzy działu Compliance • Menedżerzy projektów

WYBÓR ODPOWIEDNIEJ CERTYFIKACJI:

Certyfikat ISO 31000 jest certyfikatem zawodowym dla specjalistów chcących wyk azać swoje kompetencje do wdrażania, utrzymania oraz zarządzania programem zarządzania ryzykiem zgodnie z ISO 31000. Do uzyskania certyfikacji z wyższych poziomów wymagane jest doświadczenie zawodowe.