Zarządzanie incydentami i ciągłością działania oraz zgodność wg z ISO/IEC 27001 i ISO/IEC 27002:2005

dr inż. Bolesław Szomański

bolkosz@wsisiz.edu.pl

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości

A.13.1. **Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości**

Cel:

Zapewnienie że zdarzenia naruszenia bezpieczeństwa informacji oraz słabości, związane z systemami informatycznymi, są zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących.

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości(2)

- *A.13.1.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji*
  - Zgłaszanie zdarzeń
    - związanych z bezpieczeństwem informacji
    - poprzez odpowiednie kanały organizacyjne
  - powinno być
  - wykonywane tak szybko,
    - jak to możliwe .

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości(2)

- **Zalecenia :**
  - **opracowanie formalnej procedury zgłaszania**
    - wraz z
    - **procedurą reagowania na wystąpienie danego naruszenia i eskalacji**
    - **określających działania podejmowane**
    - **po otrzymaniu zgłoszenia o naruszeniu;**
  - **Wyznaczenie punktu kontaktowego znanego i powszechnie dostępnego**

13. 13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości(3)

- **Uświadomienie**
  - **pracowników**
  - **Wykonawców**
  - **użytkowników trzeciej strony**
  - **Zapoznanie z procedurą i lokalizacją punktu;**
- **Procedury zgłaszania powinny obejmować:**
  - **odpowiedni proces zwrotnego informowania zgłaszających zdarzenia tak, że po zamknięciu problemu przekazywane są im wyniki jego obsługi;**
  - **formularze zgłaszania zdarzeń związanych z bezpieczeństwem informacji wspomagające proces zgłaszania i pomagające zgłaszającym zapamiętać wszystkie niezbędne działania na wypadek takiego zdarzenia;**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości(4)

- **poprawne zachowanie na wypadek zdarzeń związanych z bezpieczeństwem informacji, tzn.:**
  - **natychmiastowe zanotowanie wszystkich ważnych szczegółów (np. typu niezgodności lub naruszenia, błędu działania, wiadomości z ekranu, dziwnego zachowania);**
  - **zakaz podejmowania jakichkolwiek własnych działań, lecz natychmiastowe zgłoszenie do punktu kontaktowego;**
- **odwołania do ustanowionego formalnego procesu dyscyplinarnego, który określa sposób postępowania z pracownikami, wykonawcami i użytkownikami reprezentującymi stronę trzecią, którzy naruszają bezpieczeństwo.**

❑ **W środowiskach o wysokim ryzyku, można wprowadzić alarm działania pod przymusem**

❑ **Szczegółowo także ISO TR 18044**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości(5)

❑ **A. 13.1.2** ***Zgłaszanie słabości systemu bezpieczeństwa***

❖ **Wszyscy pracownicy,**
- ❖ **wykonawcy i**
- ❖ **użytkownicy reprezentujący stronę trzecią**
- ❖ **korzystający z systemów informacyjnych i**
  - ❖ usług
- ❖ **powinni być zobowiązani**
- ❖ **do zgłaszania**
  - ❖ wszelkich
- ❖ **zaobserwowanych lub**
- ❖ **podejrzewanych**
- ❖ **słabości bezpieczeństwa**
- ❖ **w systemach i usługach**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości(6)

- **Zaleca się,**
  - aby wszyscy **pracownicy**,
  - **wykonawcy** i
  - **użytkownicy** reprezentujący stronę **trzecią**
- **zgłaszali takie sytuacje albo do kierownictwa,**
  - albo bezpośrednio do swojego dostawcy usług
- **tak szybko,**
  - jak to **możliwe**, aby
  - **uniknąć**
- **incydentów naruszenia bezpieczeństwa informacji.**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości(6)

