Zarządzanie ryzykiem w bezpieczeństwie informacji

dr inż. Bolesław Szomański

bolkosz@wsisiz.edu.pl

Zarządzania ryzykiem

- ***Zarządzanie i kontrola ryzyka jest dzisiaj***
  - ***najdonioślejszym tematem w świecie biznesu***
    - Robin Kendall
    - „Zarządzanie Ryzykiem dla Menadżerów”2000
    - Można dodać
    - A dzisiaj jest jeszcze ważniejszym (2008).

Zarządzanie ryzykiem

- Zarządzanie ryzykiem jest procesem, który pozwala kierownictwu na zrównoważenie operacyjnych i
  - ekonomicznych kosztów środków ochrony z uzyskanym wynikiem w dążeniu do skuteczności
- ***Fundamentalną zasadą na której opiera się proces zarządzania ryzykiem jest to, że***
- ***celem jest ochrona danego podmiotu - organizacji a nie jej zasobów informacyjnych***

Definicje

- **Ryzyko**
  - **kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji**
    - **W niektórych standardach**
    - **ryzyko może się wiązać zarówno z**
      - aspektami pozytywnymi (szanse) jak i
      - negatywnymi (zagrożenia)

Definicje

- **skutek**
  - negatywna zmiana w odniesieniu do osiąganego poziomu celów biznesowych
- **ryzyko w bezpieczeństwie informacji**
  - potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów
  - powodując w ten sposób szkodę dla organizacji
    - *UWAGA Ryzyko jest mierzone jako kombinacja prawdopodobieństwa zdarzenia i jego następstw.*
- **unikanie ryzyka**
  - decyzja o nieangażowaniu się lub działanie w kierunku wycofania się z ryzykownej sytuacji

Definicje

- **informowanie o ryzyku**
  - wymiana lub dzielenie się informacjami o ryzyku między decydentami a innymi uczestnikami N3)
- **estymacja ryzyka**
  - proces przypisywania wartości prawdopodobieństwu i następstwom ryzyka
    - UWAGA 1, dla estymacji ryzyka używa się terminu "działanie" zamiast "proces".
  - UWAGA 2
    - **W kontekście niniejszej normy, używa się**
    - terminu "prawdopodobieństwo" zamiast
    - "prawdopodobieństwo matematyczne"
- **identyfikowanie ryzyka**
  - proces znajdowania, zestawiania i charakteryzowania elementów ryzyka

Definicje

- **redukowanie ryzyka**
  - działania, podejmowane w celu zmniejszenia prawdopodobieństwa,
  - negatywnych następstw,
    - lub obu,
  - związanych z ryzykiem
- **zachowanie ryzyka**
  - akceptowanie ciężaru straty lub korzyści z zysku, z określonego ryzyka
    - *UWAGA W kontekście bezpieczeństwa informacji,*
    - *w przypadku zachowywania ryzyka rozważane są jedynie negatywne*
    - *następstwa (straty).*
- **transfer ryzyka**
  - dzielenie z inną stroną ciężaru straty lub korzyści z zysku, dla ryzyka

Definicje

- akceptowanie ryzyka
  - **decyzja, aby zaakceptować ryzyko**
    - **risk acceptance**
- analiza ryzyka
  - **systematyczne korzystanie z informacji w celu zidentyfikowania źródeł i oceny ryzyka.**
    - **risk analizys**
- Szacowanie ryzyka
  - **całościowy proces analizy ryzyka i oceny ryzyka**
    - **risk assessment**

Definicje

- ocena ryzyka
  - **proces porównywania estymowanego ryzyka z założonymi kryteriami ryzyka w celu wyznaczenia wagi ryzyka.**
    - **risk evaluation**
- zarządzanie ryzykiem
  - **skoordynowane działania w celu kierowania i kontroli organizacji z uwzględnieniem ryzyka**
    - **risk management**
- postępowanie z ryzykiem
  - **proces polegający na wyborze i wdrożeniu środków modyfikujących ryzyko**
    - **risk treatment**
- Ryzyko szczątkowe
  - **Ryzyko pozostające po postępowaniu z ryzykiem**

ISO/IEC 27005 zarządzanie ryzykiem w bezpieczeństwie informacji

- **Przedmowa**
- **Wprowadzenie**
- **1. Zakres normy**
- **2. Powołania normatywne**
- **3. Terminy i Definicje**
- **4. Struktura niniejszej normy międzynarodowej**
- **5. Informacje podstawowe**
- **6. Przegląd procesu zarządzania ryzykiem w bezpieczeństwie informacji**
- **7. Ustanowienie kontekstu**
  - **7.1 Rozważania ogólne**
  - **7.2. Podstawowe kryteria**
  - **7.3 Zakres i granice**
  - **7.4. Organizacja zarządzania ryzykiem w bezpieczeństwie informacji**

Budowa ISO/IEC 27005

- **8 Szacowanie ryzyka w bezpieczeństwie informacji**
  - **8.1 Ogólny opis szacowania ryzyka w bezpieczeństwie informacji .**
  - **8.2 Analiza ryzyka**
  - **8.2.1 Identyfikowanie ryzyka**
    - **8.2.2 Estymacja ryzyka**
  - **8.3 Ocena ryzyka**
- **9 Postępowanie z ryzykiem w bezpieczeństwie informacji**
  - **9.1 Ogólny opis postępowania z ryzykiem**
  - **9.2 Redukowanie ryzyka**
  - **9.3 Zachowanie ryzyka**
  - **9.4 Unikanie ryzyka**
  - **9.5 Transfer ryzyka**

Budowa ISO/IEC 27005

- **10 Akceptowanie ryzyka w bezpieczeństwie informacji**
- **11 Informowanie o ryzyku w bezpieczeństwie informacji**
- **12 Monitorowanie i przegląd ryzyka w bezpieczeństwie informacji**
  - **12.1 Monitorowanie i przegląd czynników ryzyka**
  - **12.2 Monitorowanie, przegląd i doskonalenie zarządzania ryzykiem.**

5. Informacje podstawowe

- **Systematyczne podejście do zarządzania ryzykiem w bezpieczeństwie informacji jest niezbędne**
  - **Dla określenia potrzeb organizacji**
  - **Tworzenia SZBI**
- **Zaleca się żeby zarządzanie ryzykiem było ciągłym procesem i obejmowało**
  - **Zidentyfikowanie ryzyk**
  - **Oszacowanie ryzyk**
  - **Informowanie o prawdopodobieństwie i następstwie ryzyka**

