Elementy wymagań ISO/IEC 27001 i zalecenia ISO/IEC 17799 organizacyjne

dr inż. Bolesław Szomański

bolkosz@wsisiz.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*)**

5 - Polityka bezpieczeństwa (1)

A.5.1. Polityka bezpieczeństwa

Cel*: Zapewnienie, że kierownictwo wspiera i kieruje bezpieczeństwem informacji zgodnie z wymaganiami biznesowymi i właściwymi przepisami prawa oraz regulacjami wewnętrznymi*

- ***A.5.1.1 Dokument polityki bezpieczeństwa informacji***
  - **Dokument polityki powinien zostać**
  - **zatwierdzony przez kierownictwo,**
  - **opublikowany i**
  - **udostępniony wszystkim pracownikom i**
  - **właściwym stronom zewnętrznym**

5 - Polityka bezpieczeństwa (2)

- **Dokument polityki bezpieczeństwa informacji**
  - **powinien zawierać co najmniej:**
    - **definicję bezpieczeństwa informacji,**
      - **jej ogólne cele i**
        - zakres oraz
      - **znaczenie bezpieczeństwa dla współużytkowania informacji**
    - **oświadczenie o intencjach kierownictwa,**
      - **potwierdzające cele i zasady bezpieczeństwa informacji**
        - w odniesieniu do
      - **strategii i**
      - **wymagań biznesowych;**
    - **strukturę wyznaczania celów**
      - **stosowania zabezpieczeń i zabezpieczeń,**
        - w tym
      - **strukturę**
        - szacowania i
        - **zarządzania ryzykiem**;

5 - Polityka bezpieczeństwa (2a)

- **krótkie wyjaśnienie polityki bezpieczeństwa,**
  - **zasad,**
  - **standardów i**
  - **wymagań zgodności**
    - mających szczególne znaczenie dla organizacji:
  - **zgodność z**
    - **prawem**,
    - regulacjami i
    - wymaganiami wynikającymi z umów;
  - **wymagania dotyczące**
    - **kształcenia**,
    - szkoleń i
    - uświadamiania w dziedzinie bezpieczeństwa;
  - **zarządzanie ciągłością działania biznesowego;**
  - **konsekwencje naruszenia polityki bezpieczeństwa**

5 - Polityka bezpieczeństwa (3)

- **definicje**
  - **ogólnych i**
  - **szczególnych obowiązków**
    - w odniesieniu do zarządzania bezpieczeństwem informacji,
  - **w tym zgłaszania przypadków naruszenia bezpieczeństwa;**
- **odsyłacze do dokumentacji mogącej uzupełniać politykę, np.**
  - **bardziej szczegółowych polityk bezpieczeństwa i**
  - **procedur dotyczących poszczególnych systemów informatycznych lub**
  - **zalecanych do przestrzegania przez użytkowników zasad bezpieczeństwa.**

5 - Polityka bezpieczeństwa (4)

- ***A.5.1.2. Przegląd i ocena polityki bezpieczeństwa informacji***
  - **Polityka bezpieczeństwa**
    - **powinna być poddawana**
  - **regularnemu przeglądowi,**
    - **a w przypadku istotnych zmian**
  - **powinna zapewniać, że pozostaje**
    - **przydatna,**
    - **adekwatna i**
    - **skuteczna**

5 - Polityka bezpieczeństwa (5)

- **Zaleca się żeby polityka miała właściciela o zatwierdzonych przez kierownictwo uprawnieniach**
- **Zaleca się, aby przegląd obejmował**
  - **Zbadanie możliwości udoskonalenia**
    - **polityki bezpieczeństwa informacji w organizacji**
      - oraz
    - **podejścia do**
      - **zarządzania** bezpieczeństwem informacji
      - uwzględniających
    - **zmiany**
      - środowiska organizacyjnego,
      - warunków biznesowych,
      - prawnych lub
      - środowiska technicznego.

5 - Polityka bezpieczeństwa (6)

- Zaleca się, aby
  - przegląd polityki bezpieczeństwa informacji
  - brał pod uwagę wyniki przeglądów realizowanych przez kierownictwo.
- Zaleca się opracowanie
  - procedur przeglądów realizowanych przez kierownictwo
    - zawierających
      - harmonogram lub
      - częstość przeglądów.