- **Zaleca się, aby mechanizm zgłaszania był**
  - **prosty,**
  - **dostępny i**
  - **osiągalny.**
- **Zaleca się też, aby byli oni informowani, że nie należy, pod żadnym pozorem, próbować dowodzić podejrzewanej słabości na własną rękę..**
- **Takie zalecenie służy ich bezpieczeństwu,**
  - **bowiem testowanie słabych punktów**
  - **może być interpretowane w systemie**
  - **jako potencjalne nadużycie.**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji 13.2 Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (1)

- **A. 13.2 Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia**
- **Cel**
  - ***Zapewnienie, że stosowane jest***
  - ***spójne i***
  - ***efektywne podejście***
  - ***w zarządzaniu***
  - ***incydentami związanymi z bezpieczeństwem informacji.***

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji 13.2. Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (2)

- ***A.13.2.1. Odpowiedzialność i procedury***
  - **Powinno się**
    - **wprowadzić odpowiedzialność kierownictwa oraz**
    - **procedury**
    - **zapewniające szybką,**
    - **efektywną i**
      - uporządkowaną reakcję na
    - **incydenty związane z bezpieczeństwem informacji.**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji 13.2. Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (2)

- **Oprócz zgłaszania zdarzeń związanych z bezpieczeństwem informacji oraz słabości (patrz także 13.1),**
- **zaleca się wykorzystywanie monitorowania systemów, alarmowania i podatności (10.10.2) do**
- **wykrycia incydentów naruszenia bezpieczeństwa informacji.**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.2 Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (3)

- **Zaleca się żeby procedury zawierały**
  - **naruszenia bezpieczeństwa informacji.**
    - **gdzie jest to wymagane, także gromadzenie dowodów w celu zapewnienia zgodności z wymaganiami prawnymi.**
    - **awarie systemów informacyjnych i utratę usługi;**
    - **szkodliwe oprogramowanie (10.4.1);**
    - **odmowę usługi;**
    - **błędy wynikające z niekompletnych lub niewłaściwych danych biznesowych;**
    - **naruszenia poufności i integralności;**
    - **niewłaściwe użycie systemów informacyjnych;**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.2. Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (4)

- **dodatkowo, w odniesieniu do zwykłych planów ciągłości działania (patrz 14.1.3), zaleca się, aby procedury obejmowały (patrz także 13.2.2):**
  - **analizę i identyfikację przyczyny incydentu;**
  - **ograniczanie zasięgu naruszenia;**
  - **jeśli to potrzebne, planowanie i wdrażanie działań naprawczych w celu uniknięcia ponownego wystąpienia incydentu;**
  - **komunikację z podmiotami dotkniętymi incydentem i tymi, które są zaangażowane w jego usunięcie;**
  - **raportowanie działań do odpowiednich osób**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.2 Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (5)

- **jeśli zachodzi taka potrzeba, to zaleca się gromadzenie i zabezpieczanie dzienników audytu lub podobnych dowodów (patrz 13.2.3) w celu:**
  - **wewnętrznej analizy problemu;**
  - **wykorzystania w postępowaniu dowodowym;**
  - **negocjacji rekompensat ze strony dostawców oprogramowania lub usług**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.2. Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (6)

- **ponadto zaleca się, aby procedury zapewniały, że:**
  - **tylko jednoznacznie zidentyfikowany i uprawniony personel ma dostęp do działających systemów i rzeczywistych danych (patrz także 6.2 – dostęp zewnętrzny);**
  - **wszystkie podejmowane działania awaryjne są szczegółowo dokumentowane;**
  - **działania awaryjne są zgłaszane kierownictwu i sprawnie przeglądane;**
  - **integralność systemów biznesowych i zabezpieczeń jest potwierdzana z minimalnym opóźnieniem.**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.2. Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (6a)

- **Należy zapewnić, że cele**
  - **Zarządzania incydentami naruszenia bezpieczeństwa informacji**
  - **są uzgodnione z kierownictwem oraz**
  - **osoby odpowiedzialne za zarządzanie incydentami naruszenia bezpieczeństwa informacji**
  - **rozumieją priorytety organizacji związane z obsługą takich incydentów.**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.2. Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (7)

