Projektowanie i wdrażanie systemów zarządzania bezpieczeństwem informacji zgodnie z ISO/IEC 27003 dokumentacja

dr inż. Bolesław Szomański
bolkosz@wit.edu.pl

Plan prezentacji

- Norma ISO/IEC 27003:2010
- Dokumenty wymagane przez ISO/IEC 27001
- Przykładowe procesy w SZBI

ISO/IEC 27003:2010

- Information technology --
- Security techniques –
- Information security management system
- implementation guidance

- Technika Informatyczna Techniki Bezpieczeństwa
- System Zarządzania Bezpieczeństwem Informacji
- Wytyczne do Wdrożenia

- Brak polskiego tłumaczenia

Spis treści ISO/IEC 27003:2010

Tło

- ISO/IEC 27003 został przygotowany przez
  - komitet techniczny ISO/TC JTC 1
  - Technika informatyczna
- Podkomitet SC27 Techniki Bezpieczeństwa

- I został zatwierdzony przez przynajmniej 75% komitetów członkowskich

Wprowadzenie

- Celem niniejszej normy międzynarodowej jest
  - dostarczenie praktycznych zaleceń
- dla opracowania planu wdrożenia
  - Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w organizacji
- zgodnie z ISO/IEC 27001:2005
- Proces opisywany w niniejszej normie
  - został zaprojektowany aby wspierać
  - wdrożenie ISO/IEC 27001:2005 (patrz części 4,5,7) i
  - aby udokumentować

Wprowadzenie

- A) przygotowanie rozpoczęcia planu wdrożenia SZBI
  - w organizacji poprzez zdefiniowanie struktury organizacyjnej
  - dla projektu i
  - uzyskanie akceptacji kierownictwa
- B) udokumentować krytyczne działania
  - dla projektu SZBI i
- C) przedstawić przykłady dla spełnienia wymagań ISO/IEC 27001:2005

Wprowadzenie

- Wykorzystując niniejszą normę międzynarodową
  - organizacja organizacja będzie mogła opracować
  - procesy dla zarządzania bezpieczeństwem,
  - dostarczając interesariuszom zapewnienie że
  - ryzyko dla aktywów informacyjnych jest
  - ciągle utrzymywane na
    - akceptowalnym poziomie bezpieczeństwa
    - zdefiniowanym przez organizację

Wprowadzenie

- Niniejsza norma międzynarodowa
  - nie obejmuje działalności operacyjnej i
    - innych działań SZBI, ale
  - zawiera koncepcję jak zaprojektować działania które
  - przyniosą wyniki po rozpoczęciu funkcjonowania SZBI.
- Wynikiem koncepcja jest
  - końcowy plan wdrożenia projektu.
- Wykonanie zależnej od organizacji
  - specyficznych części projektu SZBI jest
  - poza zakresem niniejszej normy międzynarodowej.
- Zaleca się żeby wdrożenie projektu SZBI było prowadzone
  - za pomocą standardowych metodologii projektowych

1. Zakres

- Niniejsza norma międzynarodowa koncentruje się
  - na krytycznych aspektach koniecznych dla
  - pomyślnego zaprojektowania i wdrożenia SZBI
  - zgodnie z ISO/IEC 27001:2005
- Opisuje ona proces określenia specyfikacji SZBI i
  - projektowania od koncepcji o otrzymania planu wdrożenia.
- Dokument rozpoczyna się od
  - procesu uzyskania akceptacji kierownictwa dla wdrożenia SZBI
  - zdefiniowania projektu wdrożenia SZBI
    - (określanego w niniejszej normie jako projekt SZBI),
  - poprzez dostarczenie zaleceń jak planować projekt SZBI,
  - kończąc na końcowym projekcie wdrożenia SZBI

Zakres

- Intencją tego dokumentu jest używanie go przez organizacje wdrażające SZBI.
- Nadaje się do wykorzystania dla
  - wszystkich typów organizacji
  - Biznesowych
  - Agencji rządowych
  - Nie-dochodowych
  - Każdej wielkości

Zakres

- Złożoność i ryzyko w każdej organizacji
  - są unikalne i te
  - specyficzne wymagania kieruje wdrożeniem SZBI
- Małe organizacje mogą stwierdzić
  - działania podane w niniejszej normie międzynarodowej
  - nadają się do zastosowania dla niech i
  - mogą je uprościć
- Duże lub złożone organizacje mogą uznać że
  - warstwa organizacja lub system zarządzania jest potrzebny do
    - zarządzania działaniami określonymi w niniejszej normie skutecznie.
- Jednakże w obu przypadkach użyteczne działania
  - mogą być planowane poprzez
  - wykorzystanie niniejszej normy międzynarodowej

Zakres

- Niniejsza norma międzynarodowa przyjmuje postać zaleceń
  - i nie określa żadnych wymagań.
- Intencją Niniejszej normy międzynarodowej
  - jest użycie wspólnie z ISO/IEC 27002:2005
    - i ISO/IEC 27002:2005, ale
    - nie ma intencji zmiany lub/i zmniejszania wymagań
    - określonych ISO/IEC 27001:2005 lub
    - wytycznych podawanych w IOS?IEC 27002:20005.
  - Twierdzenie o zgodności z
    - niniejszą normą międzynarodową
    - nie jest odpowiednie

Powołania normatywne

- ISO/IEC 27000:2009
- ISO/IEC 27001:2005

Terminy i definicje

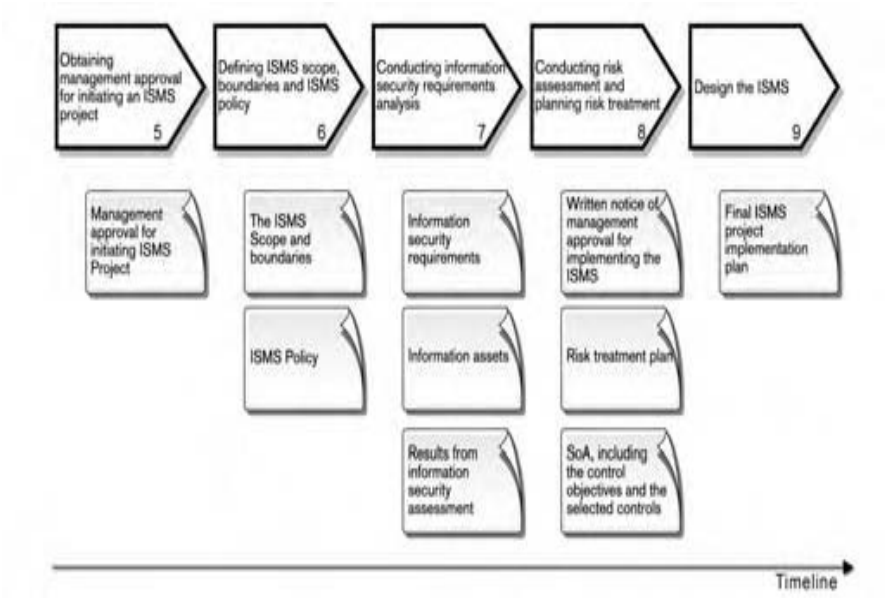
- 3.1 projekt SZBI
  - Wszystkie ustrukturalizowane działania
  - prowadzone przez organizację dla wdrożenia SZBI

