Projektowanie i wdrażanie systemów zarządzania bezpieczeństwem informacji zgodnie z ISO/IEC 27001

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

Plan prezentacji

- **Norma ISO/IEC 27001**
- **Budowa polityki bezpieczeństwa - *ćwiczenie***
- **Przykładowy plan wdrożenia ISO/IEC 27001**

ISO/IEC 27001:2005 opublikowana 15.10.2005

- ISO/IEC 27001:2005
  Information Security Management System (ISMS) requirements
- **Następca normy BS 7799-2:2002, która obowiązywała do lipca 2007**
- **Polskie wydanie**
  - **PN ISO/IEC 27001:2007**
  - **Techniki Informacyjne Techniki Bezpieczeństwa**
  - **Systemy Zarządzania Bezpieczeństwem Informacji**

ISO/IEC 27001:2005 budowa

0. wprowadzenie
1. Zakres normy
2. Powołania
3. Terminologia i definicje
4. **System zarządzania bezpieczeństwem informacji**
5. **Odpowiedzialność kierownictwa**
6. **Wewnętrzny audyt SZBI (w BS 7799-2 pkt 6.4)**
7. **Przegląd dokonywany przez kierownictwo**
8. **Doskonalenie SZBI**

Zał. A. Cele stosowania zabezpieczeń i zabezpieczenia już wywodzące się z normy ISO 17799:2005

Zał. B. Zasady OECD w normie (zamiast wytycznych wprowadzania w BS 7799-2)

Zał. C. Korespondencja z ISO 9001:2000 i ISO 14001:2004

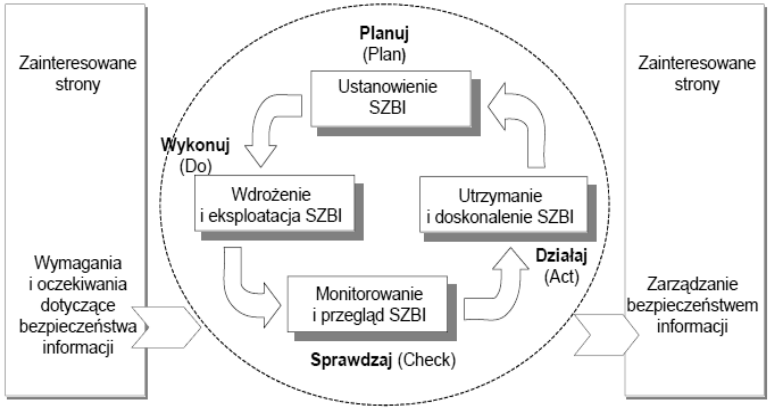
Zakres normy

- **Wymagania zawarte w tej normie są podstawowe i nadają się do zastosowania**
  - **we wszystkich typach organizacji**
  - **niezależnie od ich typu, wielkości i rodzaju**
- **Jakiekolwiek wykluczenie wymagań z punktów 4-8 jest niedopuszczalne**
  - **jeżeli organizacji chce zapewnić zgodność z normą ISO/IEC 27001**

1. Zakres normy (2)

- **Wykluczenie zabezpieczeń z załącznika A**
  - **musi być uzasadnione,**
  - **oparte o wyniki analizy ryzyka i**
  - **zaakceptowane przez odpowiedzialne osoby.**
- **Jeżeli jakieś zabezpieczenie jest wykluczone**
  - **potwierdzenie zgodności z normą jest możliwe jeżeli**
  - **nie wpływa to na zdolność i odpowiedzialność organizacji do**
  - **zapewnienia bezpieczeństwa informacji**
  - **spełniającego wymagania bezpieczeństwa**
    - o **wynikające z analizy ryzyka i**
    - o **przestrzegania przepisów prawnych i regulacyjnych**

Ciągłe doskonalenie



Ciągłe doskonalenie cd.

Planuj (ustanowienie SZBI)

Ustanowienie polityki SZBI celów procesów i procedur istotnych dla zarządzania ryzykiem oraz doskonalenia bezpieczeństwa informacji tak aby uzyskać wyniki zgodne z ogólnymi politykami i celami organizacji.