5 - Polityka bezpieczeństwa (7)

- Zalecane dane wejściowe do przeglądu
  - informacje zwrotne od zainteresowanych stron;
  - wyniki niezależnych przeglądów (patrz 6.1.8);
  - stan
    - działań zapobiegawczych i
    - korygujących (patrz 6.1.8 i 15.2.1);
  - wyniki poprzednich przeglądów
    - realizowanych przez kierownictwo;
  - wydajność procesów i
    - zgodność polityki bezpieczeństwa informacji;
  - zmiany,
    - które mogą wpłynąć na podejście organizacji do zarządzania bezpieczeństwem informacji,
      - w tym
    - środowiska organizacyjnego,
    - warunków biznesowych,

5 - Polityka bezpieczeństwa (7)

    - dostępności zasobów,
    - zobowiązań kontraktowych,
    - regulacji i
    - warunków prawnych lub
    - środowiska technicznego;
  - informacje dotyczące trendów
    - związanych z
    - zagrożeniami i
    - podatnościami;
  - informacje dotyczące
    - zgłoszonych incydentów naruszenia bezpieczeństwa informacji (patrz 13.1);
  - rekomendacje wydane przez właściwe organy (patrz 6.1.6).

5 - Polityka bezpieczeństwa (8)

- Zaleca się aby
  - dane wyjściowe zawierały wszelkie
  - decyzje i
  - działania związane z:
    - doskonaleniem podejścia organizacji
      - do zarządzania bezpieczeństwem informacji i jego procesów;
    - doskonaleniem celów stosowania zabezpieczeń i zabezpieczeń;
    - doskonaleniem w odniesieniu do
      - przydzielania zasobów lub
      - odpowiedzialności;
- Zaleca się
  - prowadzenie zapisu przeglądów
    - realizowanych przez kierownictwo.
- Zaleca się, aby
  - wszelkie zmiany polityki były zatwierdzone przez kierownictwo.

6 - Organizacja bezpieczeństwa informacji (2)

6.1 – Organizacja wewnętrzna

- A.6.1. Cel: *Zarządzanie bezpieczeństwem informacji wewnątrz organizacji:*
- A.6.1.1 Zaangażowanie kierownictwa w bezpieczeństwo informacji
  - **Kierownictwo powinno aktywnie wspierać**
    - bezpieczeństwo w organizacji
    - **przez ustalenie wyraźnego kierunku,**
    - **demonstrowanie zaangażowania,**
    - **jednoznaczne przypisanie**
      - i przyjmowanie
    - **odpowiedzialności**
      - w zakresie bezpieczeństwa informacji. .

6 - Organizacja bezpieczeństwa informacji (3)

6.1 – Organizacja wewnętrzna

- **Zaleca się, aby kierownictwo:**
  - **zapewniało, że cele bezpieczeństwa informacji są**
    - **identyfikowane,**
    - **spełniają wymagania organizacji i są**
    - **włączone do odpowiednich procesów;**
  - **określało,**
    - **poddawało przeglądom i**
    - **zatwierdzało politykę bezpieczeństwa informacji;**
  - **poddawało przeglądom**
    - **skuteczność wdrażania polityki bezpieczeństwa informacji;**
  - **zapewniało klarowne**
    - **wskazania i**
    - **widoczne wsparcie dla**
    - **inicjatyw z zakresu bezpieczeństwa informacji;**
  - **zapewniało środki**
    - **potrzebne dla zapewnienia bezpieczeństwa informacji;**

Rozdział 6 - Organizacja bezpieczeństwa informacji (3a)

6.1 – Organizacja wewnętrzna

- **zatwierdzało w organizacji**
  - **poszczególne role i**
  - **odpowiedzialności**
    - związane z **bezpieczeństwem** informacji;
- **inicjowało**
  - **plany i**
  - **programy utrzymujące**
  - **właściwą świadomość**
    - problematyki bezpieczeństwa informacji;
- **zapewniało, że**
  - **wdrożenia zabezpieczeń informacji są**
  - **skoordynowane w całej organizacji (patrz 6.1.2).**

Rozdział 6 - Organizacja bezpieczeństwa informacji (4)

6.1 – Organizacja wewnętrzna

- **Zaleca się, aby kierownictwo**
  - **określiło potrzebę,**
    - wewnętrznego lub
    - zewnętrznego,
  - **Specjalistycznego doradztwa**
  - **z zakresu bezpieczeństwa informacji oraz**
    - dokonywało **przeglądów** i
    - koordynowało
      - *wyniki takiego* **doradztwa**
      - *w organizacji.* .