4.1 Struktura niniejszej normy międzynarodowej

- 4.1 Podstawowa struktura rozdziałów
  - Wdrożenie SZBO jest ważną działalnością i
    - zwykle jest prowadzone jako projekt w organizacji
  - Niniejsza norma międzynarodowa objaśnia
    - wdrożenie SZBI poprzez
  - skoncentrowanie się na inicjatywie,
    - planowaniu i definiowaniu procesu
  - Proces planowania końcowego wdrożenia SZBI
    - zawiera pięć faz z których każda jest
    - przedstawiona w oddzielnym rozdziale
  - Wszystkie rozdziały mają zbliżoną strukturę jak opisano poniżej

4.

- Te pięć faz to
  - Uzyskanie akceptacji kierownictwa
    - dla rozpoczęcia projektu SZBI (5)
  - Definiowanie zakresu, granic i polityki SZBI (6)
  - Prowadzenie analizy
    - wymagań bezpieczeństwa informacji (7)
  - Prowadzenie oceny ryzyka i
    - planowanie postępowania z ryzykiem (8)
  - Projektowanie SZBI (9)



4.1

- Dodatkowe informacje są przedstawione w załącznikach
  - Podsumowanie działań z odsyłaczami do ISO/IEC 27001:2005
  - Role i odpowiedzialności w bezpieczeństwie informacji
  - Informacja o planowaniu audytów wewnętrznych
  - Struktura polityk
  - Informacja o planowaniu monitorowania i pomiaru

4.2 Podstawowa struktura rozdziału

- Każdy rozdział zawiera
  - Jeden lub wiele celów znajdujących się na
    - początku rozdziału
  - Jedno lub wiele działań niezbędnych do
    - osiągnięcia celu etapów lub celów
  - Każde działanie jest określone w podklasach
  - Działanie w każdej podklasie ma poniższą strukturę
- Działanie
  - Definiuje co jest potrzebne dla wykonania
    - działania lub części działań

4.2

- **Wejście**
  - **Wejście określa punkt startowy taki jak**
    - **istnienie udokumentowanych decyzji lub**
    - **wyjścia z innych działań opisanych**
      - w niniejszej normie międzynarodowej
  - **Wejście może być określana jako**
    - **kompletne wyjście z działania w związanym rozdziale lub**
    - **specyficzna informacja z działania**
      - dodanego poprzez powołanie rozdziału

4.2

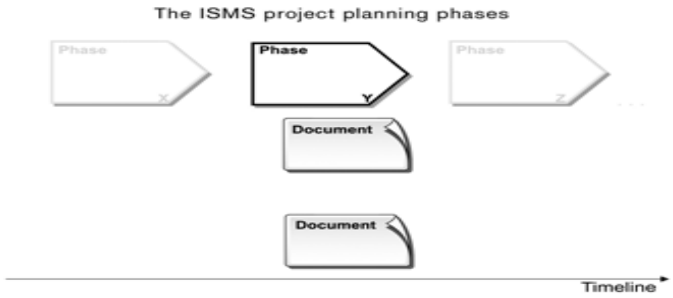
- **Zalecenie**
  - **Zalecenie podaje szczegółową informację jak wykonać te działanie.**
  - **Niektóre zalecenia mogą nie być odpowiednie**
  - **we wszystkich przypadkach**
    - **i inne sposoby osiągnięcia wyników mogą być właściwsze**

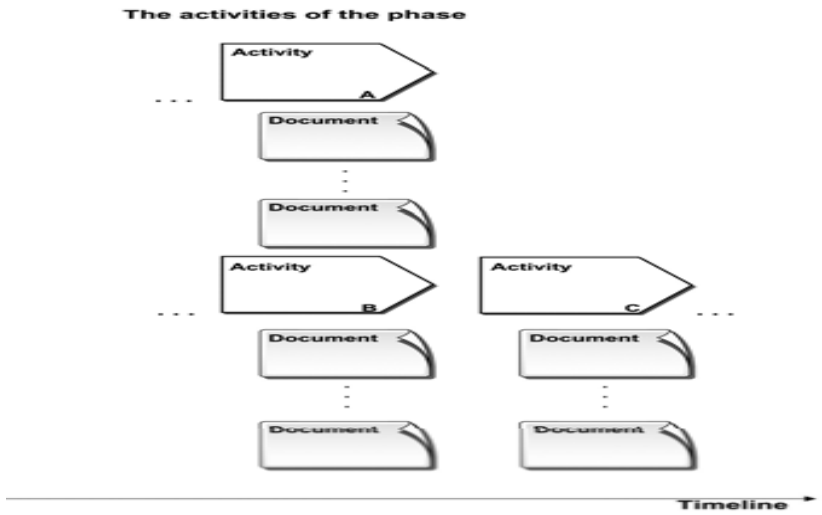
4.2

- **Wyjście**
  - **Wyjście określa wynik poprzez zakończenie działalności**
    - **lub dostarczenie wyniku**
    - **np. dokument**
  - **Wyjście jest takie same niezależnie od**
    - **wielkości organizacji lub zakresu SZBI**
- **Inne informacje**
  - **Inne informacje dostarczają dodatkową informacje,**
    - **która towarzyszy wykonywaniu działania**
    - **np. odwołania do innych norm**

4.3 Diagramy

- **Projekt jest często przedstawiony w**
  - **postaci graficznej lub diagramów jako pokazujący**
  - **działania i wyjścia**