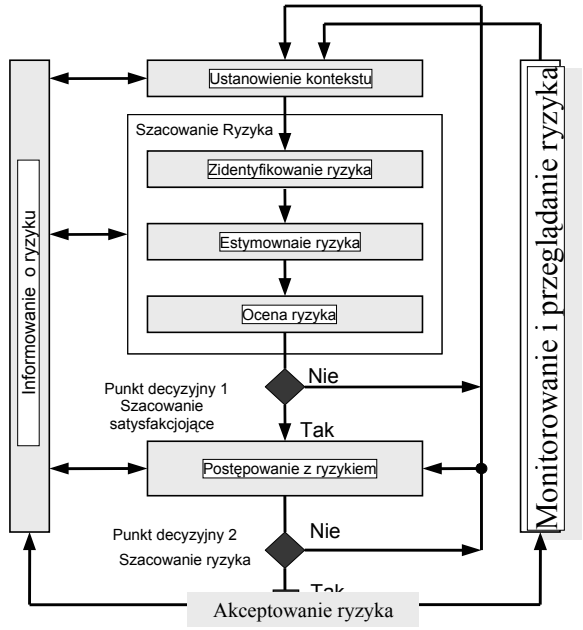
5. Informacje podstawowe

- **Ustanowienie priorytetów dla postępowania z ryzykiem**
- **Określenie priorytetów działań podjętych w celu zredukowania ryzyka**
- **Zaangażowanie uczestników w momencie podejmowania decyzji w procesie zarządzania ryzykiem oraz**
  - **stałe informowanie ich o statusie zarządzania ryzykiem**
- **Skuteczność monitorowania postępowania z ryzykiem**
- **Regularne monitorowanie i przegląd ryzyk oraz procesu zarządzania ryzykiem**
- **Zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem**
- **Szkolenie kierownictwa i personelu w zakresie ryzyk oraz działań podejmowanych w celu ograniczenia ryzyk**

5. Informacje podstawowe

- **Proces zarządzania ryzykiem w bezpieczeństwie informacji może być zastosowany do:**
  - **Organizacji jako całości**
  - **Dowolnej części organizacji (działów, fizycznej lokalizacji, usługi)**
  - **Dowolnego systemu informacyjnego**
  - **zabezpieczeń istniejących, planowanych lub o wybranym aspekcie (np. planowanie ciągłości działania)**

6. Proces zarządzania ryzykiem wg ISO/IEC 27005



Koniec pierwszych i kolejnych iteracji

6. Proces zarządzania ryzykiem

- **Planowanie**
  - **Ustanowienie kontekstu**
  - **Szacowanie ryzyka**
  - **Opracowanie planu postępowania z ryzykiem**
  - **Akceptowanie ryzyka**
- **Wdrożenie**
  - **Wdrożenie planu postępowania z ryzykiem**
- **Sprawdzenie**
  - **Ciągłe monitorowanie i przegląd ryzyka**
- **Doskonalenie**
  - **Utrzymanie i doskonalenie procesu zarządzania ryzykiem bezpieczeństwa informacji**

7. Określenie zakresu

- **7.2 Podstawowe kryteria**
  - **Zależne od zakresu i celów zarządzania ryzykiem**
  - **Mogą być także inne dla każdej iteracji**
  - **Kryteria oceny ryzyka**
  - **Kryteria skutków**
  - **Kryteria akceptacji**
  - **Dodatkowe zasoby dla**
    - **Przeprowadzenia szacowania ryzyka i ustanowienia planu postępowania z ryzykiem**
    - **Zdefiniowania i wdrożenia polityk i procedur a także zabezpieczeń**
    - **Monitorowania zabezpieczeń**
    - **Monitorowania procesu zarządzania ryzykiem bezpieczeństwa informacji**

7. Określenie zakresu

- **Kryteria oceny ryzyka**
  - **Strategiczna wartość biznesowa procesów informacyjnych**
  - **Krytyczność zasobów informacyjnych**
  - **Wymagania prawne i regulacyjne i zobowiązania kontraktowe**
  - **Operacyjne i biznesowe znaczenie dostępności, poufności i integralności**
  - **Oczekiwanie i postrzeganie udziałowców i negatywne skutki dla dobrego imienia i reputacji**
  - **Dodatkowo kryteria szacowania ryzyka mogą być wykorzystane do określenia priorytetów działań przy postępowaniu z ryzykiem**

7. Określenie zakresu

- **Kryteria skutków**
  - **Powinny być opracowane i wyspecyfikowane poprzez określenie stopnia uszkodzeń lub kosztów uwzględniając:**
    - **Poziom klasyfikacji aktywów informacyjnych**
    - **Naruszenie bezpieczeństwa informacji (utrata poufności, integralności i dostępności)**
    - **Narażone operacje (wewnętrzne lub trzeciej strony)**
    - **Straty w biznesie i wartości finansowej**
    - **Naruszenie planów i terminów**
    - **Utrata reputacji**
    - **Naruszenie prawych regulacyjnych i kontraktowych wymagań**

7. Określenie zakresu

- **Kryteria akceptowania ryzyka**
  - **Powinny opracowane i wyspecyfikowane**
  - **Zależą one od polityki organizacji celów oraz interesów udziałowców**
  - **Organizacja określa swoją własną skalę poziomów akceptacji ryzyka**
    - Kryteria akceptowania ryzyka mogą zawierać wiele progów określających docelowy poziom ryzyka
    - Ale zawierać możliwość dla wyższego kierownictwa do zaakceptowania ryzyka powyżej tego poziomu w określonych warunkach

7. Określenie zakresu

- Kryteria mogą być określane w stosunku szacowanego przychodu do szacowanego ryzyka
- Różne kryteria akceptacji mogą być zastosowane dla różnych klas ryzyka (np.. niespełnienie wymagań prawnych nieakceptowalne ale wysokie ryzyko dopuszczalne w przypadku wymagań umów)
- Kryteria mogą zawierać wymagania dla dalszego postępowania

- **Kryteria mogą być różne zależnie od czasu jak długo ryzyko będzie istniało**
- **Kryteria powinny uwzględniać**
  - Kryteria biznesowe
  - Prawne i regulacyjne aspekty
  - Operacje
  - Technologię
  - Finanse
  - Czynniki ludzkie i socjalne

7. Określenie zakresu

❑7.3 Zakres i granice

- **Powinny uwzględniać**

- **Strategiczne cele organizacji strategie i polityki**
- **Procesy biznesowe**
- **Funkcje organizacji i strukturę**
- **Prawne, regulacyjne i kontraktowe wymagania**
- **Polityką bezpieczeństwa informacji organizacji**
- **Podejście organizacji o zarządzania ryzykiem**
- **Aktywa informacyjne**

7. Określenie zakresu

- **Lokalizację organizacji i jej geograficzne charakterystyki**
- **Uwarunkowania wpływające na organizację**
- **Oczekiwania udziałowców**
- **Środowisko socjo-kulturalne**
- **Interface (wymiana informacji z otoczeniem)**

- **I dodatkowo uzasadnienie wykluczenia z zakresu**
- **Przykłady zakresu**
  - **Aplikacja, infrastruktura informatyczna, proces biznesowy, część organizacji**