6 - Organizacja bezpieczeństwa informacji(4)
6.1 – Organizacja wewnętrzna

- *A.6.1.2. Koordynacja bezpieczeństwa informacji*
  - **Działania w zakresie bezpieczeństwa informacji**
    - powinny być
    - **koordynowane przez**
    - **reprezentantów**
      - różnych części organizacji
    - **pełniących odpowiednie**
      - role i
      - funkcje.

6 - Organizacja bezpieczeństwa informacji(4a)
6.1 – Organizacja wewnętrzna

- **Zazwyczaj koordynacja bezpieczeństwa informacji**
  - wymaga **współdziałania**:
  - **kierownictwa,**
  - **użytkowników,**
  - **administratorów,**
  - **projektantów aplikacji,**
  - **audytorów i**
  - **pracowników działu bezpieczeństwa oraz**
- **specjalistycznych umiejętności**
  - **z takich dziedzin, jak**
    - **ubezpieczenia**,
    - **prawo**,
    - **zarządzanie**
      - *zasobami* **ludzkimi**,
      - **informatyką** *lub*
      - **ryzykiem**.

6 - Organizacja bezpieczeństwa informacji (5)
6.1 – Organizacja wewnętrzna

Zaleca się, aby działania koordynacyjne:

- **zapewniały, że**
  - **zadania**
    - w zakresie bezpieczeństwa są
  - **realizowane zgodnie**
    - z polityką bezpieczeństwa informacji;
- **określały postępowanie z niezgodnościami;**
- **zatwierdzały**
  - **metodykę i**
  - **procesy**
    - związane z **bezpieczeństwem** informacji,
    - np. dla **klasyfikacji** informacji lub
    - **szacowania** ryzyka;

6 - Organizacja bezpieczeństwa informacji (5a)
6.1 – Organizacja wewnętrzna

- **określały znaczące**
  - **zmiany zagrożeń i**
  - **stopień narażenia informacji lub**
  - **środków służących**
    - do przetwarzania informacji na zagrożenia;
- **szacowały**
  - **adekwatność i**
  - **koordynowały wdrożenie zabezpieczeń;**
- **skutecznie**
  - **promowały w organizacji**
  - **kształcenie,**
  - **szkolenia i**
  - **uświadamianie w**
    - zakresie bezpieczeństwa informacji;

6 - Organizacja bezpieczeństwa informacji (5b)

6.1 – Organizacja wewnętrzna

- **oceniały**
  - informacje uzyskane z
  - **monitorowania i**
  - **przeglądu incydentów**
    - naruszenia bezpieczeństwa informacji oraz
  - **zalecały odpowiednie działania**
    - *w stosunku do*
    - zidentyfikowanych **incydentów**
      - *naruszenia bezpieczeństwa informacji.*

6 - Organizacja bezpieczeństwa informacji (6)

6.1 – Organizacja wewnętrzna

- ***A.6.1.3. Przydział odpowiedzialności w zakresie bezpieczeństwa informacji***
  - **Wszelka odpowiedzialność za bezpieczeństwo informacji**
    - **powinna być**
  - **wyraźnie zdefiniowana.**

6 - Organizacja bezpieczeństwa informacji (6)

6.1 – Organizacja wewnętrzna

- **Powiązanie**
  - **podziału funkcji i**
  - **odpowiedzialności z**
    - **polityką bezpieczeństwa**
- **Zaleca się, aby**
  - **odpowiedzialność**
    - **za ochronę indywidualnych aktywów i**
    - **realizację określonych procesów bezpieczeństwa była**
  - **wyraźnie zdefiniowana.**

6 - Organizacja bezpieczeństwa informacji (6)

6.1 – Organizacja wewnętrzna

- **Tam gdzie potrzebne**
  - **odpowiedzialność**
  - **dodatkowo wsparta wytycznymi**
- **Jasne określenie**
  - **lokalnych obowiązków związanych z**
  - **ochroną aktywów lub**
  - **działaniem określonych procesów bezpieczeństwa,**
    - **takich jak planowanie ciągłości działania.**
- **Osoby, którym**
  - **przypisano odpowiedzialność za bezpieczeństwo**
  - **mogą delegować do tych obowiązków inne osoby.**
    - **Jednakże,**
  - **pozostają one jednak**
  - **nadal odpowiedzialne i**

6 - Organizacja bezpieczeństwa informacji (8)

6.1 – Organizacja wewnętrzna

- zaleca się im weryfikację,
  - czy wszystkie
- delegowane zadania są wykonywane
- poprawnie.