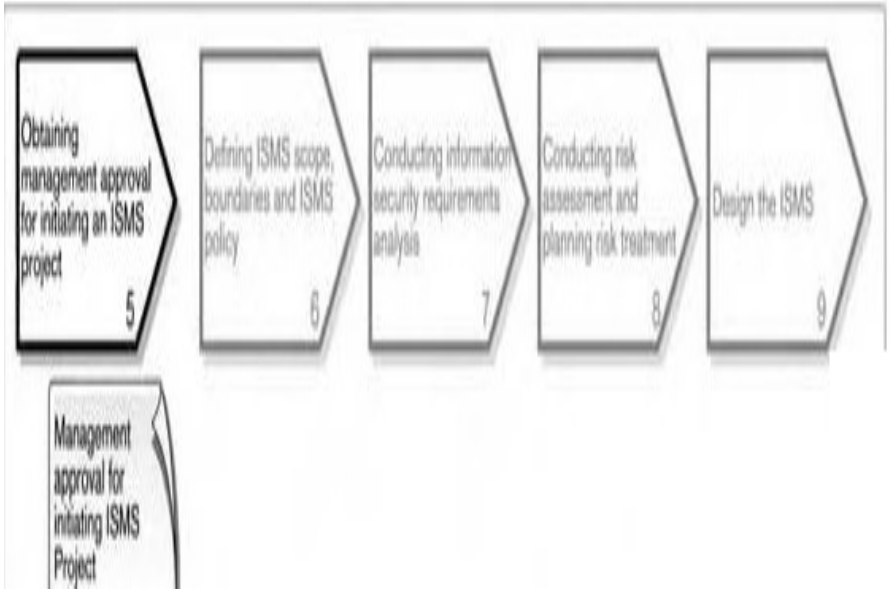


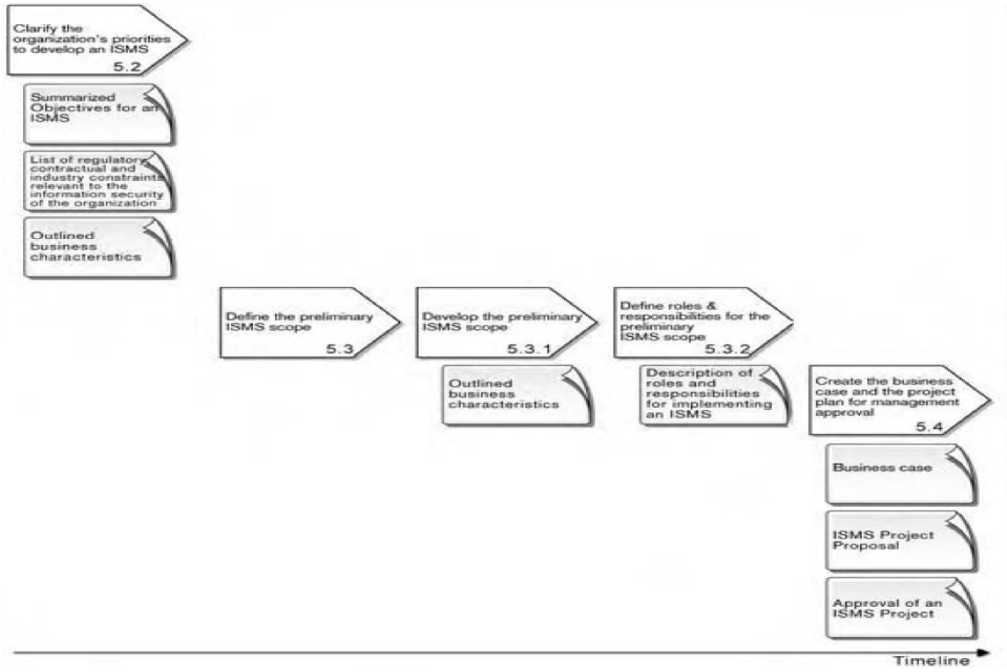
5. Uzyskanie akceptacji kierownictwa dla rozpoczęcia projektu SZBI

❑5.1. Przegląd akceptacji kierownictwa dla rozpoczęcia projektu SZBI

❑*Cel*

- *Uzyskanie akceptacji kierownictwa dla rozpoczęcia*
- *projektu SZBI przez*
- *określenie przypadku biznesowego i*
- *planu projektu*





5.2. Wyjaśnienie priorytetów organizacji dla opracowania SZBI

- **Działanie**
  - Zaleca się żeby Cele wdrożenia SZBI były włączone
  - poprzez spełniania priorytetów dotyczących
  - bezpieczeństwa informacji i wymagań
- **Wejście**
  - Cele strategiczne organizacji
  - Przegląd systemu zarządzania
  - Wykaz prawnych, regulacyjnych i kontraktowych wymagań dotyczących bezpieczeństwa informacji
  - mających zastosowanie dla organizacji

5.2

- **Wyjście**
  - Podsumowanie celów,
    - priorytetów bezpieczeństwa informacji i
    - wymagań dla SZBI
  - Wykaz regulacyjnych kontraktowych i branżowych
    - wymagań związanych z bezpieczeństwem informacji
  - Ogólna charakterystyka biznesu,
    - organizacji lokalizacji
    - aktywów i
    - technologii

5.3. Zdefiniowanie zakresu SZBI

- **5.3.1 Opracowanie wstępnego zakresu SZBI**
- **Działanie**
  - Zaleca się żeby cele wdrożenia SZBI zawierały
  - wstępną definicję zakresu, która jest
  - niezbędna dla projektu SZBI
- **Wejście**
  - Wyjście z 5.2
- **Wyjście**
  - Dokument zawierający wstępny zakres SZBI