Wykonuj (wdrożenie i eksploatacja SZBI)

Wdrożenie i eksploatacja polityki SZBI, zabezpieczeń, procesów i procedur)

Sprawdź (monitorowanie i przegląd SZBI)

sprawdzaj a gdzie to możliwe mierz wydajność procesów w stosunku do polityki bezpieczeństwa, celów i doświadczeń praktycznych oraz raportuj wyniki zarządowi w celu dokonywania przeglądu

Popraw (utrzymywanie i doskonalenie SZBI)

wprowadzaj działania korygujące i zapobiegawcze w oparciu o wyniki audytów wewnętrznych i przeglądów kierownictwa oraz innych związanych informacji aby ciągle doskonalić SZBI.

3. Definicje [2]

- System zarządzania bezpieczeństwem informacji
  - SZBI
  - **ta część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji**
  - ***UWAGA system zarządzania obejmuje strukturę organizacyjną, polityki, zaplanowane działania, zakresy odpowiedzialności, praktyki, procedury, procesy i zasoby*.**
    - **information security management system (ISMS)**

3. Definicje [5]

- **deklaracja stosowania** (SoA)
  - **dokument, w którym opisano cele zabezpieczania oraz zabezpieczenia, które odnoszą się i mają zastosowanie w SZBI danej organizacji,**
  - **Uwaga**
    - **Cele stosowania zabezpieczeń i zabezpieczenia oparte są o rezultaty i wnioski wynikające z procesów szacowania i postępowania z ryzykiem, wymagań prawnych lub wymagań nadzoru, zobowiązań kontraktowych, wymagań biznesowych organizacji w odniesieniu do bezpieczeństwa informacji**
    - **statement of applicability**

4. System Zarządzania Bezpieczeństwem Informacji (SZBI) [1]

4.1. Wymagania podstawowe

- **Organizacja powinna**
  - **Ustanowić**
  - **Wdrożyć**
  - **Eksploatować**
  - **Monitorować**
  - **Przeglądać**
  - **Utrzymywać**
  - **Ciągle doskonalić**
- ***Udokumentowany* SZBI**
  - W kontekście
  - **Działalności biznesowej**
  - **Ryzyka**
- **Zastosowany proces opiera się na modelu PDCA**

4. SZBI [2]

4.2. Ustanowienie i zarządzanie SZBI

4.2.1. Ustanowienie SZBI

- **Organizacja powinna określić zakres i granice SZBI uwzględniając charakterystyki:**
  - **Prowadzonej działalności**
  - **Organizacji**
  - **Lokalizacji**
  - **Aktywów**
  - **Technologii**
  - **Zawierający**
    - Dokładny opis i decyzję dla każdego wyłączenia z zakresu

4. SZBI [3]

- **Określić politykę SZBI, uwzględniającą charakter prowadzonej działalności, organizacji, jej lokalizacji, aktywów i technologii która:**
  - **Zawiera ramy ustalania celów, oraz**
    - wyznacza ogólny kierunek i
    - zasady działania dotyczące bezpieczeństwa informacji
  - **Bierze pod uwagę**
    - wymagania biznesowe,
    - prawne i
    - Charakterze regulacyjnym
    - oraz kontraktowe
    - dotyczące bezpieczeństwa informacji
  - **Ustanawia**
    - kontekst strategiczny
    - związany z zarządzaniem ryzykiem
      - *dający obszar*
    - ustanowienia i
    - utrzymania SZBI
  - **Określa kryteria oceny ryzyka i strukturę oceny ryzyka**
  - ***Została zaakceptowana przez kierownictwo***
    - *Uwaga polityka SZBI może być zestawem wszystkich polityk bezpieczeństwa, może być w jednym dokumencie*

4. SZBI [4]

- **Określić podejście do szacowania ryzyka**
  - **Wskazać Metodykę szacowania ryzyka**
    - odpowiednią dla SZBI
    - Identyfikującą wymagania
      - *Biznesowe bezpieczeństwa informacji*
      - *Prawne i regulacyjne*
  - **Wyznaczyć kryteria akceptowania ryzyka**
    - *i*
    - Zidentyfikować akceptowalne poziomy ryzyka
  - **Wybrana metoda szacowania ryzyka powinna zapewnić, że szacowanie to daje porównywalne i powtarzalne rezultaty**
    - Uwaga istnieją różne metody szacowania ryzyka przykłady ISO 13335-3
  - ***Uwaga ISO 13335-3 został uchylona obecnie ISO/IEC 27005***