7. Określenie zakresu

- **7.4 Organizacja zarządzania ryzykiem bezpieczeństwa informacji**
  - **Powinna być utworzona i utrzymywana**
  - **Podstawowe role i odpowiedzialności to:**
    - **Zaprojektowanie procesu zarządzania ryzykiem bezpieczeństwa informacji**
    - **Identyfikacja i analiza udziałowców**
    - **Zdefiniowanie ról i odpowiedzialności wszystkich stron zarówno wewnętrznych jak i zewnętrznych**
    - **Ustanowienie związków pomiędzy organizacją i udziałowcami oraz związków z ryzykiem wysokiego poziomu i innymi odpowiednimi projektami i działaniami**

ISO/IEC 27005

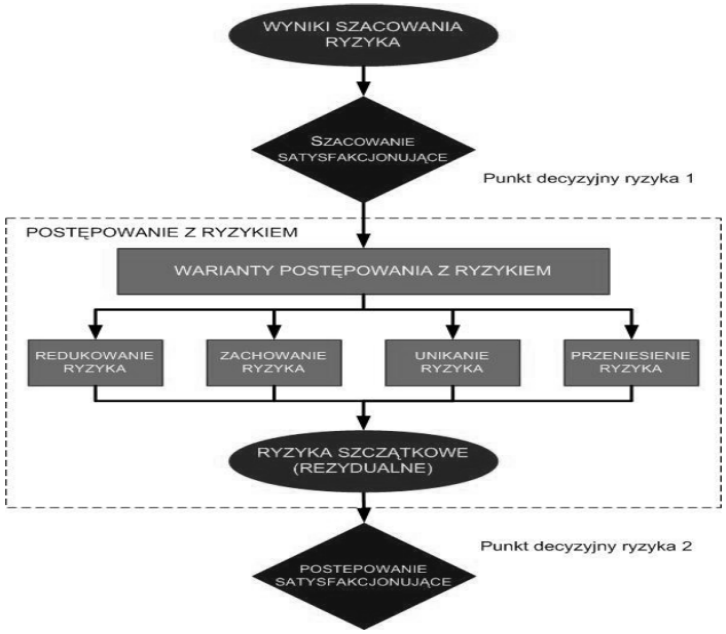
- **8. Szacowanie ryzyka w bezpieczeństwie informacji**
  - **8.1. Ogólny opis szacowania ryzyka w bezpieczeństwie informacji**
  - **8.2. Analiza ryzyka**
  - **8.2.1. Identyfikowanie ryzyka**
    - **8.2.1.1. Wprowadzenie do identyfikacji**
    - **8.2.1.2 Identyfikacja aktywów → załącznik B1**
    - **8.2.1.3. Identyfikacja zagrożeń → załącznik C**
    - **8.2.1.4. Identyfikacja istniejących zabezpieczeń**
    - **8.2.1.5. Identyfikacja podatności → załącznik D1**
    - **8.2.1.6. Identyfikacja skutków**

8. Szacowanie ryzyka w bezpieczeństwie informacji

- **8.2.2. Estymacja ryzyka**
  - 8.2.2.1. Metodyki oceny ryzyka
    - *Jakościowe*
    - *Ilościowe*
  - 8.2.2.2. Szacowanie skutków
  - 8.2.2.3. Szacowanie szansy wystąpienia skutków
  - 8.2.2.4 Poziom oszacowania ryzyka
- **8.3. Ocena ryzyka**

9. Postępowanie z ryzykiem związanym z bezpieczeństwem informacji

- **9.1 Ogólny opis postępowania z ryzykiem**
  - **Dane wejściowe:**
    - **Lista ryzyk z priorytetami zgodnymi z kryteriami oceny ryzyka,**
    - **w odniesieniu do scenariuszy incydentów, prowadzących do tych ryzyk.**
  - **Działania:**
    - **Zaleca się wybór zabezpieczeń w celu zredukowania, zachowania, uniknięcia lub transferu ryzyk i określenia planu postępowania z ryzykiem.**
  - **Wytyczne do wdrożenia:**
    - **Istnieją cztery warianty postępowania z ryzykiem:**
      - redukowanie ryzyka (zob. 9.2),
      - zachowanie ryzyka (zob. 9.3),
      - unikanie ryzyka (zob. 9.4) i
      - transfer ryzyka (zob. 9.5).



9.1

- **Cztery warianty postępowania z ryzykiem nie wyłączają się wzajem**
- **Ogólnie, zaleca się, aby niekorzystne następstwa ograniczyć na tyle, na ile jest to uzasadnione względami praktycznymi i niezależnie od jakichkolwiek bezwzględnych kryteriów.**
- ***Zaleca się, aby kierownictwo rozważyło rzadkie, ale poważne ryzyka.***
- **W takich przypadkach może zachodzić potrzeba wdrożenia zabezpieczenia, które nie ma ściśle ekonomicznego uzasadnienia**
- **Czasem organizacja może odnieść znaczącą korzyść z połączenia wariantów takich, jak ograniczenie prawdopodobieństwa ryzyk, ograniczenie ich następstw oraz transfer lub zachowanie każdego z ryzyk szczątkowych.**

- **Dane wyjściowe:**
  - **Plan postępowania z ryzykiem i ryzyka szczątkowe będące przedmiotem decyzji kierownictwa organizacji o akceptacji.**

9.2

9.2 Redukowanie ryzyka

- **Działanie:**
  - **Zaleca się zredukowanie ryzyka przez wybór zabezpieczeń tak,**
  - **aby ryzyko szczątkowe można było ponownie oszacować jak ryzyko do zaakceptowania.**
- **Wytyczne do wdrożenia:**
  - **Zaleca się wybór właściwych i uzasadnionych zabezpieczeń w celu spełnienia wymagań zidentyfikowanych w szacowaniu i postępowaniu z ryzykiem.**
  - **Zaleca się, aby wybór ten uwzględniał zarówno kryteria akceptowania ryzyka, jak i wymagania wymagające z przepisów prawa, regulacji wewnętrznych oraz zobowiązań kontraktowych.**
  - **Zaleca się, aby wybór ten uwzględniał koszt i czas wdrożenia zabezpieczeń lub aspekty techniczne, środowiskowe i kulturowe.**

9.2

- **W trakcie wyboru zabezpieczeń i podczas ich wdrożenia zaleca się uwzględnienie różnych ograniczeń. Zwykle, pod uwagę brane są następujące:**
  - Ograniczenia czasowe
  - Ograniczenia finansowe
  - Ograniczenia techniczne
  - Ograniczenia związane z eksploatacją
  - Ograniczenia kulturowe
  - Ograniczenia etyczne
  - Ograniczenia środowiskowe
  - Ograniczenia prawne
  - Łatwość użycia
  - Ograniczenia dotyczące personelu
  - Ograniczenia związane z integracją nowych i istniejących zabezpieczeń