❑ Zaleca się aby

- aktywa i
- procesy bezpieczeństwa związane z każdym systemem były
  - zidentyfikowane i
  - jasno zdefiniowane;
- dla każdego aktywu lub
- procesu bezpieczeństwa był
- wyznaczony podmiot za nie odpowiedzialny oraz
- szczegóły tej odpowiedzialności były udokumentowane;
- poziomy uprawnień były wyraźnie
  - określone i
  - udokumentowane.

6 - Organizacja bezpieczeństwa informacji (9)

6.1 – Organizacja wewnętrzna

❑ *A.6.1.4 Proces autoryzacji urządzeń służących do przetwarzania informacji*

❖ Powinien zostać

❖ zdefiniowany

❖ i wdrożony

❖ Proces autoryzacji

❖ Przez Kierownictwo

- nowych środków
  - *służących*
- do przetwarzania informacji.

6 - Organizacja bezpieczeństwa informacji (9)

6.1 – Organizacja wewnętrzna

❑ Odpowiednie dopuszczenia

- powinny być potwierdzone przez
- kierownictwo sankcjonujące przeznaczenie i sposób użycia

❑ Zapewniające

- zgodność z innymi komponentami systemu

❑ Zasady używanie osobistych (prywatnych) urządzeń

6 - Organizacja bezpieczeństwa informacji (10)

6.1 – Organizacja wewnętrzna

❑ *A.6.1.5. Umowy o zachowaniu poufności*

❖ Wymagania

- dla umów o zachowaniu poufności i
  - nie ujawnianiu informacji
- odzwierciedlające potrzeby organizacji
  - w zakresie ochrony informacji powinny być
- określone i
- regularnie przeglądane

6 - Organizacja bezpieczeństwa informacji (10a)

6.1 – Organizacja wewnętrzna

- **Zaleca się aby umowy były sformułowane w sposób**
  - **prawnie skuteczny i**
  - **uwzględniały następujące elementy**
    - **definicję informacji, która ma być chroniona (np. informacja wrażliwa);**
    - **spodziewany czasu trwania umowy, włączając w to przypadki, w których obowiązek zachowania poufności może być bezterminowy;**
    - **wymagane działania, w momencie zakończenia umowy;**
    - **odpowiedzialności i działania podpisujących podejmowane**
      - w celu **uniknięcia nieupoważnionego** ujawnienia informacji;

6 - Organizacja bezpieczeństwa informacji (11)

6.1 – Organizacja wewnętrzna

- **własności informacji,**
  - **tajemnic przemysłowych i**
  - **własności intelektualnej oraz**
  - **w jaki sposób odnosi się to do ochrony informacji wrażliwej;**
- **dozwolonego użycia wrażliwej informacji oraz**
  - **praw podpisującego do jej użycia;**
- **prawa do audytu i**
  - **monitorowania działań związanych z**
  - **informacją wrażliwą;**
- **procesu powiadamiania i**
  - **raportowania**
  - **nieuprawnionego ujawnienia lub**
  - **przełamania poufności informacji;**
- **zasad zwrotu i**
  - **niszczenia informacji**
  - **przy zakończeniu umowy;**

6 - Organizacja bezpieczeństwa informacji(12)

6.1 – Organizacja wewnętrzna

- **działań podejmowanych**
  - **w przypadku naruszenia warunków umowy.**

- **Mogą być dodane inne elementy**
- **Zaleca się, aby**
  - **umowy o zachowaniu poufności i**
    - **nieujawnianiu informacji były**
  - **zgodne z odpowiednimi**
  - **przepisami prawa i regulacjami (patrz 15.1.1).**
- **Zaleca się aby**
  - **umowy były przeglądane**
  - **jeżeli zmieniają się warunki zatrudnienia**

6 - Organizacja bezpieczeństwa informacji(12)

6.1 – Organizacja wewnętrzna

- **A.6.1.6. Kontakty z organami władzy**
  - **Powinny być**
  - **utrzymywane**
  - **właściwe kontakty**
  - **z organami władzy**

6 - Organizacja bezpieczeństwa informacji (14)
6.1 – Organizacja wewnętrzna

- Zalecenie opracowanie
  - procedury dla kontaktów z
    - organami ścigania,
    - strażą pożarną,
    - organami regulacyjnymi i
    - nadzorującymi
  - Oraz
- jak, i w
  - jakim czasie należy
  - informować o zidentyfikowanych incydentach naruszenia bezpieczeństwa informacji,
    - jeśli zachodzi podejrzenie złamania prawa.
- Atakowane z internetu organizacje
  - mogą potrzebować odpowiedniego wsparcia np.
  - od operatorów telekomunikacyjnych lub
  - dostawców usług internetowych