4. SZBI [5]

- **Określić ryzyko**
  - **Określić aktywa w zakresie SZBI i ich właścicieli**
  - **Określić zagrożenia dla tych aktywów**
  - **Określić podatności, które mogą być wykorzystane przez zagrożenia**
  - **Określić skutki utraty poufności, integralności i dostępności w odniesieniu do aktywów**
- **Analizować i ocenić ryzyko**
  - **Oszacować szkody i straty dla biznesu wynikające z naruszenia bezpieczeństwa, biorąc pod uwagę konsekwencje utraty: poufności integralności i dostępności aktywów**
  - **Oszacować realne prawdopodobieństwo naruszenia bezpieczeństwa w świetle istotnych zagrożeń i podatności oraz konsekwencji związanych z tymi aktywami oraz aktualnie wdrożonymi zabezpieczeniami**
  - **Wyznaczyć poziomy ryzyka**
  - **Stwierdzić kiedy ryzyko jest akceptowane lub wymaga odpowiedniego postępowania**
    - Opierając się na
    - Kryteriach zaakceptowania ryzyka

4. SZBI [6]

- **Zidentyfikować i określić warianty dla postępowania z ryzykiem.**
  - **Możliwe działania obejmują**
    - Zastosowanie odpowiednich zabezpieczeń
    - Zaakceptowanie ryzyka w sposób świadomy i obiektywny,
      - *przy założeniu że jasno spełniają warunki wyznaczone w polityce organizacji oraz kryteria akceptacji ryzyk*
    - Unikanie ryzyk
    - Przeniesienie ryzyka do innych organizacji
      - *Np. ubezpieczycieli, dostawców*

4. SZBI [6]

- **Wybrać cele stosowania zabezpieczania i zabezpieczenia.**
  - **Spełniające wymagania określone przez**
    - szacowanie ryzyka i
    - postępowanie z ryzykiem
  - **Biorąc pod uwagę**
    - kryteria akceptowania ryzyka oraz
    - Wymagania prawne, nadzoru i kontraktowe
  - **Cele zabezpieczenia i zabezpieczenia z załącznika A powinny być wybrane jako część tego procesu by w odpowiedni sposób spełnić zidentyfikowane wymagania**
  - **Lista celów stosowania zabezpieczeń i zabezpieczeń w załączniku A nie jest wyczerpująca,**
  - **mogą więc być wybrane dodatkowe cele stosowania zabezpieczeń i zabezpieczenia**
    - Uwaga załącznik A zawiera obszerny spis celów zabezpieczania i zabezpieczeń znajdujących powszechne zastosowanie.
    - Użytkownicy powinni traktować załącznik jako punkt wyjścia do wyboru zabezpieczeń, aby upewnić się że żadna istotna opcja zabezpieczeń nie zostanie przeoczona

4. SZBI [6a]

- ***Uzyskać akceptację kierownictwa dla ryzyk szczątkowych***
- ***Uzyskać autoryzację kierownictwa dla wdrożenia i eksploatacji SZBI***
- **Przygotować deklarację stosowania (SoA)**
  - **Deklaracja powinna zawierać**
    - Cele zabezpieczenia i zabezpieczenia wybrane oraz uzasadnienie ich wyboru
    - Cele zabezpieczenia i zabezpieczenie już wdrożone
    - Wykluczenie jakiegokolwiek celu zabezpieczenia i wykluczenia zabezpieczeń zawartych w załączniku A i wraz z uzasadnieniem wykluczenia
      - *Uwaga deklaracja stosowania dostarcza podsumowania dotyczącego postępowania z ryzykiem. Uzasadnienie wyłączeń umożliwia powtórne sprawdzenie, że żadne zabezpieczenie nie zostało nieumyślnie pominięte*

4. SZBI [7]

❑ 4.2.2. Wdrożenie i eksploatacja SZBI

- **Organizacja powinna**
  - **Sformułować plan postępowania z ryzykiem**
    - Określający określone działania zarządu, zasoby, odpowiedzialności i priorytety dla zarządzania ryzykami związanymi z bezpieczeństwem informacji
  - **Wdrożyć plan postępowania z ryzykiem**
    - w celu spełnienia celów stosowania zabezpieczeń w tym uzasadnienie poniesionych środków, role i odpowiedzialności
  - **Wdrożyć zabezpieczenia tak aby osiągnąć cele stosowania zabezpieczeń**
  - ***Zdefiniować jak mierzyć skuteczność wybranych zabezpieczeń***
    - *Oraz jak te pomiary będą wykorzystane w ocenie skuteczności zabezpieczeń do uzyskiwania porównywalnych i powtarzalnych wyników*
      - Uwaga pomiar skuteczności zabezpieczeń umożliwia kierownictwu i personelowi określić jak dobrze zabezpieczenia spełniają zaplanowane cele zabezpieczeń
  - **Wdrożyć programy szkolenia i uświadamiania**