9.3

9.3 Zachowanie ryzyka

- **Działanie: Zaleca się podjecie decyzji o zachowaniu ryzyka bez dalszych działań w oparciu o ocenę ryzyka.**
  - *UWAGA W punkcie ISO/IEC 27001 4.2.1 f 2) "poznanie i zaakceptowanie ryzyk, w sposób świadomy i obiektywny, przy założeniu, że jasno spełniają warunki wyznaczone w polityce organizacji oraz kryteria akceptowania ryzyk" opisano to samo działanie.*
- **Wytyczne do wdrożenia:**
  - **Jeśli poziom ryzyka spełnia kryteria akceptowania ryzyka, to nie ma potrzeby wdrażania dodatkowych zabezpieczeń i ryzyko może być zachowane.**

9.4

9.4 Unikanie ryzyka

- **Działanie:**
  - **Zaleca się unikanie działań lub warunków, które powodują powstanie określonych ryzyk.**
- **Wytyczne do wdrożenia:**
  - **W przypadku, gdy zidentyfikowane ryzyka są interpretowane jako zbyt wysokie,**
  - **lub koszty wdrożenia innych wariantów postępowania z ryzykiem przewyższają korzyści,**
  - **może być podjęta decyzja o całkowitym uniknięciu ryzyka, przez wycofanie się z planowanej lub istniejącej działalności**
  - **lub zbioru działalności,**
  - **lub zmianę warunków, w których działalność ta jest prowadzona.**

9.5

9.5 Transfer ryzyka

- **Działanie:**
  - **W oparciu o ocenę ryzyka, zaleca się transfer ryzyka do innej strony, która może skutecznie zarządzać ryzykiem.**
- **Wytyczne do wdrożenia:**
  - **Transfer ryzyka oznacza podjecie decyzji o dzieleniu określonych ryzyk z zewnętrznymi stronami.**
  - **Transfer ryzyka może powodować powstanie nowych ryzyk lub modyfikację istniejących, zidentyfikowanych ryzyk.**
  - **Z tego względu może być potrzebne dodatkowe postępowanie z ryzykiem.**
  - **Transfer może być realizowany przez ubezpieczenie, które pokryje następstwa lub przez podwykonawstwo wykonywane przez partnera, którego rolą będzie monitorowanie systemu informacyjnego i podejmowanie natychmiastowych działań w celu powstrzymania ataku, zanim wyrządzi szkodę o określonym poziomie.**

9.5

- **Zaleca się odnotowanie, że może istnieć możliwość transferu odpowiedzialności za zarządzanie ryzykiem,**
- **natomiast zwykle nie ma możliwości przeniesienia odpowiedzialności za skutki.**
- **Zwykle klienci postrzegają negatywne skutki jako błąd organizacji.**

10 Akceptowanie ryzyka związanego z bezpieczeństwem informacji

- **Dane wejściowe:**
  - **Plan postępowania z ryzykiem i oszacowanie ryzyka szczątkowego przedłożone kierownictwu organizacji do decyzji o akceptacji**
- **Działanie:**
  - **Zaleca się podjęcie i formalne udokumentowanie decyzji o zaakceptowaniu ryzyka oraz odpowiedzialności za decyzję (w odniesieniu do ISO/IEC 27001 pkt. 4.2.1 h)).**
- **Wytyczne do wdrożenia:**
  - **Zaleca się, aby plany postępowania z ryzykiem opisywały, w jaki sposób postępować z oszacowanymi ryzykami, aby spełnić kryteria akceptowania ryzyka (zob. Rozdział 7.2 Kryteria akceptowania ryzyka).**
  - **Jest istotne, aby odpowiedzialni członkowie kierownictwa dokonali przeglądu i zatwierdzili proponowane plany postępowania z ryzykiem oraz wynikowe ryzyka szczątkowe, a także zapisali wszystkie warunki związane z taką aprobatą.**

10 Akceptowanie ryzyka związanego z bezpieczeństwem informacji

  - **Kryteria akceptowania ryzyka mogą być bardziej złożone niż jedynie określenie, czy ryzyko szczątkowe znajduje się poniżej, czy powyżej pojedynczej wartości progowej.**
  - **Czasami , kryteria akceptowania ryzyka są nieodpowiednie i zaleca się, w miarę możliwości, ich zmianę.**
  - **Gdy jest to niemożliwe**
    - zaleca się żeby podejmujący decyzję w sposób jawny dołączył komentarz do ryzyk i zawarł uzasadnienie dla decyzji pominięcia normalnych kryteriów akceptowania ryzyka.
- **Dane wyjściowe:**
  - **Lista zaakceptowanych ryzyk wraz z uzasadnieniem dla tych ryzyk, które nie spełniają normalnych dla organizacji kryteriów akceptowania ryzyka.**

11 Informowanie o ryzyku związanym z bezpieczeństwem informacji

- **Dane wejściowe:**
  - **Wszystkie informacje o ryzyku pozyskane w trakcie działań związanych z zarządzaniem ryzykiem**
- **Działanie:**
  - **Zaleca się wymianę lub dystrybucję informacji o ryzyku między podejmującymi decyzje a innymi uczestnikami.**
- **Wytyczne do wdrożenia:**
  - **Informowanie o ryzyku jest działaniem podejmowanym w celu osiągnięcia porozumienia co do sposobu zarządzania ryzykiem przez wymianę lub dystrybucję informacji o ryzyku między podejmującymi decyzję a innymi uczestnikami.**
  - **Informacje obejmują, ale nie są ograniczone do istnienia, charakteru, formy, prawdopodobieństwa, powagi, postępowania i możliwości zaakceptowania ryzyk.**

11.

  - **Zaleca się, aby przeprowadzać działania informacyjne dotyczące ryzyka, mające na celu:**
    - Zapewnienie wiarygodności wyników zarządzania ryzykiem w organizacji
    - Zbieranie informacji o ryzyku
    - Dystrybucję rezultatów z szacowania ryzyka i prezentowania planu postępowania z ryzykiem
    - Uniknięcie lub ograniczenie zarówno pojawiania się, jak i następstw naruszeń bezpieczeństwa informacji z powodu braku wzajemnego zrozumienia podejmujących decyzję i uczestników
    - Wsparcie dla procesu podejmowania decyzji
    - Uzyskanie nowej wiedzy o bezpieczeństwie informacji
    - Koordynowanie z innymi stronami oraz planowanie reakcji, prowadzących do ograniczenia następstw każdego incydentu
    - Wytworzenie u podejmujących decyzje oraz uczestników poczucia odpowiedzialności za ryzyka
    - Podniesienie świadomości

11.