- ***A.13.2.2 Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji***
  - **W organizacji powinny istnieć**
  - **mechanizmy umożliwiające zliczenie i**
  - **monitorowanie**
    - **rodzajów,**
    - **rozmiarów i**
    - **kosztów incydentów**
      - związanych z bezpieczeństwem informacji

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.2. Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (7)

- **Zaleca się wykorzystywanie informacji zebranych w trakcie oceny incydentów naruszenia bezpieczeństwa informacji do**
  - **identyfikowania incydentów powtarzających się lub o znacznych konsekwencjach.**

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji

13.2. Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (7)

- ***A.13.2.3. Gromadzenie materiału dowodowego***
  - **Jeśli działania podejmowane**
  - **po wystąpieniu incydentu**
    - **związanego z bezpieczeństwem informacji**
    - **obejmują kroki prawne**
      - (natury cywilnoprawnej lub karnej),
    - **to powinno się**
      - gromadzić,
      - zachować i
      - przedstawić
    - **materiał dowodowego**
    - **zgodnie z zasadami materiału dowodowego**
    - **obowiązującymi w odnośnym prawodawstwie**

13.2. Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (7)

- Zaleca się opracowanie i stosowanie procedur wewnętrznych przy zbieraniu i przedstawianiu materiału dowodowego na potrzeby postępowania dyscyplinarnego prowadzonego w organizacji.
- W ogólnym przypadku zasady związane z materiałem dowodowym odnoszą się do:
  - dopuszczalności materiału dowodowego: czy materiał dowodowy może być wykorzystany w sądzie, czy nie;
  - wagi materiału dowodowego: jakości i kompletności materiału dowodowego.

13.2 Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (9)

- zaleca się, aby organizacja zapewniła, że jej systemy informacyjne są zgodne z opublikowanymi normami lub praktycznymi zasadami tworzenia takiego materiału dowodowego.
- Zaleca się, aby waga dostarczonego materiału dowodowego była zgodna z odnośnymi wymaganiami.
- Zaleca się utrzymanie jakości i kompletności zabezpieczeń poprawnie i w sposób ciągły używanych do ochrony materiału dowodowego (tzn. proces zabezpieczania materiału dowodowego);
- Zaleca się, aby przez okres, w którym materiał dowodowy przeznaczony do odtworzenia ma być przechowywany i przetwarzany, utrzymać mocny ślad dowodowy

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji
13.2 Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (10)

- Warunki uzyskania śladu dowodowego:
  - dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją kto go znalazł, gdzie, kiedy i kto był świadkiem tego zdarzenia;;
  - dla dokumentów na nośnikach komputerowych:
    - zaleca się utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych;
  - zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność;
- zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków;

13. Zarządzanie incydentami w zakresie bezpieczeństwa informacji
13.2 Zarządzanie incydentami naruszenia bezpieczeństwa informacji i udoskonalenia (11)

- zaleca się, aby przechowywać w bezpieczny sposób jedną nienaruszoną kopię nośnika i dziennika zdarzeń.
- Zaleca się przeprowadzenie wszelkich działań śledczych na kopiach materiału dowodowego.
- Zaleca się ochronę integralności wszystkich materiałów dowodowych.
- Zaleca się, aby kopiowanie tych materiałów było nadzorowane przez zaufany personel, a
  - informację, gdzie i kiedy kopiowanie miało miejsce, kto je wykonał oraz przy pomocy jakich narzędzi lub programów zapisać.