4. SZBI [7a]

- **Zarządzać eksploatacją SZBI**
- **Zarządzać zasobami SZBI**
- **Wdrożyć procedury i inne działania**
  - w celu natychmiastowego
    - *Wykrycia zdarzeń*
    - *Reakcji na incydenty*

4. SZBI [8]

❑4.2.3. Monitorowanie i przegląd SZBI

- **Organizacja powinna podjąć następujące działania**
  - **Wykonywać *monitorowanie i przegląd procedur* i inne zabezpieczenia w celu:**
    - Natychmiastowego wykrywania błędów w wynikach przetwarzania
    - Natychmiastowego identyfikowania naruszenia bezpieczeństwa oraz incydentów zakończonych niepowodzeniem lub sukcesem
    - Umożliwienia kierownictwu określenia czy działania delegowane na poszczególne osoby lub wdrożone za pomocą środków informatycznych są wykonywane w zgodnie z oczekiwaniami
    - Pomocy w wykrywaniu naruszeń bezpieczeństwa tym samym niedopuszczenie do incydentów bezpieczeństwa przez użycie indykatorów
    - Określania czy działania podjętych w celu rozwiązania problemów związanych z naruszeniem bezpieczeństwa były skuteczne

4. SZBI [8a]

- **Dokonywać regularnych przeglądów skuteczności SZBI w tym:**
  - Zgodności z polityką i celami bezpieczeństwa oraz
  - Przeglądy zabezpieczeń
    - *biorąc pod uwagę*
  - Wyniki Audytów bezpieczeństwa
  - Incydentów
  - Rezultaty pomiaru skuteczności
  - Sugestie oraz
  - Informacje zwrotne
    - *od wszystkich zainteresowanych stron*
- *Dokonywać pomiarów skuteczności zabezpieczeń*
  - *w celu zweryfikowania że*
  - *wymagania bezpieczeństwa są spełnione*

4. SZBI [9]

- **Dokonywać przeglądu szacowania ryzyka w zaplanowanych odstępach czasu, przeglądu ryzyka szczątkowego oraz przeglądu poziomu ryzyka akceptowalnego biorąc pod uwagę zmiany**
  - Organizacji
  - Technologii
  - Celów i procesów biznesowe
  - Zidentyfikowanych zagrożeń
  - Skuteczność stosowanych zabezpieczeń
  - Zdarzeń zewnętrznych (zmiany przepisów prawnych lub regulacyjnych, zmiany wymagań kontraktowych i zmian w klimacie społecznym)
- **Przeprowadzać wewnętrzne audyty w regularnych odstępach czasu**
  - Uwaga Audyty wewnętrzne czasami zwane audytami pierwszej strony są przeprowadzane przez lub w imieniu organizacji na potrzeby wewnętrzne
- **W regularnych odstępach czasu podejmować przeglądy SZBI tak aby zapewnić że zakres jest odpowiedni oraz doskonalenie w procesach SZBI jest zidentyfikowane**
- *Uaktualniać plany bezpieczeństwa biorąc pod uwagę wyniki*
  - *monitoringu i*
  - *przeglądów*
- **Rejestrować działania i zdarzenia mające wpływ na skuteczność i wydajność SZBI**

4. SZBI [10]

❑4.2.4. Utrzymanie i doskonalenie SZBI

- **Organizacja powinna regularnie**
  - **Wdrażać zidentyfikowane udoskonalenia do SZBI**
  - **Podejmować odpowiednie działania korygujące i zapobiegawcze**
    - Wyciągać wnioski z doświadczeń w dziedzinie bezpieczeństwa zarówno organizacji innych jak i własnych
  - **Informować wszystkie zainteresowane strony o działaniach i udoskonaleniach na odpowiednim do okoliczności poziomie szczegółowości oraz jeżeli trzeba uzgodnić sposób dalszego postępowania**
  - **Upewnić się że**
    - zastosowane udoskonalenia
    - spełniają postawione cele