- **Jest ważne, aby współpracować z odpowiednią komórką organizacyjną odpowiedzialną za „public relations lub za działania informacyjne podejmowane w celu koordynowania wszystkich zadań związanych z informowaniem o ryzyku.**
- **Ma to zasadnicze znaczenie w przypadku działań związanych z komunikacją w sytuacjach kryzysowych, przykładowo, w odpowiedzi na określone incydenty.**

- **Dane wyjściowe:**
  - **Ciągłe zrozumienie w organizacji dla procesu zarządzania ryzykiem związanym z bezpieczeństwem informacji oraz jego wyników.**

12 Monitorowanie i przegląd ryzyka związanego z bezpieczeństwem informacji

❑12.1 Monitorowanie i przegląd czynników ryzyka

- **Dane wejściowe:**
  - **Wszystkie informacje o ryzyku uzyskane z działań związanych z zarządzaniem ryzykiem**
- **Działanie:**
  - **Zaleca się monitorowanie i przegląd ryzyk i ich czynników**
    - (tzn. wartości aktywów, skutków, zagrożeń, podatności, prawdopodobieństwa wystąpienia)
    - w celu identyfikowania każdej zmiany w kontekście organizacji na wczesnym etapie, oraz
    - w celu utrzymania obrazu kompletnej mapy ryzyka.

12.1

- **Wytyczne do wdrożenia:**
  - **Ryzyka nie są statyczne.**
  - **Zagrożenia, podatności, prawdopodobieństwo lub następstwa mogą zmieniać się w sposób nagły, bez żadnej oznaki.**
  - **Potrzebny jest zatem monitoring w celu wykrycia tych zmian.**
  - **Takie działanie może być wspierane przez usługi zewnętrzne, które zapewniają informacje dotyczące nowych zagrożeń lub podatności.**
  - **Zaleca się, aby organizacje zapewniały, że monitorowane są w sposób ciągły następujące czynniki ryzyka:**
    - Nowe aktywa, które zostały włączone w zakres zarządzania ryzykiem
    - Konieczne modyfikacje wartości aktywów, np. z powodu zmienionych wymagań biznesowych

12.1

    - Nowe zagrożenia, które mogą być aktywne zarówno na zewnątrz, jak i wewnątrz organizacji i które dotąd nie były oszacowane
    - Prawdopodobieństwo, że nowe lub zwiększone podatności mogłyby umożliwić zagrożeniom wykorzystanie tych nowych lub zmienionych podatności
    - Zidentyfikowane podatności w celu określenia tych, które są narażone na nowe lub pojawiające się powtórnie zagrożenia
    - Większe skutki lub następstwa oszacowanych zagrożeń, podatności i ryzyk łącznie powodujących nieakceptowalny poziom ryzyka
    - Incydenty związane z bezpieczeństwem informacji
  - **Rezultaty działań związanych z monitorowaniem ryzyka mogą stanowić dane wejściowe do innych działań związanych z przeglądem ryzyka.**
  - **Zaleca się, aby organizacja dokonywała przeglądu wszystkich ryzyk regularnie, oraz w przypadku pojawienia się większych zmian**
- **Dane wyjściowe:**
  - **Ciągłe dostosowywanie zarządzania ryzykami do celów biznesowych organizacji i kryteriów akceptowania ryzyka.**

12.2

12.2 Monitorowanie, przegląd i doskonalenie zarządzania ryzykiem

- **Dane wejściowe:**
  - **Wszystkie informacje o ryzyku uzyskane z działań związanych z zarządzaniem ryzykiem**
  - **Działanie:**
    - Zaleca się, aby proces zarządzania ryzykiem był w sposób ciągły monitorowany, przeglądany i doskonalony, stosownie do potrzeb.
- **Wytyczne do wdrożenia:**
  - **Ciągłe monitorowanie i przegląd jest konieczne dla zapewnienia, że kontekst, wyniki szacowania ryzyka i postępowania z ryzykiem, jak i plany zarządzania ryzykiem odpowiadają potrzebom i okolicznościom.**

12.2

- **Zaleca się, aby organizacja zapewniła, że proces zarządzania ryzykiem związanym z bezpieczeństwem informacji oraz związane z nim działania**
  - pozostają odpowiednie do aktualnych okoliczności i
  - są kontynuowane.
- **Zaleca się, aby o każdym uzgodnionym udoskonaleniu procesu lub działań koniecznych do zwiększenia zgodności z procesem był**
  - powiadamiany menadżer odpowiedniego szczebla, tak aby
  - zapewnić, że żadne ryzyko lub element ryzyka nie został pominięty lub niedoszacowany oraz
  - podjęto odpowiednie działania i decyzje w celu zagwarantowania realistycznego spojrzenia na ryzyko oraz utrzymania możliwości reakcji.

12.2

- **Zaleca się, aby te działania monitoringu i przeglądu odnosiły się (lecz nie było ograniczone) do:**
  - Kontekstu prawnego i środowiskowego
  - Kontekstu związanego z konkurencją
  - Podejścia do szacowania ryzyka
  - Wartości i kategorii aktywów
  - Kryteriów skutków
  - Kryteriów oceny ryzyka
  - Kryteriów akceptowania ryzyka
  - Całkowitego kosztu utrzymania
  - Koniecznych zasobów

12.2

- **Monitorowanie ryzyka może skutkować modyfikacją lub uzupełnieniem podejścia, metodyki lub używanych narzędzi, w zależności od:**
  - **Zidentyfikowanych zmian**
  - **Iteracji szacowania ryzyka**
  - **Celu procesu zarządzania ryzykiem związanym z bezpieczeństwem informacji (np. ciągłość działania, odporność na incydenty, zgodność)**
  - **Przedmiotu procesu zarządzania ryzykiem**
    - (np. organizacja, jednostka organizacyjna, proces informacyjny, jego techniczne wdrożenie, aplikacja, połączenie z internetem)

Dane wyjściowe:

- **Ciągłe dostosowanie procesu zarządzania ryzykiem związanym z bezpieczeństwem informacji do celów biznesowych organizacji lub uaktualnienie procesu.**

Załączniki do ISO/IEC 27005

- Załącznik A (informacyjny)

- **Definiowanie zakresu i granic procesu zarządzania ryzykiem w bezpieczeństwie informacji**
  - A.1 Studium organizacji
  - A.2 Lista ograniczeń dotyczących organizacji
  - A.3 Lista powołań legislacyjnych i regulacyjnych mających zastosowanie w organizacji
  - A.4 Lista ograniczeń dotyczących zakresu
    - Załącznik B (informacyjny)
- **Identyfikowanie i wartościowanie aktywów oraz szacowanie skutków**
  - B.1 Przykłady identyfikowania aktywów
    - B.1.1 Identyfikowanie aktywów podstawowych
    - B.1.2 Lista i opis aktywów wspierających

Załączniki do ISO/IEC 27005

  - B.2 Wartościowanie aktywów
  - B.3 Szacowanie skutków
    - Załącznik C (informacyjny)
- **C. Przykłady typowych zagrożeń**
    - Załącznik D (informacyjny)
- **D. Podatności i metody szacowania podatności**
  - D.1 Przykłady podatności
  - D.2 Metody szacowania podatności technicznych