5.3

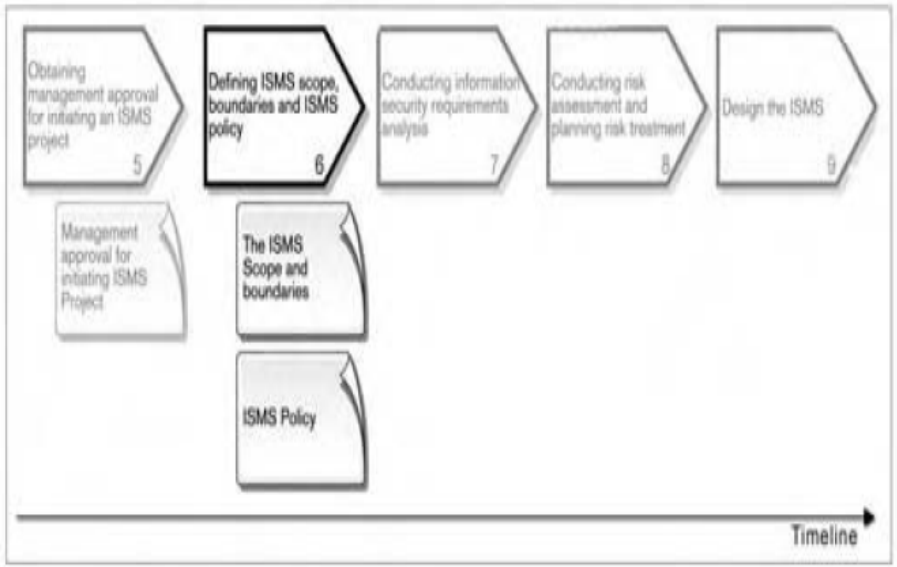
- **5.3.2. Zdefiniowanie ról i odpowiedzialności dla wstępnego zakresu SZBI**
- **Działanie**
  - Zaleca się aby Ogólne role i odpowiedzialności
    - dla wstępnego zakresu SZBI zostały zdefiniowane
- **Wejście**
  - Wyjście z 5.3.1
  - Wykaz interesariuszy którzy
    - uzyskają korzyści z wyników projektu SZBI
- **Wyjście**
  - Dokument lub tabela określająca role i odpowiedzialności
  - z nazwiskami i organizacją potrzebną dla udanego wdrożenia SZBI

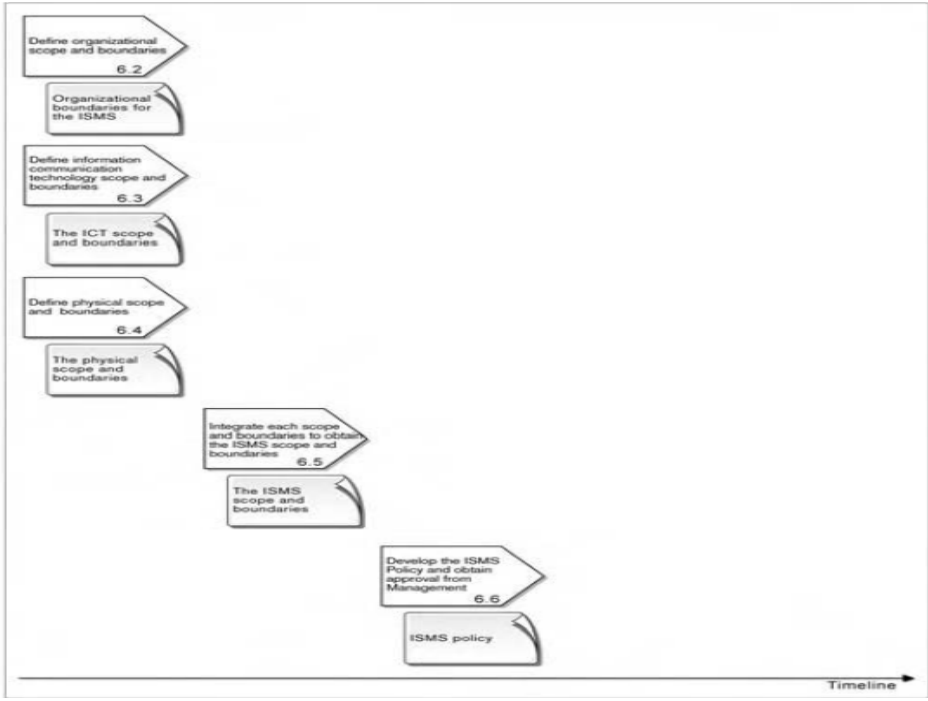
5.4 Utworzenie opisu biznesowego i projektu planu do zaakceptowania przez kierownictwo

- **Działanie**
  - **Zaleca się żeby aprobata kierownictwa i zapewnienie zasobów dla wdrożenia SZBI były uzyskane poprzez określenie opisu biznesowego i propozycji projektu SZBI**
  - **Wejście**
    - **Wyjście z 5.2.**
    - **Wyjście z 5.3**
      - Zakres SZBI
      - Związane role i odpowiedzialności
  - **Wyjście**
    - **udokumentowana akceptacja przez kierownictwo**
      - wykonywania projektu i przydzielonych zasobów
    - **Opis biznesowy**
    - **Wstępny projekt SZBI z kamieniami milowymi**
      - Takimi jak szacowanie ryzyka, wdrożenie, wewnętrzny audyt,
      - przegląd dokonywany przez kierownictwo

6. Definiowanie zakresu, granic i polityki SZBI

- **6.1. Przegląd definiowania zakresu, granic i polityki SZBI**
- **Cel**
  - **Określenie szczegółowego zakresu i granic SZBI**
  - **Oraz opracowanie polityki SZBI i**
  - **Uzyskanie poparcia od kierownictwa**