4. SZBI [11]

4.3 Wymagania dotyczące dokumentacji

❑ 4.3.1 Założenia

- *Dokumentacja powinna zawierać*
  - *zapisy decyzji zarządu*
    - *zapewniające że działania są*
    - *odpowiednie do decyzji zarządu i*
    - *polityk oraz*
    - *zapewnienie że zapisane wyniki są odtwarzalne*
  - **Ważnym jest aby można był wskazać powiązania pomiędzy wybranymi zabezpieczeniami i dotyczącymi ich rezultatami szacowania ryzyka i procesu postępowania z ryzykiem, a następnie z odpowiednimi politykami i celami SZBI**
- **Dokumentacja SZBI powinna obejmować**
  - **Udokumentowaną politykę bezpieczeństwa oraz**
    - celów stosowania zabezpieczeń
  - **Zakres SZBI**
  - **procedury i zabezpieczenia służące realizacji SZBI**

4. SZBI [12]

- ***Opis metodologii szacowania ryzyka***
- **Raport z szacowania ryzyka**
- **Plan postępowania z ryzykiem**
- **Udokumentowane procedury potrzebne organizacji aby efektywnie**
  - Planować
  - Wykonywać
  - Sterować
    - *procesami bezpieczeństwa informacji*
    - *Oraz*
  - ***Określenie jak mierzyć skuteczność zabezpieczeń***
- **Zapisy wymagane przez normę**
- **Deklarację stosowania**

4. SZBI [12a]

- **Uwaga**
  - Tam gdzie w niniejszej normie pojawia się termin udokumentowana procedura, oznacza to że procedura jest zdefiniowana, udokumentowana, wdrożona i utrzymywana
  - Zakres dokumentacji SZBI może być odmienny dla różnych organizacji z uwagi na
    - *Wielkość i rodzaj działalności*
    - *Zakres i złożoność wymagań bezpieczeństwa oraz zarządzanego systemu*
  - Dokumenty i zapisy mogą przybrać dowolną formę lub być przechowywane na dowolnym typie nośnika

4. SZBI (13)

❑ 4.3.2. Nadzór nad dokumentami

- **Dokumenty wymagane przez SZBI powinny być chronione i nadzorowane**
- **Udokumentowana procedura powinna być ustanowiona w celu:**
  - **zatwierdzania dokumentów przed ich wydaniem,**
  - **przeglądu i aktualizacji dokumentów w razie potrzeby oraz ponownego zatwierdzania.**
  - **zapewnienia, że zidentyfikowano zmiany i aktualny status zmian dokumentów,**
  - **zapewnienia, że najnowsze wersje odpowiednich dokumentów są dostępne w miejscach ich użytkowania,**

4. SZBI(14)

- **zapewnienia, że dokumenty pozostają**
  - czytelne i
  - łatwe do zidentyfikowania,
- *Zapewnienia że dokumenty są*
  - *dostępne dla osób które ich potrzebują i są*
  - *przesyłane,*
  - *przechowywane i*
  - *ostatecznie usuwane zgodnie*
  - *z procedurami zgodnymi z ich*
  - *klasyfikacją*
- **zapewnienia, że**
  - dokumenty pochodzące z zewnątrz są
  - zidentyfikowane
- **zapewnienia,że**
  - rozpowszechnianie dokumentów jest
  - nadzorowane
- **zapobiegania**
  - niezamierzonemu stosowaniu
  - nieaktualnych dokumentów
- **zastosowanie odpowiedniej ich identyfikacji,**
  - jeżeli są zachowane z jakichkolwiek powodów.

SZBI (15)

4.3.2. Nadzór nad zapisami

- **W celu dostarczenia świadectwa potwierdzającego zgodność z wymaganiami oraz skutecznej eksploatacji SZBI powinny być ustanowione i utrzymywane zapisy.**
  - **Zapisy powinny być chronione i nadzorowane**
  - **SZBI powinien uwzględniać wszystkie odnośne wymagania prawna, wymagania nadzoru i kontraktowe**
  - **Zapisy powinny być zawsze**
    - czytelne,
    - łatwe do zidentyfikowania i
    - odtwarzalne