Załączniki do ISO/IEC 27005

- Załącznik E (informacyjny)

- **E. Podejścia do szacowania ryzyka w bezpieczeństwie informacji**
  - E.1 Ogólne szacowanie ryzyka w bezpieczeństwie informacji
  - E.2 Szczegółowe szacowanie ryzyka w bezpieczeństwie informacji
    - E.2.1 Przykład 1 Macierz z wcześniej zdefiniowanymi wartościami . 56
    - E.2.2 Przykład 2 Ranking zagrożeń przez pomiar ryzyka
    - E.2.3 Przykład 3 Szacowanie wartości prawdopodobieństwa i potencjalnych następstw ryzyka
- Załącznik F (informacyjny)
- **F. Ograniczenia przy redukowaniu ryzyka**

A. Definiowanie zakresu i granic procesu zarządzania ryzykiem bezpieczeństwa informacji

- **A1. Studium organizacji**
  - Ocena organizacji
  - Główny cel organizacji
  - Działalność Biznesowa organizacji
  - Misja organizacji
  - Wartości organizacji
  - Struktura organizacji
  - Schemat organizacyjny
  - Strategia organizacji

A. Określenie zakresu i granic ...

- A2. Lista ograniczeń dotyczących organizacji
  - Polityczne
  - Strategiczne
  - Terytorialne
  - Wynikające z klimatu politycznego i ekonomicznego
  - Strukturalne
  - Funkcjonalne
  - Związane z personelem
  - Wynikające z kalendarza organizacji

A. Określenie zakresu i granic ...

  - Związane z metodami
  - Natury kulturalnej
  - Budżetowe
- A.3 Wykaz odsyłaczy do przepisów prawnych i regulacyjnych mających zastosowanie w organizacji

A. Określenie zakresu i granic ...

- A.4. Lista ograniczeń dotyczących zakresu
  - ograniczenia wynikające z istniejących wcześniej procesów
  - ograniczenia techniczne
  - ograniczenia finansowe
  - ograniczenia środowiskowe
  - ograniczenia czasowe
  - ograniczenia związane z metodami
  - ograniczenia organizacyjne

B. Identyfikacja i wartościowanie aktywów i szacowanie skutków

- B1 Przykłady identyfikacji aktywów
  - Podstawowe
  - Wspierające
- B1.1. Identyfikowanie aktywów podstawowych
  - Procesy (lub podprocesy) biznesowe i działania
    - Procesy których utrata lub degradacja uniemożliwia spełnianie misję organizacji
    - Procesy zawierające tajemnice lub technologię stanowiące własność intelektualną
    - Procesy które jeżeli zostaną zmodyfikowane mogą w dużym stopniu wpłynąć na misję organizacji
    - Procesy które są niezbędne dla spełnienia wymagań kontraktowych prawnych i regulacyjnych

B1.1. Identyfikacja aktywów ...

- **Informacje**
  - **Niezbędne informacje dla misji organizacji lub jej działalności biznesowej**
  - **Informacje osobowe**
  - **Informacje strategiczne**
  - **Kosztowne informacje (do pozyskania, przechowywania, przetwarzania i transmisji):**

B.1.2. Lista i opis aktywów wspierających

- **Sprzęt:**
  - **Urządzenia przetwarzania danych (aktywne)**
  - **Urządzenia przenośne**
  - **Urządzenia stacjonarne**
  - **Urządzenia peryferyjne**
  - **Nośniki danych (pasywne)**
  - **Nośniki elektroniczne**
  - **Inne nośniki**

B.1.2. Wykaz i opis aktywów wspierających

- **Oprogramowanie**
  - **System operacyjny**
  - **Oprogramowanie usługowe, utrzymania lub administracyjne**
  - **Pakiety oprogramowania lub standardowe oprogramowanie**
  - **Aplikacje biznesowe**
    - Standardowe
    - Dedykowane
- **Sieć**
  - **Media i usługi wspierające**
  - **Przekaźniki aktywne i pasywne**
  - **Interface komunikacyjne**

B.1.2. Wykaz i opis aktywów wspierających

- **Personel**
  - **Decydenci**
  - **Użytkownicy**
  - **Personel operacyjny i utrzymania**
  - **Twórcy oprogramowania**
- **Siedziba**
  - **Lokalizacja**
    - Środowisko Zewnętrzne
    - Siedziba
    - Strefa
    - Podstawowe usługi

B.1.2. Wykaz i opis aktywów wspierających

- Łączność
- Systemy wspomagające

- **Organizacja**
  - **Organy władzy**
  - **Struktura organizacji**
  - **Organizacja projektowa lub systemowa**
  - **Kooperanci/dostawcy/producenci**

B.2. Wartościowanie aktywów

- **Kryteria**
- **Redukcja do wspólnej bazy**
  - **Czyli określenie możliwych skutków wynikających z utraty poufności, integralności, dostępności, niezaprzeczalności, rozliczalności, autentyczności lub niezawodności aktywów**
    - **Naruszenie przepisów prawa i/lub regulacji**
    - **Pogorszenie wydajności działalności biznesowej**
    - **Utrata wizerunku/ negatywny wpływ na reputację**
    - **Naruszenie ochrony danych osobowych**
    - **Narażenie bezpieczeństwa osób**

B.2. Szacowanie aktywów

  - **Niekorzystne efekty spełnienia wymagań prawnych**
  - **Naruszenie poufności**
  - **Naruszenie porządku publicznego**
  - **Straty finansowe**
  - **Przerwanie działalności biznesowej**
  - **Narażenie ochrony środowiska**
- **Inne podejście**
  - **Przerwanie świadczenia usług**
  - **Utrata zaufania klienta**
  - **Zakłócenie wewnętrznej operacji**
  - **Zakłócenie operacji trzeciej strony**
  - **Naruszenie przepisów prawa lub regulacji**
  - **Naruszenie umowy**

B.2. Szacowanie aktywów

- **Niebezpieczeństwo dla personelu/użytkowników**
- **Atak na prywatne życie użytkowników**
- **Straty finansowe**
- **Koszty działań ratunkowych i naprawczych**
- **Utrata dóbr/funduszy/aktywów**
- **Utrata klientów, utrata dostawców**
- **Postępowanie prawne i kary**
- **Utrata przewagi konkurencyjnej**
- **Utrata technologicznego/technicznego przewodnPSSwa**
- **Utrata technicznej reputacji**
- **Osłabienie zdolności negocjacyjnych**

B.2. Szacowanie aktywów

- Kryzysy przemysłowe (strajki)
- Kryzysy rządowe
- Zwolnienia
- Szkoda materialna