14 Zarządzanie ciągłością działania (1)

14.1 Aspekty zarządzania ciągłością działania

Cel: Przeciwdziałanie przerwom
w działalności biznesowej oraz
ochrona krytycznych procesów biznesowych
przed rozległymi awariami systemów informacyjnych
lub katastrofami oraz
zapewnienie wznowienia działalności
w wymaganym czasie

14 Zarządzanie ciągłością działania (1)

- *A.14.1. Włączanie bezpieczeństwa informacji do procesu zarządzania ciągłością działania*
  - Powinno się opracować i
    - utrzymywać
  - zarządzany proces zapewnienia ciągłości działania w organizacji,
  - który określa wymagania bezpieczeństwa potrzebne
  - do zapewnienia ciągłości działania organizacji.

14 Zarządzanie ciągłością działania (1a)

- **Kluczowe elementy** zarządzania ciągłością działania:
  - **identyfikowanie** i
    - nadawanie **priorytetów**
    - **krytycznym procesom** biznesowym;
  - **rozważenie wykupienia**
    - **odpowiedniego ubezpieczenia,**
      - które może stanowić część
    - **procesu zapewnienia ciągłości działania;**

14 Zarządzanie ciągłością działania (2)

14.1 Aspekty zarządzania ciągłością działania

- **sformułowanie i**
  - **opisanie strategii ciągłości działania**
  - **zgodnej z ustalonymi celami i**
  - **priorytetami biznesowymi;**
- **sformułowanie i**
- **opisanie planów zapewnienia ciągłości działania**
- **zgodnych z przyjętą strategią;**
- **regularne testowanie i**
- **aktualizowanie przyjętych planów i procesów;**
- **zapewnienie, że zarządzanie ciągłością działania jest włączone w procesy i strukturę organizacji.**

14 Zarządzanie ciągłością działania (3)

14.1 Aspekty zarządzania ciągłością działania

- *A.14.1.2.Ciągłość działania i szacowanie ryzyka*
  - Powinno się
  - zidentyfikować zdarzenia, które
    - mogą spowodować
  - przerwanie procesów biznesowych,
  - łącznie z prawdopodobieństwem ich wystąpienia oraz
  - konsekwencjami dla bezpieczeństwa informacji.

14 Zarządzanie ciągłością działania (3)

14.1 Aspekty zarządzania ciągłością działania

- **Zaleca się oparcie aspektów zapewnienia ciągłości działania**
  - **związanych z bezpieczeństwem informacji**
  - **na określeniu zdarzeń lub**
  - **ciągów zdarzeń, które**
    - **mogą spowodować przerwy procesów biznesowych organizacji,**
    - **np.. awarie sprzętu, błędy ludzkie, kradzież, pożar, katastrofy naturalne oraz akty terroryzmu**
- **Następnie zaleca się szacowanie ryzyka, tak aby**
  - **określić skutki tych przerw**
    - **(zarówno pod względem skali uszkodzeń, jak i czasu jaki upłynął do momentu przywrócenia normalnego funkcjonowania)**

14 Zarządzanie ciągłością działania (4)

14.1 Aspekty zarządzania ciągłością działania

- *A.14.1.3. Opracowanie i wdrażanie planów ciągłości działania*
  - Powinno się
  - opracować i
  - wdrożyć
  - plany utrzymania lub
    - odtworzenia działalności,
  - zapewniające dostępność informacji
    - na wymaganym poziomie i
    - w wymaganym czasie
  - po wystąpieniu przerwy lub
    - awarii
  - krytycznych procesów biznesowych

14 Zarządzanie ciągłością działania (4)

14.1 Aspekty zarządzania ciągłością działania

- **rozpoznanie i uzgodnienie wszystkich zakresów odpowiedzialności i procedur awaryjnych;**
- **wdrożenie procedur awaryjnych, tak aby umożliwić naprawę i przywrócenie działania w wymaganym czasie;**
- **dokumentację uzgodnionych procedur i procesów;**
- **odpowiednie przeszkolenie personelu w zakresie uzgodnionych awaryjnych procedur i procesów, w tym zarządzania w sytuacjach kryzysowych;**
- **testowanie i aktualizacja tych planów.**