4. SZBI (16)

- **Należy udokumentować i wdrożyć zabezpieczenia służące do**
  - identyfikowania,
  - przechowywania,
  - ochrony,
  - odtwarzaniu
  - archiwizacji
  - czasu przechowywania
  - Niszczenia
    - *zapisów*
- **Zapisy powinny dotyczyć realizacji procesów zgodnie z opisem zawartym w 4.2 oraz wszystkich incydentów związanych bezpieczeństwem w odniesieniu do SZBI**
  - Przykłady
    - *Lista gości,*
    - *Raporty z audytów,*
    - *Autoryzacja dostępu*

5. Odpowiedzialność kierownictwa (1)

5.1. Zaangażowanie kierownictwa

- **Kierownictwo powinno przedstawić świadectwo zaangażowania w ustanowienie, eksploatację, monitorowanie, przeglądy, utrzymanie obsługę i doskonalenie SZBI poprzez**
  - **Ustanowienie polityki SZBI**
  - **Zapewnienie że cele i plany bezpieczeństwa informacji zostały ustanowione**
  - **Określenie ról i zakresów odpowiedzialności za bezpieczeństwo informacji**
  - **Informowanie organizacji o znaczeniu realizacji celów bezpieczeństwa informacji oraz zgodności z polityką bezpieczeństwa, odpowiedzialności wobec prawa oraz potrzeby ciągłego doskonalenia**
  - **Dostarczanie wystarczających zasobów dla opracowania, wdrożenia, monitorowania, przeglądów, eksploatacji i utrzymania SZBI**
  - **Decydowanie o kryteriach akceptowania ryzyka i akceptowanym poziomie ryzyka**
  - ***Zapewnienia przeprowadzania wewnętrznych audytów SZBI***
  - **Przeprowadzanie przeglądów SZBI realizowanych przez kierownictwa**

5. Odpowiedzialność kierownictwa (2)

5.2. Zarządzanie zasobami

- **5.2.1 Zapewniania zasobów**
  - **Organizacja powinna określić i zapewnić zasoby potrzebne dla**
    - **Ustanowienia, wdrożenia, eksploatacji monitorowania, przeglądu utrzymania i doskonalenia SZBI**
    - **Zapewnienia że procedury bezpieczeństwa informacji wspomagają wymagania biznesu**
    - **Identyfikacji i odniesienia się do wymagań prawnych i nadzoru oraz zobowiązań kontraktowych**
    - **Utrzymania odpowiedniego bezpieczeństwa przez poprawne wdrożenie wszystkich zastosowanych zabezpieczeń**
    - **przeprowadzenia przeglądów kiedy to konieczne oraz odpowiedniego reagowania na ich wyniki**
    - **poprawy skuteczności SZBI tam, gdzie jest to wymagane**

5. Odpowiedzialność kierownictwa (3)

- **5.2.2. Szkolenie, uświadomienie i kompetencje**
  - **Organizacja powinna zapewnić że cały personel, który posiada zakresy obowiązków określone w SZBI jest kompetentny do wykonywania wymaganych zadań poprzez:**
    - **Określanie koniecznych kompetencji personelu wykonującego prace wpływające na SZBI**
    - **zapewnienie kompetentnego szkolenia lub podjęcia innych działań np. zatrudnianie kompetentnych pracowników) w celu realizacji tych potrzeb**
    - **Ocenę skuteczności przeprowadzonych szkoleń i podjętych działań**
    - **prowadzeniu zapisów o wykształceniu, szkoleniach, umiejętnościach, doświadczeniu i kwalifikacjach**
  - **Organizacja powinna zapewnić, że cały odpowiedni personel jest świadomy co do związku i znaczenia swoich działań dotyczących bezpieczeństwa informacji oraz wkładu dla osiągnięcie celów SZBI**

6. Audyty wewnętrzne

- **6. Wewnętrzne audyty SZBI**
  - **Audyty powinny być przeprowadzane w zaplanowanych odstępach czasu w celu określenia czy:**
    - **Cele stosowania zabezpieczeń**
    - **Zabezpieczenia**
    - **Procesy**
    - **Procedury**
  - **są**
    - **Zgodne z wymaganiami normy i odpowiednimi przepisami prawa oraz regulacyjnym**
    - **Zgodne z zidentyfikowanymi wymaganiami bezpieczeństwa informacji**
    - **Faktycznie wdrożone i utrzymywane**
    - **Realizowane w oczekiwany sposób**

