Elementy wymagań Zarządzania bezpieczeństwem informacji wg ISO/IEC 27001 i ISO/IEC 27002 bezpieczeństwo fizyczne

dr inż. Bolesław Szomański

bolkosz@wsisiz.pw.edu.pl

Filozofia prezentacji wymagań i zabezpieczeń zgodnie z załącznikiem A

- **Nagłówek rozdziały normy ISO 17799**
- Obszary tematyczne - o różnym poziomie komplikacji
- ***Cele zabezpieczenia (objectives)***
- **Wymagania dotyczące stosowania zabezpieczeń (z ISO 27001)**
- **Zalecenia z ISO/IEC 17799 (27002)**
- **Wskazówki realizacji (*implementation guidance*)**

9 - Bezpieczeństwo fizyczne i środowiskowe

- **A 9.1 Obszary bezpieczne**
- **A 9.2 Zabezpieczenie sprzętu**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (1)

A.9.1. Obszary bezpieczne

Cel: *zapewnienie ochrony przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w siedzibie organizacji oraz w odniesieniu do informacji.*

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (2)

- *A.9.1.1 Granica obszaru zabezpieczanego*
  - Granice obszaru bezpiecznego
    - (bariery, takie jak
      - ściany,
      - bramki wejściowe na kartę lub
      - recepcja z obsługą)
    - powinny być stosowane w celu
    - ochrony obszarów zawierających
    - informacje i
      - środki przetwarzania informacji.

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (2)

- **wyraźne określenie obszaru zabezpieczanego;**
- **solidne konstrukcje budynku lub miejsca,**
  - gdzie znajdują się urządzenia do przetwarzania informacji;
- **stanowisko recepcyjne obsługiwane przez człowieka lub**
  - zapewnienie innych środków kontroli fizycznego dostępu;
- **rozciąganie barier fizycznych**
  - od właściwej podłogi do właściwego sufitu
    - *Uwzględnić czynniki środowiskowe, takie jak pożar lub zalanie.*
- **Zaleca się, aby wszystkie drzwi pożarowe w obwodzie budynku były**
  - zabezpieczone alarmem i
  - wyposażone w zamek samozatrzaskowy.
  - Fizyczne oddzielenie urządzeń przetwarzających informacje firmy i strony trzeciej

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (3)

- *A.9.1.2 Fizyczne zabezpieczenie wejścia*
  - obszary bezpieczne
    - powinny być chronione
    - przez właściwe zabezpieczenia wejścia
      - zapewniające, że
  - tylko autoryzowany personel
  - ma prawo dostępu

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (3)

- **Zalecenia**
  - **Nadzór nad gośćmi**
  - **w tym rejestrowanie godziny**
    - **wejścia i wyjścia**
  - **Stosowanie zabezpieczeń w tym kart zbliżeniowych**
- **Dostęp do wrażliwych informacji oraz**
  - **urządzeń przeważających informacje ograniczony do osób uprawnionych**
- **Przyznawanie personelowi strony trzeciej ograniczonego dostępu i jego monitorowanie**
- **Zalecenie dla personelu noszenia identyfikatorów**
- **Regularne sprawdzanie praw dostępu**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (4)

- ***A.9.1.3. Zabezpieczenie biur,pomieszczeń i urządzeń***
  - **Powinno się**
  - **zaprojektować**
    - **i stosować**
  - **ochronę fizyczną**
    - **biur,**
    - **pomieszczeń i**
    - **urządzeń.** .

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (4)

- **Uwzględnienie przepisów bhp**
- **Najważniejsze urządzenia powinny być rozmieszczane tak, aby**
  - **uniknąć publicznego do nich dostępu.**
- **budynki powinny być**
  - **skromne i w**
  - **minimalnym stopniu**
    - wskazywać na swoje przeznaczenie,
- **Książki adresowe i**
  - **wewnętrzne książki telefoniczne**
  - **wskazujące usytuowanie urządzeń przetwarzania wrażliwych informacji**
  - **nie powinny być łatwo dostępne dla osób z zewnątrz**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (5)

- **A.9.1.4 Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi**
  - **Powinno się opracować i**
  - **stosować ochronę fizyczną przed**
    - **zniszczeniami spowodowanymi przez**
      - pożar,
      - powódź,
      - trzęsienie ziemi,
      - wybuch,
      - niepokoje społeczne i inne
      - formy naturalnych lub
      - spowodowanych przez człowieka
    - **katastrof.**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (7)

- **Materiały**
  - **niebezpieczne lub**
  - **łatwopalne**
  - **powinny być bezpiecznie składowane**
  - **w odpowiedniej odległości od obszaru bezpiecznego.**
- **Duże ilości materiałów,**
    - np. biurowych,
  - **nie powinny być przechowywane**
  - **w pomieszczeniach komputerowych,**
  - **aż do chwili, kiedy będą potrzebne.**
- **W celu zapobieżeniu skutkom katastrofy w głównej siedzibie,**
  - **sprzęt zapasowy i**
  - **nośniki kopii zapasowych**
  - **powinny być składowane w pomieszczeniach**
  - **znajdujących się w bezpiecznej odległości.**
- **Umieszczenie sprzętu przeciwpożarowego w odpowiednich miejscach**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (8)