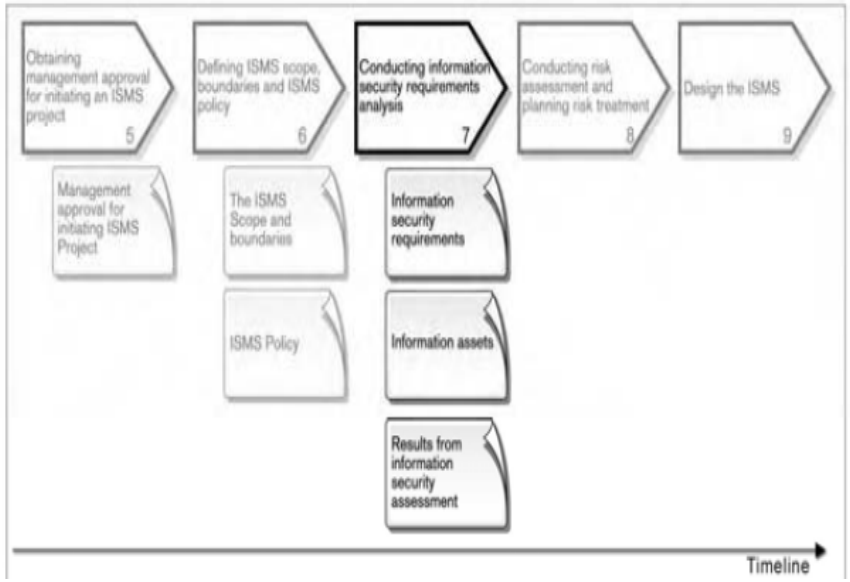


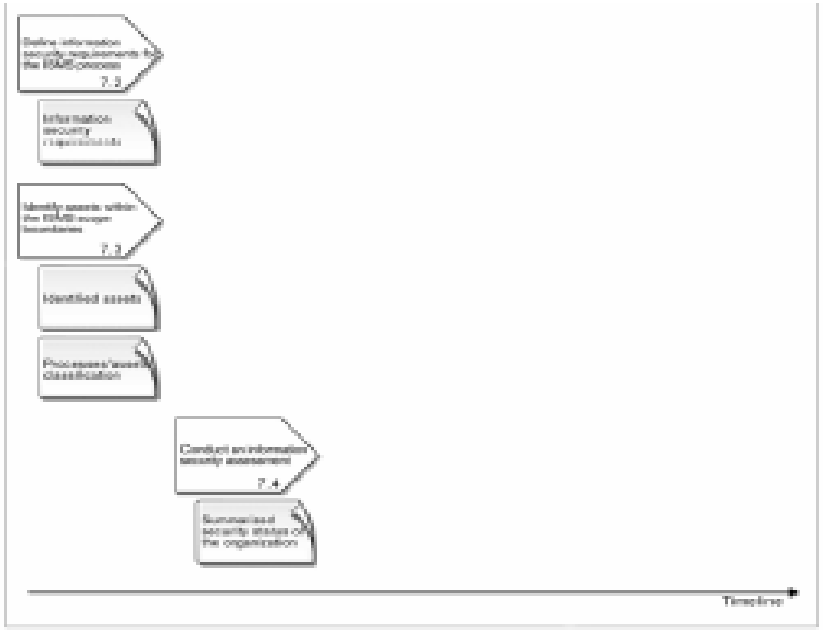
6

6.2 Definiowanie organizacyjnego zakresu i granic
6.3 Definiowanie teleinformatycznego zakresu i granic
6.4. Definiowanie fizycznego zakresu i granic
6.5. Integrowanie wszystkich zakresów i granic aby otrzymać zakres i granice SZBI
6.6. Opracowanie polityki SZBI i uzyskanie akceptacji przez kierownictwo

7. Prowadzenie analizy wymagań bezpieczeństwa informacji

- **7.1. Przegląd prowadzenia analizy wymagań bezpieczeństwa informacji**
- *Cel*
  - *Określenie związanych wymagań wspomaganych przez SZBI*
  - *Identyfikowanie aktywów informacyjnych*
  - *I uzyskanie bieżącego statusu bezpieczeństwa informacji w zakresie*





7

- **7.2 Definiowanie wymagań bezpieczeństwa dla procesów SZBI**
- **7.3. Identyfikowanie aktywów w zakresie SZBI**
- **7.4 Prowadzenie oceny bezpieczeństwa informacji**

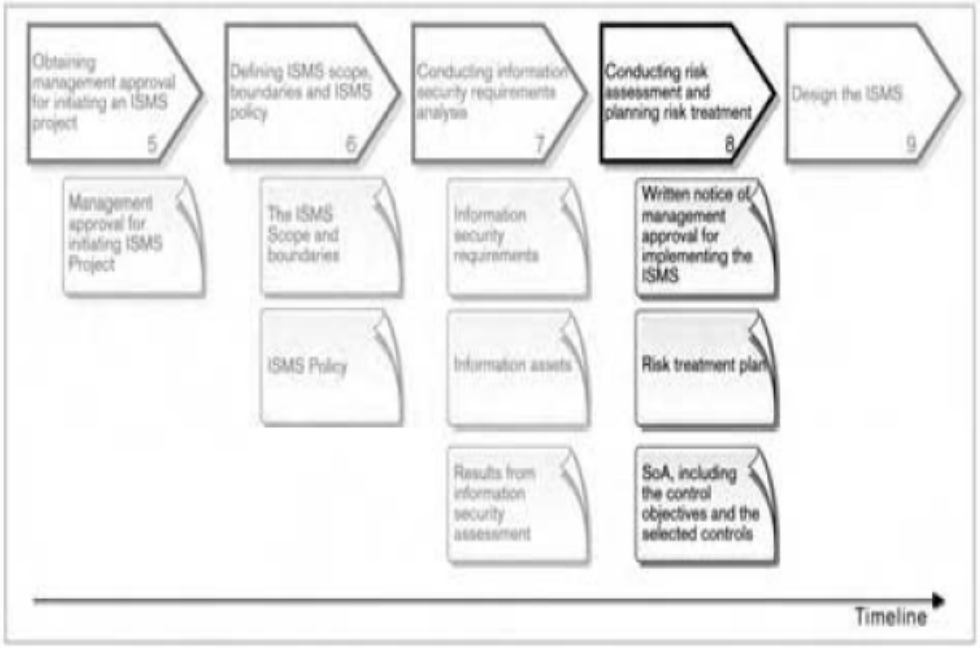
8. Prowadzenie oceny ryzyka i planowanie postępowania z ryzykiem

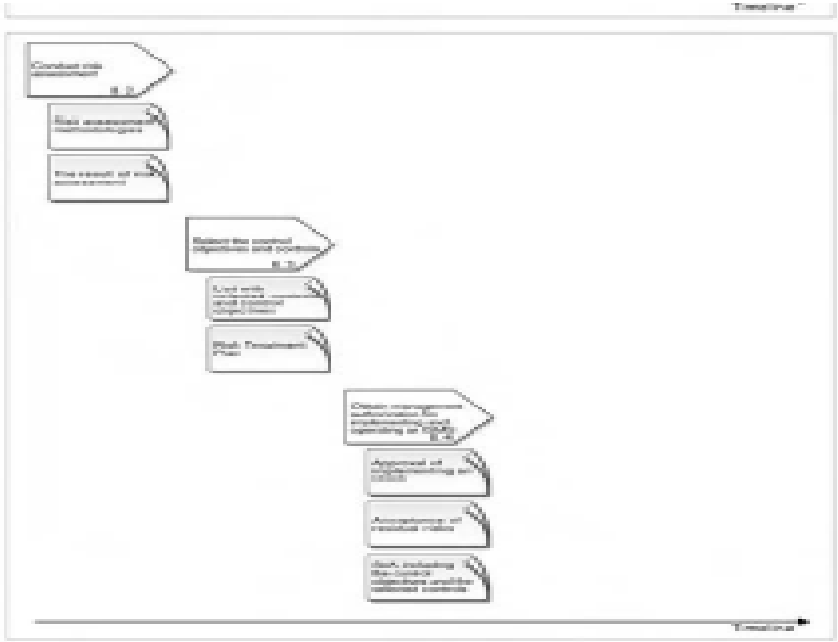
❑8.1. Przegląd prowadzenia oceny ryzyka i