6 - Organizacja bezpieczeństwa informacji (15)
6.1 – Organizacja wewnętrzna

- **A. 6.1.7. Kontakty z grupami zainteresowania bezpieczeństwem**
  - **Powinno się utrzymywać**
    - **kontakty z**
    - **grupami zainteresowania bezpieczeństwem,**
    - **specjalistycznymi forami związanymi z bezpieczeństwem**
      - oraz
    - **profesjonalnymi stowarzyszeniami**

6 - Organizacja bezpieczeństwa informacji (15)
6.1 – Organizacja wewnętrzna

- **Zaleca się rozważyć kontakty z grupami w celu:**
  - **poszerzania i**
  - **aktualizacji wiedzy na temat**
  - **najlepszych praktyk bezpieczeństwa informacji;**
  - **zapewnienia, że**
    - **zrozumienie środowiska bezpieczeństwa informacji jest**
      - **aktualne** i
      - **kompletne**;

6 - Organizacja bezpieczeństwa informacji (16)
6.1 – Organizacja wewnętrzna

- **otrzymywania wczesnych ostrzeżeń,**
  - **porad i**
  - **łat odnoszących się do**
    - ataków i
    - podatności;
- **uzyskania dostępu do**
  - **specjalistycznego doradztwa z zakresu bezpieczeństwa informacji;**
- **wymiany informacji o**
  - **nowych technologiach,**
  - **produktach,**
  - **zagrożeniach i**
  - **podatnościach;**
- **zapewnienia odpowiednich kontaktów**
  - **w przypadku postępowania z incydentami naruszenia bezpieczeństwa (patrz także 13.2.1).**

6 - Organizacja bezpieczeństwa informacji (17)
6.1 – Organizacja wewnętrzna

- *A.6.1.8. Niezależne przeglądy bezpieczeństwa informacji*
  - **Podejście do zarządzania bezpieczeństwem informacji**
    - **oraz jego realizacji**
      - (tzn. cele stosowania zabezpieczeń,
      - zabezpieczenia,
      - polityki,
      - procesy i
      - procedury bezpieczeństwa informacji)
  - **powinny być poddawane**
  - **niezależnym przeglądom w**
    - **zaplanowanych odstępach czasu**
    - **lub wtedy, gdy wystąpiły w nich znaczące zmiany.**

6 - Organizacja bezpieczeństwa informacji (17)
6.1 – Organizacja wewnętrzna

- **Zaleca się, aby niezależny przegląd był**
  - **inicjowany przez kierownictwo.**
  - **Taki niezależny przegląd jest potrzebny, aby zapewnić, że**
    - **podejście organizacji do zarządzania bezpieczeństwem informacji jest ciągle**
      - przydatne,
      - adekwatne i
      - skuteczne.
- **Zaleca się, aby przegląd obejmował ocenę możliwości udoskonalenia**
  - **oraz potrzeby zmian podejścia do bezpieczeństwa, włączając w to polityki i cele stosowania zabezpieczeń.**

6 - Organizacja bezpieczeństwa informacji (18)
6.1 – Organizacja wewnętrzna

- **Przegląd może być wykonywany np. przez**
  - **Komórkę audytu wewnętrznego**
  - **Niezależnego kierownika**
  - **Zewnętrzną organizację specjalizującą się w dokonywaniu takich przeglądów**
    - **Osoby sprawdzające mają odpowiednie**
  - **Umiejętności**
  - **Doświadczenie**
- **Zaleca się**
  - **przechowywanie wyników i**
  - **podjęcia działań korygujących**
  - **jeśli będzie to wskazane przez przegląd**

6 - Organizacja bezpieczeństwa informacji (19)
6.2 – Zewnętrzne strony

- A.6.2. *Cel: Utrzymanie bezpieczeństwa informacji*
  - *należących do organizacji oraz*
  - *środków przetwarzania informacji,*
    - *do których mają dostęp,*
    - *Za pomocą których*
    - *przetwarzają,*
    - *komunikują się*
      - ***lub którymi***
    - *zarządzają strony zewnętrzne.*