14 Zarządzanie ciągłością działania (5)

14.1 Aspekty zarządzania ciągłością działania

- *A.14.1.4. Struktura planowania ciągłości działania*
  - **Powinno się zachować**
    - **jednolitą strukturę planów ciągłości działania,**
    - **aby zapewnić się, że**
      - wszystkie plany ciągłości oraz
      - wymagania bezpieczeństwa informacji
    - **są ze sobą zgodne oraz**
      - w celu zidentyfikowania
    - **priorytetów**
      - testowania i
      - utrzymania

14 Zarządzanie ciągłością działania (5)

14.1 Aspekty zarządzania ciągłością działania

- **W strukturze planowania ciągłości działania powinny znaleźć się:**
  - **warunki uruchomienia planów;**
  - **procedury awaryjne, które opisują działania podejmowane po wystąpieniu incydentu;**
  - **ustalenia dotyczące zarządzania kontaktami z mediami i efektywnej współpracy z odpowiednimi władzami, np. policją, strażą pożarną i samorządem lokalnym;**
  - **procedury przywracania do stanu normalnego;**
  - **procedury wznowienia działalności,**

14 Zarządzanie ciągłością działania (6)

14.1 Aspekty zarządzania ciągłością działania

- **harmonogram utrzymania, który określa, jak i kiedy plan będzie testowany oraz proces związany z utrzymaniem tego planu;**
- **działania edukacyjne i podnoszące świadomość;**
- **obowiązki poszczególnych osób ze wskazaniem, kto jest odpowiedzialny za wykonanie którego elementu planu.**
- **Krytyczne aktywa i zasoby potrzebne do wykonywania procedur awaryjnych odtwarzania i wznowienia**

14 Zarządzanie ciągłością działania (7)

14.1 Aspekty zarządzania ciągłością działania

- *A.14.5. Testowanie, utrzymywanie i ponowna ocena planów ciągłości działania*
  - **Powinno się regularnie**
  - **testować i**
  - **uaktualniać plany ciągłości działania,**
    - tak aby zapewnić
    - **ich aktualność i**
    - **efektywność.**

14 Zarządzanie ciągłością działania (7)

14.1 Aspekty zarządzania ciągłością działania

Uwzględnienie podczas testowania:

- **testowanie różnych scenariuszy na "papierze";**
- **symulacje;**
- **testowanie technicznych możliwości przywrócenia stanu sprzed awarii**
  - **(efektywności przywrócenia systemów informacyjnych do stanu poprzedniego)**
- **testowanie odtworzenia stanu poprzedniego w alternatywnej siedzibie**
  - **(procesy biznesowe biegną równolegle z działaniami związanymi z przywracaniem stanu poprzedniego, poza główną lokalizacją);**

14 Zarządzanie ciągłością działania (8)

14.1 Aspekty zarządzania ciągłością działania

- **testy urządzeń i usług dostawców**
  - **(zapewnienie, że usługi i produkty dostarczane przez zewnętrznych dostawców będą odpowiadać umowom);**
- **próby generalne**
  - **(sprawdzanie, czy organizacja, personel, sprzęt, instalacje i procesy radzą sobie z przerwami w działaniu).**

14 Zarządzanie ciągłością działania (9)

14.1 Aspekty zarządzania ciągłością działania

Do przykładowych sytuacji, które mogą wymagać aktualizacji planów, należą:

- **pozyskanie nowego sprzętu,**
- **wprowadzenie nowej wersji systemu operacyjnego oraz**
- **zmiany:**
  - **personelu;**
  - **adresów i numerów telefonów;**
  - **strategii biznesowej;**
  - **lokalizacji, urządzeń i zasobów;**
  - **przepisów prawnych;**
  - **kontrahentów, dostawców i głównych klientów;**
  - **procesów, w tym**
    - wprowadzenie nowych, bądź
    - wycofanie starych;
  - **ryzyka (operacyjnego i finansowego).**