- **planowania postępowania z ryzykiem**

❑*Cel*

- *Definiowanie metodyki*
  - o *postępowania z ryzykiem,*
  - o *identyfikowanie analizowanie i ocena ryzyk*
  - o *w bezpieczeństwa informacji*
  - o *dla wyboru opcji postępowania z ryzykiem i*
  - o *wyboru celów stosowania zabezpieczeń i zabezpieczeń*





8

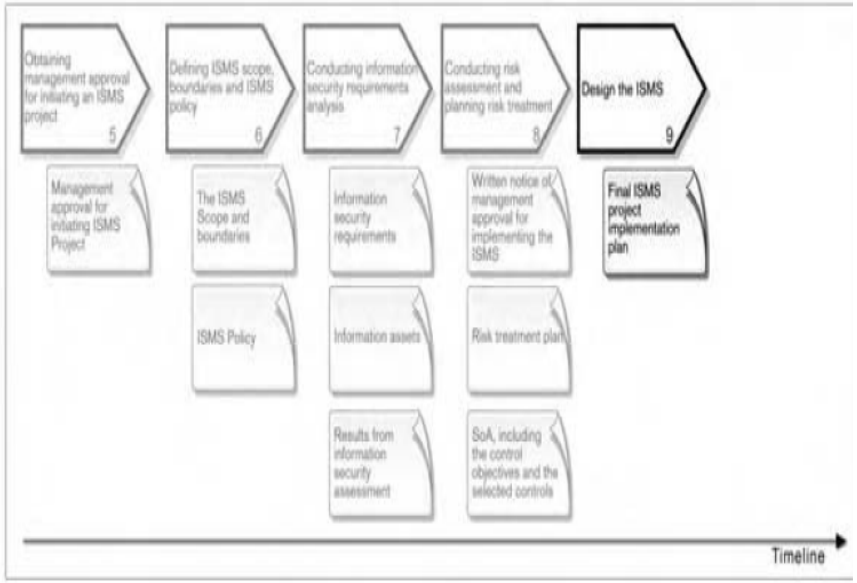
- **8.2 Prowadzenie oceny ryzyka**
- **8.3. Wybór celów zabezpieczeń i zabezpieczeń**
- **8.4 Uzyskanie autoryzacji kierownictwa**
  - **dla wdrożenia i eksploatacji SZBI**

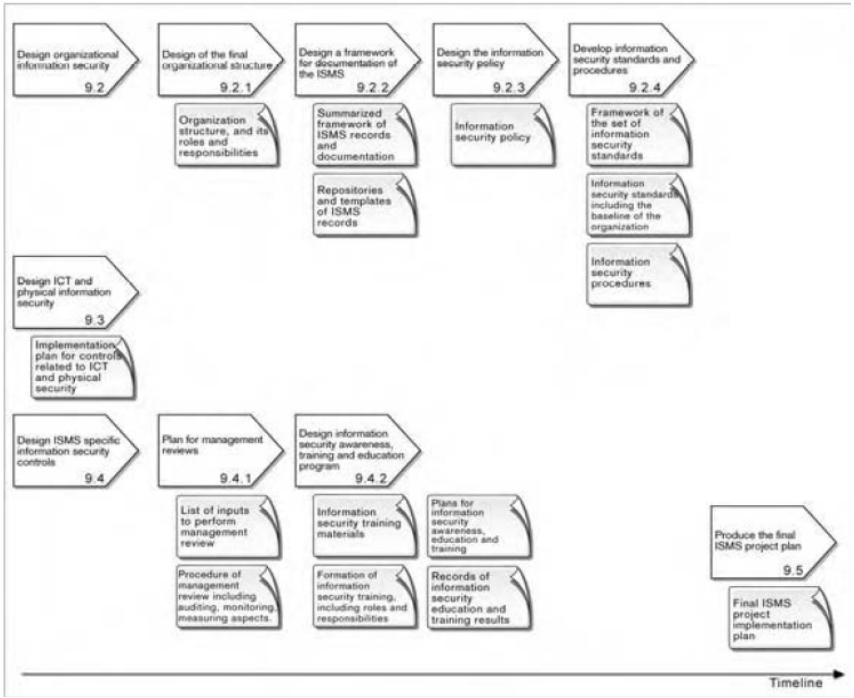
9. Projektowanie SZBI

❑9.1 Przegląd projektowania SZBI

❑*Cel*

- *Zakończenie planu wdrożenia SZBI poprzez*
  - *Zaprojektowanie bezpieczeństwa organizacyjnego*
  - *w oparciu o wybrane opcje postępowania z ryzykiem*
  - *Jak również wymagania dotyczące zapisów i dokumentacji*
  - *I zaprojektowanie zabezpieczeń integrujących*
  - *bezpieczeństwo teleinformatyczne, fizyczne i organizacyjne*
    - *procesy i*
  - *zaprojektowanie wymagań specyficznych dla SZBI*





9

- **9.2 Projektowanie organizacyjnego bezpieczeństwa informacji**
  - **9.2.1 Projektowanie ostatecznej struktury organizacyjnej**
    - dla bezpieczeństwa informacji
  - **9.2.2 Projektowanie struktury dla dokumentowania SZBI**
  - **9.2.3 Projektowanie polityki bezpieczeństwa informacji**
  - **9.2.4. Opracowanie standardów i procedur bezpieczeństwa informacji**
- **9.3 Projektowanie teleinformatycznego i**
  - **fizycznego bezpieczeństwa informacji**
- **9.4 Projektowanie szczegółów bezpieczeństwa informacji**
  - **9.4.1 Plan przeglądów dokonywanych przez kierownictwo**
  - **9.4.2 Projektowanie uświadamiania, szkolenia i nauczania**
- **9.5 Otrzymanie końcowego planu projektu SZBI**