- Skala
- Zależności
- Rezultat

B3. Szacowanie skutków

- Bezpośrednie
  - Finansowa wartość zastąpienia utraconych aktywów (lub ich części)
  - Koszty nabycia, skonfiguracji i zainstalowania nowych aktywów lub odtworzenia z kopii zapasowej
  - Koszty zawieszonych operacji spowodowanej incydentem dopóki usługa realizowana przez aktywa nie zostanie przywrócona
  - Skutki naruszenia bezpieczeństwa informacji

B3. Szacowanie skutków

- Pośrednie
  - Koszty utraconych korzyści
  - Koszty przerwanych operacji
  - Potencjalne niepoprawne użycie informacji uzyskanych na skutek naruszenia bezpieczeństwa
  - Naruszenie statutowych lub regulacyjnych zobowiązań
  - Naruszenie kodeksu etycznego postępowania

C. Przykłady typowych zagrożeń

N-naturalne, P-przypadkowe, U-umyślne

- Fizyczne
  - Pożar U, P, N
  - Zalanie N,P,U
  - Zanieczyszczenie N,P,U
  - Poważny Wypadek N,P,U
  - Zniszczenie urządzeń lub nośników N,P,U
  - Kurz, korozja, zamarznięcie N,P,U
- Zjawiska Naturalne
  - zjawiska klimatyczne N
  - zjawiska sejsmiczne N
  - zjawiska wulkaniczne N
  - zjawiska meteorologiczne N
  - Powódź N

C. Przykłady typowych zagrożeń

- Utrata podstawowych usług
  - Awaria klimatyzacji lub dostawy wody P,U
  - Utrata dostaw prądu N,P,U
  - Awaria wyposażenia telekomunikacyjnego P,U
- Zakłócenia spowodowane przez promieniowanie
  - Promieniowanie elektromagnetyczne N,P,U
  - Promieniowanie cieplne N,P,U
  - Impuls elektromagnetyczny N,P,U

C. Przykłady typowych zagrożeń

- Naruszenie bezpieczeństwa informacji
  - Przechwycenie na skutek zjawiska interferencji U
  - Zdalne szpiegowanie U
  - Podsłuchanie U
  - Kradzież nośników lub dokumentów U
  - Kradzież urządzeń U
  - Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników P,U
  - Ujawnienie P,U
  - Dane z niewiarygodnych źródeł P,U
  - Manipulowanie sprzętem U
  - Sfałszowanie oprogramowania P,U
  - Detekcja pozycji U

C. Przykłady typowych zagrożeń

- Awarie techniczne
  - Awaria urządzenia P
  - Niewłaściwe funkcjonowanie urządzenia P
  - Przeciążenie systemu informacyjnego P,U
  - Niewłaściwe funkcjonowanie oprogramowania P
  - Naruszenie zdolności utrzymania systemu informacyjnego P,U
- Nieautoryzowane działania
  - Nieautoryzowane użycie urządzeń U
  - Nieuprawnione kopiowanie oprogramowania U
  - Używanie fałszywego lub skopiowanego oprogramowania P,U
  - zniekształcenie danych U
  - Nielegalne przetwarzanie danych U

C. Przykłady typowych zagrożeń

- Naruszenie bezpieczeństwa funkcji
  - Błąd użytkowania P
  - Naruszenie praw P,U
  - Zabieranie praw U
  - Odmowa działania U
  - Naruszenie dostępności personelu N,P,U

C. Przykłady typowych zagrożeń

- **Źródła zagrożeń ludzkich**
  - **Haker, craker**
    - **motywacja**
      - Wyzwanie
      - Ego
      - Rebelia
      - Status
      - Pieniądze
    - **Potencjalne skutki**
      - Hacking
      - Inżynieria społeczna
      - Wtargnięcie do systemu, włamanie
      - Nieautoryzowany dostęp

C. Przykłady typowych zagrożeń

- **Przestępca komputerowy**
  - **Motywacja**
    - **Zniszczenie informacji**
    - **Nielegalne ujawnienie informacji**
    - **Korzyść finansowa**
    - **Nieautoryzowana zmiana danych**
  - **skutki**
    - **Przestępstwa komputerowe**
    - **Czyn przestępczy (np. powtórne odtworzenie, podszycie się, przechwycenie)**
    - **Przekupstwo informacyjne**
    - **Spoofing (sfałszowanie adresu źródłowego)**
    - **Wtargnięcie do systemu**

C. Przykłady typowych zagrożeń

- **Terrorysta**
  - **Motywacja**
    - **Szantaż**
    - **Zniszczenie**
    - **Wykorzystanie**
    - **Korzyści polityczne**
    - **Rozgłos medialny**
  - **skutki**
    - **Bomba / terroryzm**
    - **Wojna informacyjna**
    - **Atak na system**
    - **Penetracja systemu**
    - **Naruszanie bezpieczeństwa systemu**

C. Przykłady typowych zagrożeń

- **Szpiedzy przemysłowi**
  - **Motywacja**
    - **Przewaga konkurencyjna**
    - **Szpiegostwo gospodarcze**
  - **skutki**
    - **Przewaga obronna**
    - **Przewaga polityczna**
    - **Wykorzystanie Ekonomiczna**
    - **Kradzież informacji**
    - **Naruszenie prywatności personelu**
    - **Inżynieria społeczna**
    - **Penetracja systemów**
    - **Nieautoryzowany dostęp**

C. Przykłady typowych zagrożeń

- **Pracownicy wewnątrz**
  - **motywacja**
    - Ciekawość
    - Ego
    - Szpiegostwo
    - Korzyść finansowa
    - Zemsta
    - Niezamierzone błędy i pomyłki

C. Przykłady typowych zagrożeń

- **skutki**
  - Napaść na pracownika
  - Szantaż
  - Przeglądanie własności intelektualnej
  - Oszustwa i kradzież
  - Przekupstwo informacyjna
  - Wprowadzanie fałszywych, zniekształconych danych
  - Przechwycenie
  - Złośliwy kod
  - Sprzedaż danych osobowych
  - Błędy w systemie
  - Wtargnięcie do systemów
  - Sabotaż systemów
  - Nieautoryzowany dostęp do systemu

D.1. Przykładowe podatności

- **Sprzęt**
  - **Niewystarczająca utrzymanie/ wadliwa instalacja nośników**
  - **Brak planów okresowej wymiany**
  - **Podatność na wilgotność, kurz, zabrudzenie**
  - **Wrażliwość na promieniowanie elektromagnetyczne**
  - **Brak skutecznej kontroli zmian w konfiguracji**
  - **Podatność na zmiany napięcia**
  - **Podatność na zmiany temperatury**
  - **Niezabezpieczone przechowywanie**
  - **Brak staranności przy pozbywaniu się nośników**
  - **Niekontrolowane kopiowanie**