15 Zgodność (1)

15.1 Zgodność z przepisami prawnymi

Cel: Unikanie naruszania jakichkolwiek przepisów prawa, zobowiązań wynikających z ustaw, regulacji wewnętrznych lub umów oraz jakichkolwiek wymagań bezpieczeństwa

15 Zgodność (2)
15.1 Zgodność z przepisami prawnymi

- *A.15.1.1 Określenie odpowiednich przepisów prawnych*
  - **Wszelkie wymagania**
    - **wynikające z ustaw,**
      - zarządzeń i
      - umów oraz
      - podejście organizacji do ich wypełniania
    - **powinny być wyraźnie określone,**
      - udokumentowane i
      - aktualizowane
    - **dla każdego systemu informacyjnego w organizacji**

15 Zgodność (2a)
15.1 Zgodność z przepisami prawnymi

- **Podobnie dla zakresów obowiązków**
- **Trzeba też śledzić zmiany w przepisach prawnych**
- **Jest to robota dla prawników**

15 Zgodność (3)
15.1 Zgodność z przepisami prawnymi

- *A.15.1.2. Prawo do własności intelektualnej*
  - **Należy wprowadzić odpowiednie procedury,**
  - **w celu zapewnienia zgodności**
  - **z wymaganiami wynikającymi**
    - **z przepisów prawa ,**
    - **regulacji wewnętrznych i**
    - **umów**
  - **dotyczącymi użytkowania materiałów, które**
  - **mogą być objęte prawami do**
    - **własności intelektualnej oraz**
    - **użytkowaniem**
  - **prawnie zastrzeżonego oprogramowania .**

15 Zgodność (3)
15.1 Zgodność z przepisami prawnymi

- **Zalecenia**
  - **Naruszenie może spowodować sprawy karne (BSA)**
  - **Wymagania umów mogą nakładać ograniczenia na kopiowanie**
- **Uwaga ten punkt**
  - **obejmuje zarządzanie oprogramowaniem wg Microsoftu**

15 Zgodność (4)
15.1 Zgodność z przepisami prawnymi

- *A.15.1.3. Ochrona zapisów organizacji*
  - Należy chronić
  - ważne zapisy organizacji
  - przed utratą,
    - zniszczeniem lub
    - sfałszowaniem zgodnie z
    - wymaganiami ustawowymi,
      - regulacjami wewnętrznymi oraz
      - wymaganiami biznesowymi i
      - kontraktowymi.

15 Zgodność (4)
15.1 Zgodność z przepisami prawnymi

- **Systemy przechowywania zapisów elektronicznych powinny spełniać następujące wymagania:**
  - **publikowanie wytycznych dotyczących przechowywania, gromadzenia, obsługi i niszczenia zapisów oraz informacji;**
  - **sporządzenie harmonogramu przechowywania, określającego zasadnicze rodzaje zapisów, i okres, przez jaki będą przechowywane;**
  - **prowadzenie spisu źródeł kluczowych informacji;**
  - **wprowadzenie odpowiednich zabezpieczeń w celu ochrony zasadniczych zapisów i informacji przed utratą, zniszczeniem lub sfałszowaniem. .**

15 Zgodność (5)
15.1 Zgodność z przepisami prawnymi

- *A.15.1.4. Ochrona danych osobowych i prywatność informacji dotyczących osób fizycznych*
  - Należy zapewnić
  - zgodność ochrony danych osobowych i
  - prywatności
  - z odpowiednimi przepisami prawa,
    - regulacjami wewnętrznymi,
  - i jeśli to wymagane,
    - z zapisami odpowiednich umów.