Załączniki

- **A. Podsumowanie działań z**
  - **odsyłaczami do ISO/IEC 27001:2005**
- **B Role i odpowiedzialności w**
  - **bezpieczeństwie informacji**
- **C Informacja o planowaniu**
  - **audytów wewnętrznych**
- **D Struktura polityk**
- **E Informacja o planowaniu**
  - **monitorowania i pomiaru**

Jakie dokumenty są wymagane aby udokumentować spełnienie wymagań SZBI

- **Polityka bezpieczeństwa informacji**
- **Cele bezpieczeństwa informacji**
- **Metodyka postępowania z ryzykiem**
- **Raport z szacowania ryzyka**
- **Plan postępowania z ryzykiem**

Raport z analizy ryzyka

- **Organizacja powinna**
  - **Zidentyfikować ryzyko**
    - **zidentyfikować zasoby i ich właścicieli**
    - **Zidentyfikować zagrożenia dla tych zasobów**
    - **Zidentyfikować podatności zasobów**
    - **Zidentyfikować skutki utraty**
      - poufności,
      - integralności i
      - dostępności
  - **Ocenić ryzyko**
    - **Ocenić szkody dla biznesu wynikające z utraty bezpieczeństwa**
    - **Ocenić prawdopodobieństwo utraty bezpieczeństwa**
    - **Oszacować poziom ryzyka**
    - **Określić kiedy ryzyko jest akceptowane lub wymaga postępowania**

Cele bezpieczeństwa informacji

- Organizacja powinna sformułować cele, które
  - Dotyczą bezpieczeństwa informacji
  - Są związane z wymaganiami biznesu
  - Udokumentowane
- Realizacja celów powinna być sprawdzana

Plan postępowania z ryzykiem

- Plan postępowania z ryzykiem jest
  - uzgodnionym dokumentem
  - określający działania
  - w celu zmniejszenia
    - nie akceptowalnego ryzyka i
  - wdrożenia wymaganych zabezpieczeń
    - dla ochrony informacji

Jakie jeszcze dokumenty są wymagane aby udokumentować spełnienie wymagań SZBI

- Deklaracja stosowania
  - (jedna ale dotycząca 134 punktów)
- Polityki szczegółowe (około 10)
- Procedury wymagane w normie i załączniku A
  - (około 18)
- Zapisy wymagane przez normę

Deklaracja stosowania

- Deklaracja stosowania jest krytyczna dla celów
  - stosowania zabezpieczeń i zabezpieczeń, które
  - organizacja wybiera jako korzystne
  - dla spełnienia potrzeb biznesowych.
  - W deklaracji są także zapisane wykluczenia zabezpieczeń

  - Deklaracja stosowania jest dokumentem w którym
    - demonstrowane jest jak organizacja kontroluje ryzyko.
    - Nie powinna być ona zbyt szczegółowa, aby
      - nie przekazywać wrażliwych informacji osobom które
      - chcą przełamać zabezpieczenia
  - Deklaracja stosowania być używana przez
    - potencjalnych parterów handlowych,
    - jako samodzielny dokument lub
    - załącznik do certyfikatu używany przez organizację certyfikującą i
    - może być publicznie dostępna

Polityki

- W normie ISO 27001:2005 wymaga się oprócz
  - polityki bezpieczeństwa informacji
    - opracowanie wielu polityk
- Wynika to także z koncepcji PN 13335-1 w którym
  - zakładano kilku poziomową hierarchię polityk
- W dalszej części opracowania inne polityki
  - oprócz polityki bezpieczeństwa informacji będą
  - nazywane *politykami szczegółowymi*

Wymagane polityki szczegółowe

- *Polityka czystego biurka i czystego ekranu*
  - *(A.11.3.3)*
- *Polityki dla ochrony informacji związanej z*
  - *połączeniami pomiędzy biznesowymi*
    - *systemami informacyjnymi (A10.8.5)*
- *Polityka kontroli dostępu (A.11.1.1)*
- *Polityka przetwarzania i*
  - *komunikacji mobilnej [A.11.8.1]*
- *Polityka pracy na odległość [A.11.8.2]*

Wymagane polityki szczegółowe [3]

- Polityka korzystania *z usług sieciowych (A.11.4.1)*
- *Polityka używania zabezpieczeń kryptograficznych*
  - *(A.12.3.1)*
- *Polityka dostępu do aplikacji biznesowych [A.11.6.1]*

Udokumentowane procedury wymagane przez normę ISO 27001-:2005

- Procedura nadzoru nad dokumentacją [4.3.2]
- Procedura audytu wewnętrznego [6]
- Procedury działania korygującego [8.2]
- Procedury działań zapobiegawczych [8.3]
- Procedury natychmiastowego wykrycia i
  - reakcji na incydenty oraz
    - wykrywania błędów w wynikach przetwarzania [4.2.2g] [4.2.3a]:

Procedury

- Co z dokumentowaniem?
- Dokumentacja SZBI powinna zawierać
  - e) Udokumentowane procedury potrzebne organizacji do
    - zapewnienia efektywnego planowania, eksploatacji i
      - sterowania jej procesami bezpieczeństwa informacji
- A.8.1.1. Dokumentowanie procedur eksploatacyjnych
  - Procedury eksploatacyjne wskazane przez politykę bezpieczeństwa powinny być udokumentowane i utrzymywane
    - *Lepiej by było przez deklarację stosowania ale*
    - *polityka bezpieczeństwa informacji jest tutaj uznawana w pojęciu szerszym*
      - *(jak ISO 17799:2000)*
- Procedur z ISO 27001:2005 nie można wykluczyć
  - ale procedury wymagane przez załącznik A
  - Można wykluczyć
    - oczywiście w przypadku wykluczenia danego podpunktu załącznika A
    - i uzasadnienia tego wykluczenia

Wymagane procedury [1]

- Procedury oznaczania informacją i
  - postępowania z informacją [A.7.2.2]
- Procedury zarządzania incydentami
  - związanymi z bezpieczeństwem [A.13.1.2]
- Procedury uświadamiania użytkowników
  - o szkodliwym oprogramowaniu [A.10.4.1.]