- *A.9.1.5. Praca w obszarach bezpiecznych*
  - **Powinno się**
    - **opracować i wdrożyć**
  - **mechanizmy ochrony fizycznej oraz**
  - **wytyczne pracy**
  - **w obszarach bezpiecznych.**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (8)

- **Zalecenia**
  - **Personel powinien być poinformowany**
    - **o istnieniu obszaru bezpiecznego i**
    - **prowadzonej tam działalności**
    - **tylko w takim zakresie,**
    - **w jakim jest to niezbędne.**
  - **Powinno się unikać pracy bez nadzoru w obszarach bezpiecznych**
  - **Zamykanie i okresowe sprawdzanie obszarów w których nie pracują ludzie**
  - **Niedopuszczenie do korzystania z urządzeń fotograficznych nagrywających i audio bez upoważnienia**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (11)

- *A.9.1.6 Obszary publicznego dostępu dostaw i załadunku*
  - **Punkty dostępu,**
    - takie jak obszary
    - dostaw i
    - załadunku oraz
    - inne punkty,przez które
  - **nieuprawnione osoby mogą**
    - wejść do siedziby i,
      - *jeśli to możliwe,*
      - *Powinny być nadzorowane i jeśli to możliwe*
    - odizolowane od
    - środków służących do przetwarzania informacji
    - w celu uniknięcia nieautoryzowanego dostępu.

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (11)

- **Zalecenia**
  - **Dostęp z zewnątrz budynku**
    - **do obszaru magazynowego**
    - **powinien być ograniczony tylko do**
    - **zidentyfikowanego,**
    - **uprawnionego personelu.**
  - **Obszar magazynowy powinien być tak zaprojektowany,**
    - **aby dostawy mogły być rozładowywane bez uzyskiwania przez personel dostawcy**
    - **dostępu do innych części budynku.**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.1 Obszary bezpieczne (12)

- **Zewnętrzne drzwi obszaru magazynowego**
  - powinny być zabezpieczone
  - w czasie,
  - **gdy otwarte są**
  - **drzwi wewnętrzne.**
- **Dostarczane materiały,**
  - **przed ich przeniesieniem z obszaru magazynowego**
  - **do miejsca wykorzystania,**
  - **powinny być sprawdzane pod kątem**
  - **potencjalnych niebezpieczeństw**
- **Dostarczane materiały powinny być rejestrowane,**
  - **jeśli zachodzi taka potrzeba**
  - **na wejściu do siedziby.**
- **Jeśli to możliwe rozdzielenie przychodzących i wychodzących dostaw**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (1)

A.9.2.Cel:
Zapobieganie utracie, uszkodzeniu lub naruszeniu aktywów oraz przerwaniu działalności organizacji

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (2)

❑ ***9.2.1. Rozmieszczenie sprzętu i jego ochrona***

❖ **Sprzęt powinien być**
- **rozlokowany i**
- **chroniony**
  - w taki sposób, aby
- **redukować ryzyko wynikające z**
- **zagrożeń i**
- **niebezpiecznych czynników środowiskowych**
  - oraz
- **możliwości nieautoryzowanego dostępu.**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (2)

- **minimalizowanie ryzyka**
  - **niepożądanego dostępu do**
  - **obszarów roboczych;**
- **ograniczenie możliwości braku nadzoru nad użyciem**
  - **urządzeń przetwarzających informację wrażliwą;**
- **izolowanie elementów wymagających specjalnej ochrony,**
  - **tak aby ograniczyć wymagany ogólny poziom ochrony.**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (3)

- **zabezpieczenia przed zagrożeniami:**
  - **kradzież;**
  - **pożar;**
  - **materiały wybuchowe;**
  - **dym;**
  - **woda**
    - lub przerwa w dostawach wody
  - **kurz;**
  - **drgania;**
  - **oddziaływanie chemiczne;**
  - **interferencje pochodzące ze źródeł zasilania;**
  - **promieniowanie elektromagnetyczne**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (4)

- **wprowadzenie zasad dotyczących zakazu**
  - **jedzenia,**
  - **picia i**
  - **palenia tytoniu**
    - **w pobliżu urządzeń do przetwarzania informacji;**
- **monitorowanie czynników środowiskowych;**
- **Wyposażenie w instalację odgromową i filtry przeciwprzepięciowe**
- **specjalne zabezpieczenia**
  - **pracy sprzętu**
  - **w warunkach przemysłowych;**
- **wpływ sąsiedztwa**
  - **np. możliwość pożaru w sąsiednim budynku.**
- **Ochrona urządzeń przetwarzających informacje wrażliwe przed wyciekiem informacji związanych z ulotem elektromagnetycznym**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (5)

- *A.9.2.2. Systemy wspomagające*
  - Sprzęt powinien być chroniony przed
    - awariami zasilania i
    - zakłóceniami spowodowanymi
    - przez awarie
      - systemów wspomagających.