6. Audyty wewnętrzne(2)

- **Program audytu powinien być zaplanowany przy uwzględnieniu**
  - **Statusu procesów i obszarów**
  - **Znaczenia procesów**
  - **Znaczenia obszarów**
  - **Wyników poprzednich audytów**
- **Należy określić:**
  - **Kryteria audytu**
  - **Zakres**
  - **Częstotliwość**
  - **Metody audytów**

6. Audyty wewnętrzne (3)

- **Wybór audytorów i prowadzenie audytu powinno być**
  - **Obiektywne**
  - **Bezstronne**
  - **Nie obejmować obszaru pracy audytora**
- **Zakresy obowiązków, wymagania dla planowania i prowadzenia audytu oraz wykonywania raportów i utrzymywania zapisów powinno być określone w udokumentowanej procedurze**
- **Odpowiedzialność kierownictwa za audytowany obszar powinna zapewnić że działania w celu eliminacji wykrytych niezgodności i ich przyczyn powinny być przeprowadzone bez nieuzasadnionej zwłoki**
- **Działania poaudytowe powinny obejmować**
  - **weryfikacje podjętych działań i**
  - **Informowanie o wynikach weryfikacji**
- ***Uwaga norma ISO 19011 może dostarczyć pomocnych wytycznych do przeprowadzenia wewnętrznych audytów SZBI***

7. Przeglądy dokonywane przez kierownictwo (2)

7.1. Wstęp

- **Kierownictwo powinno dokonywać przeglądów SZBI w regularnych odstępach czasu w celu zapewnienia**
  - **Poprawności**
  - **Odpowiedniości**
  - **Skuteczności**
- **Przegląd powinien zawierać**
  - **ocenione możliwości dla doskonalenia**
  - **Potrzeby zmian w SZBI w tym**
    - Polityki bezpieczeństwa i
    - celów bezpieczeństwa
- **Wyniki przeglądu powinny być**
  - **udokumentowane**
    - a zapisy przechowywane

7. Przeglądy dokonywane przez kierownictwo (3)

7.2. Dane wejściowe do przeglądu

- **powinny zawierać :**
  - **Informacje o wynikach audytów SZBI oraz poprzednich przeglądach**
  - **Informacje zwrotne od zainteresowanych stron**
  - **Rozwiązania techniczne, produkty lub procedury, które mogą być użyte aby doskonalić wydajność i skuteczności SZBI**
  - **Status działań korygujących i zapobiegawczych**
  - **Podatności i zagrożenie co do których nie było odpowiedniego odniesienia w poprzedniej ocenie ryzyka**
  - ***Wyniki pomiaru skuteczności***
  - **Działania wykonane na skutek poprzednich przeglądów realizowanych przez kierownictwo**
  - **Jakiekolwiek zmiany które mogą dotyczyć SZBI**
  - **Zalecenia dotyczące doskonalenia**

7. Przeglądy dokonywane przez kierownictwo (4)

7.3. Dane wyjściowe z przeglądu

- **powinny zawierać wszystkie decyzje i działania związane z**
  - **Doskonaleniem skuteczności SZBI**
  - ***Uaktualnienie planu szacowania ryzyka i postępowania z ryzykiem***
  - **Modyfikacja procedur dotyczących bezpieczeństwa informacji, jeśli jest to konieczne, w celu reakcji, na wewnętrzne lub zewnętrzne zdarzenia które mogą mieć konsekwencje dla SZBI w tym zawierające zmiany w:**
    - Wymaganiach biznesowych
    - Wymaganiach bezpieczeństwa
    - Procesach biznesowych mających wpływ na wymagania biznesowe
    - Uwarunkowaniach prawnych lub wymagań nadzoru
    - Poziomie ryzyka i/lub poziomów akceptacji ryzyka
  - **Potrzebnymi zasobami**
  - **Doskonaleniem pomiarów skuteczności zabezpieczeń**

8. Doskonalenie SZBI (1)

8.1. Ciągłe doskonalenie

- **Organizacja powinna ciągle doskonalić skuteczność SZBI poprzez**
  - **Stosowanie polityki bezpieczeństwa informacji**
  - **Cele bezpieczeństwa**
  - **Wyniki audytów**
  - **Analizę monitorowanych zdarzeń**
  - **Działania korygujące**
  - **Działania zapobiegawcze**
  - **Przeglądy realizowane przez kierownictwo**