Wymagane procedury [3]

- Procedury postępowania z informacją [A.10.7.3]
- Procedury dotyczące wymiany informacji
  - [A.10.8.1]
- Formalna procedura rejestrowania i
  - wyrejestrowania użytkowników [A 11.2.1].

Wymagane procedury [5]

- Procedury pracy na odległość [A11.7.2]
- Formalne procedury kontroli zmian [A12.5.1]
- Procedura zapewnianie zgodności z prawem
  - do własności intelektualnej [A.15.1.2.]

Procesy wymienione w załączniku A

- Proces autoryzacji nowych urządzeń
  - do przetwarzania informacji [A.6.1.4]
- Formalny proces zarządzania nadzorujący
  - przydzielanie haseł [A.11.2.3]
- Formalny proces przeglądu praw dostępu [A.11.2.4]
- Proces bezpiecznego rejestrowania [A.11.5.2]
- Proces zarządzania ciągłością działania=
  - plan zapewnienia ciągłości działania+procedury+
    - zapisy z testów+urządzenia+oprogramowanie [A.14]
- Proces audytu = procedura audytu+
  - planowanie audytu + ochrona narzędzi audytu[A.15.3]

Plany

- Plan postępowania z ryzykiem [4.2.2] (było)
- Plany zarządzania ciągłością działania [A14.1.2]

Zasady i metody

- Zasady gromadzenia
  - materiałów dowodowych [A.13.2.3]
- Metoda szacowania ryzyka [4.2.1c]
- Metoda audytów [6]

Plan wdrażania systemu zarządzania bezpieczeństwa informacji przy wdrożonym SZJ

- Szkolenie dla zespołu wdrażającego
  - Rozdanie ankiety samooceny
- Wstępna analiza stanu bezpieczeństwa informacji
  - oraz istniejącej dokumentacji np procedur (z ISO 9001),
    - zarządzeń, instrukcji (w tym instrukcji kancelaryjnej)
- Audyt wstępny zwłaszcza ochrony fizycznej i
  - infrastruktury informatycznej
- Szkolenie dla zespołu prowadzącego analizę ryzyka,
  - przygotowanie metodyki analizy ryzyka

Plan ...

- Szkolenie dla naczelnego kierownictwa wraz z uzgodnieniami
  - zatwierdzenie harmonogramu prac
  - Zatwierdzenie metodyki szacowania ryzyka
  - Określenie poziomu akceptowalnego ryzyka
- Przeprowadzenie analizy ryzyka
  - w tym uzupełnienie opisów procesów o identyfikację ryzyk
- Opracowanie polityki bezpieczeństwa informacji,
  - uzupełnienie mapy procesów, celów i miar ich skuteczności

Plan ....

- Przygotowanie wstępnej wersji deklaracji stosowania –
  - określenie procedur i zabezpieczeń koniecznych do wykonania
- Określenie ewentualnych wyłączeń
- Opracowanie lub dostosowanie dokumentów wymaganych
  - przez ISO 27001 (procedury zarządzania incydentami,
    - nadzoru nad dokumentami, audytu itp.)
- Opracowanie planu postępowania z ryzykiem
- Opracowanie polityk szczegółowych
  - (np. w postaci zarządzenia dyrekcji)

Plan ...

- Opracowanie procedur „eksploatacyjnych”
  - (wymaganych przez załącznik A)
- Wdrożenie zabezpieczeń wynikających
  - z analizy ryzyka i załącznika A
- Przygotowanie ostatecznej wersji deklaracji stosowania
- Przeprowadzenie audytów wewnętrznych
- Przeprowadzenie przeglądu kierownictwa
- Funkcjonowanie systemu (3-6 miesięcy)
- Audyt certyfikacyjny (wstępny i właściwy)
- Powtórna analiza ryzyka i doskonalenie SZBI

Przykłady dodatkowych procesów w zintegrowanym systemie zarządzania(1)

- Eksploatacja systemu
- zarządzania bezpieczeństwa informacji
  - Monitorowanie bezpieczeństwa informacji
  - Planowanie i przeprowadzanie przeglądów i audytów bezpieczeństwa informacji
  - Działania korygujące i zapobiegawcze w zakresie SZBI
  - Doskonalenie SZBI
  - Nadzór nad dokumentacją i zapisami dotyczącymi SZBI

Przykłady dodatkowych procesów w zintegrowanym systemie zarządzania(2)

- Proces Zarządzanie ciągłością działania
  - Analiza zagrożeń dla ciągłości działania
  - Opracowanie planu ciągłości działania
  - Testowanie planu ciągłości działania
  - Doskonalenie planu ciągłości działania
  - Zastosowanie planu ciągłości działania
  - Przywracanie stanu wyjściowego

Przykłady dodatkowych procesów w zintegrowanym systemie zarządzania(3)

- Proces Zarządzania ryzykiem
  - Tworzenie i weryfikacja metodyki
  - Analiza ryzyka
    - Określenie aktywów
    - Określenie zagrożeń
    - Określenie podatności
    - Oszacowanie prawdopodobieństw
    - Określenie skutków
    - Uwzględnienie zabezpieczeń
    - Oszacowanie ryzyk
  - Postępowanie z ryzykami
  - Ocena wpływu zmian w otoczeniu na zagrożenia, podatności i ryzyka
  - Doskonalenie

Przykłady dodatkowych procesów w zintegrowanym systemie zarządzania(4)

- Proces Zarządzanie incydentami
  - Utworzenie struktury dla zarządzania incydentami
  - Budowa narzędzi do rejestracji incydentów
    - Np. Help desk
  - Opracowanie procedur reakcji na incydenty
  - Reagowanie na incydenty
  - Wyciąganie wniosków z incydentów
  - Doskonalenie
- Można połączyć z procedurą postępowanie
  - z wyrobem niezgodnym i odpowiednimi
  - procedurami bhp i środowiskowymi
- Patrz też ISO/IEC TR 18044

Przykłady dodatkowych procesów w zintegrowanym systemie zarządzania(5)

- Proces Ochrona Fizyczna
  - Planowanie ochrony fizycznej
    - I przygotowanie odpowiednich procedur
  - Monitorowanie ochrony fizycznej
    - I firmy realizującej ochronę fizyczną
    - Okresowo kontrola lub audyt
  - Reagowanie na incydenty z zakresu ochrony fizycznej
  - Doskonalenie ochrony fizycznej