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (6)

- **systemy wspomagające, takie jak zasilanie, zaopatrzenie w wodę, kanalizacja, ogrzewanie/wentylacja oraz klimatyzacja, odpowiednio dobrać do systemów, które obsługują.**
- **Zaleca się regularne sprawdzanie tych usługi i, jeśli trzeba, testowanie, aby funkcjonowały poprawnie i aby zredukować ryzyko ich awarii lub niepoprawnego działania**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (7)

- **zachowanie ciągłości zasilania zapewniają następujące urządzenia: zwielokrotnienie linii zasilających, zasilacze awaryjne, generatory;**
- **plany awaryjne uwzględniające działania, które mają być podjęte w przypadku awarii zasilacza;**
- **jeżeli zainstalowane są generatory, to zaleca się ich regularne testowanie, zgodnie z zaleceniami producenta;**
- **w razie awarii głównego źródła zasilania zapewnienie oświetlenia awaryjnego;**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (8)

- *A.9.2.3. Bezpieczeństwo okablowania*
  - Okablowanie zasilające i telekomunikacyjne
    - służące do transmisji danych lub
      - wspomagające usługi informacyjne
    - powinno być chronione
      - przed przejęciem lub
      - uszkodzeniem

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (6)

- **ochrona linii zasilających i telekomunikacyjnych do urządzeń przetwarzających informacje (np. prowadzenie pod ziemią);**
- **ochrona linii komunikacyjnych przed podsłuchem lub uszkodzeniem (np. rury kablowe);**
- **oddzielenie kabli zasilających od kabli telekomunikacyjnych (zapobieganie interferencji);**
- **dodatkowe zabezpieczenia dla systemów wrażliwych lub krytycznych (opancerzone rury kablowe, alternatywne trasy rutingu i mediów transmisyjnych, wykorzystanie okablowania światłowodowego, wyszukiwanie nieuprawnionych prób podłączania się do urządzeń.**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (7)

- *A.9.2.4. Konserwacja sprzętu*
  - sprzęt powinien być poprawnie konserwowany
    - dla zapewnienia jego
  - ciągłej
    - dostępności i
    - integralności

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (7)

- **konserwacja sprzętu zgodnie z zaleceniami producentów;**
- **naprawy i serwisowanie wykonywane tylko przez uprawniony personel konserwujący;**
- **rejestrowanie wszystkich awarii lub podejrzeń awarii i wszystkich działań prewencyjnych oraz napraw;**
- **odpowiednie środki zabezpieczające w przypadku wysłania sprzętu poza siedzibę (wymazywanie i nadpisywanie danych);**
- **rozszerzenie polisy ubezpieczeniowej.**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (8)

- ❑ *A.9.2.5. Bezpieczeństwo sprzętu poza siedzibą*
  - ❖ Sprzętu pozostający poza siedzibą
  - ❖ powinien być chroniony
    - ❖ przy uwzględnieniu
  - ❖ ryzyk związanych
    - ❖ z pracą
    - ❖ poza siedzibą organizacji.

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (8)

- **niebezpieczeństwa miejsc publicznych (laptopy w bagażu podręcznym);**
- **zalecenia producentów np. dotyczące ochrony przed silnym polem elektromagnetycznym;**
- **dodatkowe czynniki ryzyka w przypadku pracy w domu;**
  - **Opisane też w ISO 18028**
- **ubezpieczenie sprzętu znajdującego się poza siedzibą.**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (9)

- ❑ *A.9.2.6. Bezpieczne zbywanie sprzętu lub przekazywanie do ponownego użycia*
  - ❖ Wszystkie składniki sprzętu
  - ❖ zawierające nośniki informacji
  - ❖ powinny być sprawdzone
    - ❖ Aby przed jego zbyciem,
    - ❖ upewnić się,
  - ❖ że jakiekolwiek informacje wrażliwe i
    - ❖ licencjonowane oprogramowanie,
  - ❖ zostały usunięte lub
  - ❖ bezpiecznie nadpisane

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (9)

- **Zamiast zwykłego usuwania lub**
- **formatowania w urządzeniach zawierających informacje wrażliwe**
- **zaleca się fizyczne niszczenie,**
  - **usuwanie lub**
  - **nadpisywanie informacji**
    - przy użyciu technik zapewniających, że
  - **nie będzie można jej odtworzyć, a**
  - **nie standardowego usuwania czy formatowania.**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (10)

- ***A.9.2.7 Wynoszenie mienia***
  - **Sprzęt,**
    - **informacje lub**
    - **oprogramowanie**
  - **nie powinno być wynoszone**
  - **bez uprzedniego zezwolenia.**

9 - Bezpieczeństwo fizyczne i środowiskowe 9.2 Bezpieczeństwo sprzętu (10)

Inne zalecenia:

- **nie należy wynosić sprzętu, informacji lub oprogramowania bez wcześniejszej autoryzacji;**
- **jasne określenie pracowników, wykonawców i użytkowników reprezentujących stronę trzecią, którzy**
- **mają prawo wynoszenia aktywów;**
- **określenie i sprawdzanie czasu zwrotu wynoszonego sprzętu;**
- **jeśli to potrzebne i właściwe, rejestrowanie kiedy sprzęt jest wynoszony i kiedy zwracany.**