8. Doskonalenie SZBI (2)

8.2. Działania korygujące

- **Organizacja powinna podjąć działania w celu wyeliminowania przyczyn niezgodności związanych z wdrożeniem i funkcjonowaniem SZBI aby przeciwdziałać powtórnym ich wystąpieniom**
- **Udokumentowana procedura dla działania korygującego powinna określić wymagania dla:**
  - **Zidentyfikowaniu niezgodności**
  - **Stwierdzaniu przyczyn niezgodności**
  - **Oceny potrzeby działań w celu zapewnienia, że**
    - niezgodności się nie powtórzą
  - **Wskazaniu i wdrożeniu potrzebnych działań korygujących**
  - **zapisów rezultatów podjętych działań**
  - **Przeglądu podjętych działań korygujących**

8. Doskonalenie SZBI (3)

8.3. Działania zapobiegawcze

- **Organizacja powinna wskazywać działanie podejmowane w celu ochrony przed przyszłymi niezgodnościami tak, aby przeciwdziałać ich wystąpieniu.**
- **Działania zapobiegawcze powinny być dostosowane do wagi potencjalnych problemów.**

8. Doskonalenie SZBI (4)

- **Udokumentowana procedura działań zapobiegawczych powinna określić wymagania dla:**
  - **zidentyfikowania potencjalnych niezgodności i**
    - ich przyczyn,
  - ***Oceny potrzeby działania zapobiegawczego***
    - ***w celu zapobieżeniu niezgodnościom***
  - **wskazania i**
    - wdrożenia
    - potrzebnego działania zapobiegawczego
  - **zapisu rezultatów podjętych działań**
  - **przeglądu podjętych działań zapobiegawczych.**
- Organizacja powinna zidentyfikować zmienione ryzyka
  - zwracając uwagę na znacząco zmienione ryzyka
- Należy wskazać priorytety działań zapobiegawczych w oparciu o wyniki szacowania ryzyka
  - **Uwaga działania zapobiegające niezgodnościom są często bardziej efektywne kosztowo niż działania korygujące**

Załącznik A

- ***A5.*** **Polityka bezpieczeństwa**
- ***A6.*** **Organizacja bezpieczeństwa *informacji***
- ***A7. Zarządzanie aktywami***
- ***A8.*** **Bezpieczeństwo *zasobów ludzkich***
- ***A9.*** **Bezpieczeństwo fizyczne i środowiskowe**
- ***A10. Komunikacja i zarządzanie operacyjne***
- ***A11.*** **Kontrola dostępu**
- ***A12. Wdrażanie*****, rozwój i utrzymanie systemu**
- **A13. Zarządzanie incydentami związanymi z bezpieczeństwem**
- ***A14.*** **Zarządzanie ciągłością działania**
- ***A15.*** **Zgodność**

Załącznik B zasady OECD

- **Świadomość**
  - Zaleca się, aby uczestnicy byli świadomi potrzeby
  - bezpieczeństwa systemów informacyjnych i sieci oraz
  - tego co mogą zrobić, aby wzmocnić bezpieczeństwo.
- **Odpowiedzialność**
  - Wszyscy uczestnicy są odpowiedzialni za
  - bezpieczeństwo systemów informacyjnych i sieci.
- **Reakcja**
  - Zaleca się, aby uczestnicy współpracowali ze sobą, a
  - ich działania były podejmowane we właściwym czasie,
  - aby zapobiegać, wykrywać i reagować na incydenty bezpieczeństwa.

Załącznik B

- **Szacowanie ryzyka**
  - Zaleca się, aby uczestnicy przeprowadzili
  - Szacowanie ryzyka.
- **Bezpieczne projektowanie i wdrożenie**
  - Zaleca się, aby uczestnicy włączyli bezpieczeństwo jako
  - istotny element systemów informacyjnych i sieci.
- **Zarządzanie bezpieczeństwem**
  - Zaleca się, aby uczestnicy wprowadzili wszechstronne
  - podejście do zarządzania bezpieczeństwem.
- **Powtórna ocena**
  - Zaleca się, aby uczestnicy przejrzeli i oszacowali
  - bezpieczeństwo systemów informacyjnych i sieci oraz
  - odpowiednio zmodyfikowali polityki bezpieczeństwa,
  - praktyki, środki i procedury.

Załącznik C

- **Porównanie pomiędzy normami**
  - **ISO 27001:2005**
  - **ISO 9001:2000**
  - **ISO 14001:2004**