D.1. Przykładowe podatności

- **Oprogramowanie**
  - **Brak lub niedostateczne testowanie oprogramowania**
  - **Dobrze znane wady oprogramowania**
  - **Brak wylogowywania się po opuszczeniu stacji roboczej**
  - **Usuwanie lub ponowne używanie nośników bez odpowiedniego kasowania ich zawartości**
  - **Brak śladu audytowego**
  - **Błędne przypisanie praw dostępu**
  - **Szerokie dystrybuowanie oprogramowania**
  - **Zastosowanie programów aplikacyjnych do nieaktualnych danych**
  - **Skomplikowany interfejs użytkownika**
  - **Brak dokumentacji**
  - **Nieprawidłowe ustawienie parametrów**
  - **Niepoprawne daty**

D.1 Przykładowe podatności

- Brak mechanizmów identyfikacji i uwierzytelniania takich jak uwierzytelnianie użytkowników
- Niezabezpieczone tablice haseł
- Słabe zarządzanie hasłami
- Niepotrzebne usługi dostępne
- Niedojrzałość nowego oprogramowania
- Niejasny lub niekompletne specyfikacje dla projektantów
- Brak skutecznej kontroli zmian
- Niekontrolowane ściąganie i używania oprogramowania
- Brak kopii zapasowych
- Brak fizycznej ochrony budynku, drzwi i okien
- Błędy tworzenia raportów dla kierownictwa

D.1 Przykładowe podatności

❑ Sieć
- Brak dowodu wysłania lub odebrania wiadomości
- Niezabezpieczone linie telekomunikacyjne
- Niechroniony wrażliwy ruch
- Złe łączenie kabli
- Pojedynczy punkt uszkodzenia
- Brak identyfikacji i uwierzytelniania nadawcy i odbiorcy
- Niebezpieczna architektura sieci
- Przesyłanie haseł w postaci jawnej
- Nieodpowiednie zarządzanie siecią
- Niezabezpieczone połączenia do sieci publicznej

D.1 Przykładowe podatności

❑ Personel
- Nieobecność personelu
- Nieodpowiednie procedury zatrudniania
- Niewystarczające szkolenia z bezpieczeństwa
- Niewłaściwe użycie oprogramowania i sprzętu
- Brak świadomości bezpieczeństwa
- Brak mechanizmów monitorowania
- Praca personelu zewnętrznego lub sprzątającego bez nadzoru
- Brak polityk w zakresie poprawnego użycia środków łączności i komunikowania się

D.1 Przykładowe podatności

❑ Lokalizacja
- Niewłaściwe lub nieuważne użycie fizycznej kontroli dostępu do budynków, pomieszczeń
- Lokalizacja na terenie zagrożonym powodzią
- Niestabilna sieć elektryczna
- Brak fizycznej ochrony budynku, drzwi i okien

D.1 Przykładowe podatności

- **Organizacja**
  - Brak formalnych procedur rejestracji i wyrejestrowania użytkownika
  - Brak formalnych procesów przeglądu praw dostępu (nadzór)
  - Brak lub niewystarczające zapisy (odnoszące się do bezpieczeństwa) w umowach z klientami i/lub trzecią stroną
  - Brak procedur monitorowania urządzeń przetwarzających informacje
  - Brak regularnych audytów (nadzór)
  - Brak procedur identyfikowania i szacowania ryzyka
  - Brak raportowania błędów rejestrowanych w dziennikach administratorów i operatorów
  - Nieodpowiednia reakcja utrzymania serwisowego
  - Brak lub niewystarczający SLA

D.1 Przykładowe podatności

- Brak procedury kontroli zmian
- Brak formalnych procedur nadzoru nad dokumentacją SZBI
- Brak formalnych procedur nadzoru zapisów SZBI
- Brak formalnego procesu autoryzacji informacji publicznie dostępnych
- Brak właściwego przypisania zakresu odpowiedzialności za bezpieczeństwo informacji
- Brak planów ciągłości działania
- Brak polityki korzystania z poczty elektronicznej
- Brak procedur instalowania oprogramowania w systemach produkcyjnych
- Brak zapisów w dziennikach administratora i operatora
- Brak procedur dla przetwarzania informacji klasyfikowanych i
- Brak odpowiedzialności związanej z bezpieczeństwem informacji w zakresach obowiązków

D.1 Przykładowe podatności

- Brak lub niewystarczające zapisy (odnoszące się do bezpieczeństwa) w umowach z pracownikami
- Brak zdefiniowanego postępowania dyscyplinarnego w przypadku incydentu związanego z bezpieczeństwem informacji
- Brak formalnej polityki używania komputerów przenośnych
- Brak nadzoru nad aktywami znajdującymi się poza siedzibą
- Brak lub niewystarczająca polityka czystego biurka i czystego ekranu
- Brak autoryzacji środków przetwarzania informacji
- Brak ustanowionego mechanizmu monitorowania naruszeń bezpieczeństwa
- Brak regularnych przeglądów realizowanych przez kierownictwo
- Brak procedur raportowania o słabościach bezpieczeństwa
- Brak procedur zapewniających zgodność z prawami własności intelektualnej

D.2.Metody szacowania podatności technicznej

- **Metody aktywne**
  - Zautomatyzowane narzędzia skanujące podatności
  - Testowanie i ocena bezpieczeństwa
  - Testy penetracyjne
  - Przeglądy kodu
- **Działania**
  - Wywiady z osobami i użytkownikami
  - Ankiety
  - Inspekcja fizyczna
  - Analiza dokumentów

E.1 Metody analizy ryzyka wysokiego poziomu

- *ilościowe*
  - najczęściej oznacza analizę ryzyka i oszacowanie
  - wspomagające matematyczne obliczenia wpływu zagrożenia, częstotliwości i prawdopodobieństwa
  - operuje wyłącznie na danych numerycznych,
  - bierze pod uwagę
  - dane historyczne i statystyczne.
- *jakościowe*
  - polega na prowadzeniu rankingu zagrożeń i zasobów.
  - Bazuje na wiedzy i ocenie osób dokonujących analizy.
  - Wynik jest najczęściej opisowy, lecz można później, dokonać przełożenia słów na cyfry.
  - Podejście jest znacznie prostsze do stosowania pod warunkiem ustalenia granic dla kryteriów.

E. Podejścia do szacowania ryzyka związanego z bezpieczeństwem informacji

- E.1 Ogólne szacowanie ryzyka związanego z bezpieczeństwem informacji
- E.2. Szczegółowe metody szacowania ryzyka
  - E.2.1 Macierz z predefiniowanymi wartościami
  - E.2.2. Ranking zagrożeń poprzez pomiar ryzyka
  - E.2.3. Określenie wartości prawdopodobieństwa i możliwych skutków ryzyka

F. Ograniczenia przy redukowaniu ryzyka

- Czasowe
- Finansowe
- Techniczne
- Operacyjne
- Kulturowe
- Etyczne
- Środowiskowe
- Prawne
- Łatwość użytkowania
- Dotyczące Personelu
- Integracji nowych i istniejących zabezpieczeń