15 Zgodność (5)
15.1 Zgodność z przepisami prawnymi

- **Przepisy prawa dotyczące ochrony danych osobowych wymagają**
  - **wprowadzenia odpowiednich struktur zarządzania i kontroli.**
- **Administrator danych –**
  - **odpowiedzialny za przestrzeganie przepisów prawa w tym zakresie**
- **Administrator bezpieczeństwa informacji (ABI) -**
  - **opracowywanie wytycznych dla kierowników, użytkowników i dostawców usług dotyczące ich indywidualnych zakresów odpowiedzialności oraz określonych procedur, które powinny być przestrzegane.**

15 Zgodność (6)

15.1 Zgodność z przepisami prawnymi

- *A.15.1.5 Zapobieganie nadużywaniu urządzeń przetwarzających informacje*
  - Należy
  - wprowadzić sankcje
    - w przypadku korzystania przez użytkowników
  - ze środków służących do przetwarzania informacji
  - w nieautoryzowanych celach.

15 Zgodność (6)

15.1 Zgodność z przepisami prawnymi

- **Legalność monitorowania (opinia prawna w tym zakresie!).**
- **Prawodawstwo w zakresie przestępczości komputerowej.**
- **W trakcie procedury rejestrowania na ekranie komputera zaleca się wyświetlanie ostrzeżenia informującego,**
  - **że system, do którego użytkownik się rejestruje, jest systemem prywatnym i nieuprawniony dostęp nie jest dozwolony.**

15 Zgodność (7)

15.1 Zgodność z przepisami prawnymi

- *A.15.1.6. Regulacje dotyczące zabezpieczeń kryptograficznych*
  - Używanie zabezpieczeń kryptograficznych
  - powinno być zgodne
    - z odpowiednimi umowami,
  - prawem i
  - regulacjami wewnętrznymi.

15 Zgodność (7)

15.1 Zgodność z przepisami prawnymi

- **Kontrola państwa w tym zakresie może obejmować:**
  - **import lub eksport sprzętu komputerowego i oprogramowania przeznaczonego do wykonywania funkcji kryptograficznych;**
  - **import lub eksport sprzętu komputerowego i oprogramowania, zaprojektowanych tak, aby można było dodać do nich funkcje kryptograficzne;**
  - **obowiązkowe lub dobrowolne metody dostępu władz państwowych do informacji, które zaszyfrowano sprzętowo lub programowo w celu zapewnienia poufności ich zawartości.**

15 Zgodność (8)

15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna

Cel: *Zapewnianie zgodności systemów z politykami bezpieczeństwa i standardami bezpieczeństwa.*

15. Zgodność (9)

15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna

- ***A.15.2.1. Zgodność z polityką bezpieczeństwa i standardami***
  - **Kierownicy powinni zapewnić, że wszystkie**
  - **procedury bezpieczeństwa obszaru,**
    - **za który są odpowiedzialni, są**
  - **wykonywane prawidłowo,**
  - **tak aby osiągnąć zgodność z politykami bezpieczeństwa**
    - **i standardami**

15. Zgodność (9)

15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna

- **Zaleca się, aby**
  - **kierownicy**
  - **regularnie przeglądali**
  - **zgodność przetwarzania informacji**
    - **w obszarze, za który są odpowiedzialni,**
  - **z odpowiednimi politykami bezpieczeństwa**
    - **i standardami oraz**
  - **innymi wymaganiami bezpieczeństwa**

15. Zgodność (10)

15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna

- **Jeśli w wyniku przeglądu zostaną wykryte jakiekolwiek niezgodności, to**
  - **zaleca się, aby kierownictwo:**
    - **określiło przyczyny niezgodności;**
    - **oceniło potrzebę działań zapewniających, że niezgodność nie wystąpi ponownie;**
    - **określiło i wprowadziło odpowiednie działania korygujące;**
    - **poddało przeglądowi podjęte działania korygujące.**
- **Zaleca się rejestrowanie wyników**
  - **przeglądów i**
  - **działań korygujących podejmowanych przez kierownictwo**
  - **Oraz utrzymywanie rejestrów tych zdarzeń.**

15. Zgodność (11)

15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna

- **Zaleca się, aby kierownictwo udostępniało wyniki przeglądów osobom przeprowadzającym niezależne przeglądy (patrz 6.1.8),**
  - **jeśli niezależny przegląd jest przeprowadzany w obszarze, za który kierownictwo jest odpowiedzialne**

15. Zgodność (11)

15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna

- ***A.15.2.2. Sprawdzanie zgodności technicznej***
  - **Systemy informacyjne**
    - **powinny być regularnie**
  - **sprawdzane**
    - **pod kątem zgodności**
  - **ze standardami wdrażania zabezpieczeń.**

15. Zgodność (11)

15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna

- **Sprawdzanie technicznej zgodności wymaga analizy eksploatowanych systemów.**
  - **wymaga technicznej pomocy specjalistów którzy prowadzą je:**
    - **ręcznie**
      - Przez **doświadczonego** inżyniera **systemowego** lub
    - **Za pomocą zautomatyzowany pakietu oprogramowania,**
      - generującego raport
      - celem dokonania **późniejszej interpretacji**
      - przez technicznego specjalistę.

15 Zgodność (13)

15.2 Przeglądy polityki bezpieczeństwa i zgodności technicznej

- **Kontrola zgodności obejmuje**
  - **test penetracyjny,**
    - **przeprowadzony przez niezależnych ekspertów.**
  - **przydatny do**
    - **wykrywania podatności oraz**
    - **sprawdzania efektywności zabezpieczeń**
  - **Należy postępować ostrożnie w razie pomyślnego dokonania penetracji,**
    - **bo może to prowadzić do poważnego naruszenia bezpieczeństwa systemu**
    - **I nieumyślnego wykorzystania innych jego podatności.**
- **Kontrole takie powinny być prowadzone**
  - **jedynie przez lub**
  - **pod nadzorem kompetentnych, uprawnionych osób.**

15 Zgodność (14)

15.3 Rozważania dotyczące audytu systemów informacyjnych

Cel: *Maksymalizowanie skuteczności procesu audytu systemu informacyjnego i minimalizowanie zakłóceń z niego wynikających lub na niego wpływających*

- *A. 15.3.1. Zabezpieczenia audytu systemu informacyjnego*
  - Aby minimalizować ryzyka zakłóceń procesów biznesowych,
  - powinno się starannie planować i uzgadniać
    - wymagania audytu oraz
  - działania związane
    - ze sprawdzaniem eksploatowanych systemów

15. Zgodność (14)

15.3 Rozważania dotyczące audytu systemów informacyjnych

- **uzgadnianie** i **kontrolowanie zakresu** sprawdzenia;
- **ograniczenie kontroli** dostępu do oprogramowania i danych jedynie w **trybie odczytu**;
- **zasoby informacyjne niezbędne do prowadzenia kontroli wyraźnie określane i udostępniane;**
- **Monitorowanie i zapisywanie w dziennikach zdarzeń każdego dostępu w celu umożliwienia odwołań.**
- **Dokumentowanie wszystkich procedur, wymagań i obowiązków.**

15 Zgodność (15)

15.3 Rozważania dotyczące audytu systemów informacyjnych

- ***15.3.2. Ochrona narzędzi audytu systemów informacyjnych***
  - **Dostęp do narzędzi audytu systemu,**
  - **powinien być chroniony**
  - **aby zapobiec możliwym nadużyciom lub**
    - **naruszeniu bezpieczeństwa,**

15 Zgodność (16)

15.3 Rozważania dotyczące audytu systemów informacyjnych

- **Narzędzia takie powinny być**
  - **izolowane od eksploatowanych systemów i**
  - **systemów wykorzystywanych do prowadzenia prac rozwojowych oraz**
  - **nie powinny być przechowywane**
    - **w bibliotekach oprogramowania lub**
    - **obszarach dostępnych publicznie,**
    - **chyba że zostanie zapewniony odpowiedni poziom dodatkowej ochrony.**