6 - Organizacja bezpieczeństwa informacji (19)
6.2 – Zewnętrzne strony

- A.6.2.1. *Określenie ryzyk związanych ze stronami zewnętrznymi*
  - Ryzyka
    - dla informacji należącej do organizacji i
      - **środków służących do przetwarzania informacji**
    - związanych ze stronami zewnętrznymi oraz
    - wdrożenie odpowiednich zabezpieczeń
    - Powinno być zdefiniowane
      - **przed przyznaniem dostępu tym stronom.**

6. Organizacja bezpieczeństwa informacji (20)
6.2 – Zewnętrzne strony

- **Przy identyfikacji ryzyk**
  - **związanych z dostępem stron zewnętrznych**
  - **zaleca się wziąć pod uwagę:**
  - **środki służące do przetwarzania informacji, do których**
    - **ma być zrealizowany dostęp strony zewnętrznej;**
  - **sposób dostępu strony zewnętrznej do informacji i środków służących do przetwarzania informacji, np.:**
    - **dostęp fizyczny, np. wstęp do biur, sal komputerowych, szaf na akta;**
    - **dostęp logiczny, np. do baz danych organizacji, systemów informacyjnych;**
    - **połączenia między sieciami organizacji i stron zewnętrznych, np. połączenia stałe, dostęp zdalny;**
    - **czy jest to dostęp lokalny, czy poza lokalizacją organizacji;**
  - **wartość i wrażliwość udostępnianej informacji oraz**
    - **jej krytyczność dla procesów biznesowych;**
  - **zabezpieczenia potrzebne do ochrony informacji,**
    - **która ma nie być dostępna dla strony zewnętrznej;**

6. Organizacja bezpieczeństwa informacji (21)
6.2 – Zewnętrzne strony

- **personel strony zewnętrznej**
  - **zaangażowany w obsługę informacji należącej do organizacji;**
  - **przekazywania,**
  - **współdzielenia i**
  - **wymiany informacji;**
- **skutki braku dostępu strony trzeciej,**
  - **gdy jest on wymagany, oraz**
  - **wprowadzania lub otrzymywania niepoprawnych lub wprowadzających w błąd informacji;**
- **praktyki i procedury**
  - **obsługi incydentów naruszenia bezpieczeństwa informacji i potencjalnych szkód**
  - **oraz zasady i warunki utrzymania ciągłości dostępu stron zewnętrznych**
    - na wypadek wystąpienia **incydentu** naruszenia bezpieczeństwa informacji;

6. Organizacja bezpieczeństwa informacji (21a)
6.2 – Zewnętrzne strony

- **wymagania prawne,**
  - **regulacje oraz**
  - **inne zobowiązania kontraktowe,**
    - właściwe dla strony zewnętrznej, które
    - zaleca się wziąć pod uwagę;
- **Sposób, w jaki ustalenia mogą wpłynąć na**
  - **interesy właścicieli.**

Zaleca się, aby
  - **dostęp stron zewnętrznych do informacji należącej do organizacji**
- **był zabroniony do momentu**
- **wdrożenia odpowiednich zabezpieczeń oraz**
  - **podpisania umowy**
    - określającą **zasady** i
    - warunki **połączenia** lub
    - **dostępu** oraz
    - tryby **współpracy**.

6. Organizacja bezpieczeństwa informacji (22)
6.2 – Zewnętrzne strony

- **wymagania bezpieczeństwa oraz**
  - **zabezpieczenia lokalne wynikające**
    - **ze współpracy ze stroną zewnętrzną**
  - **były odzwierciedlone w umowie (patrz 6.2.2 i 6.2.3).**
- **Należy upewnić się, że strona zewnętrzna jest**
  - **świadoma swoich zobowiązań,**
  - **akceptuje odpowiedzialności i**
    - **zobowiązania związane z**
      - dostępem,
      - przetwarzaniem,
      - przekazywaniem lub
      - zarządzaniem **informacją**
    - **należącą do organizacji lub**
    - **środkami służącymi do przetwarzania informacji.**

6. Organizacja bezpieczeństwa informacji (23)
6.2 – Zewnętrzne strony

- **6.2.2. Bezpieczeństwo w kontaktach z klientami**
  - **Wszystkie zidentyfikowane**
  - **wymagania bezpieczeństwa**
    - **powinny zostać wprowadzone**
      - przed przyznaniem klientom
        - *dostępu do informacji lub*
        - *aktywów należących do organizacji*.

6. Organizacja bezpieczeństwa informacji (23)
6.2 – Zewnętrzne strony

- **Zaleca się uwzględnienie**
  - **następujących zasad,**
    - **odnoszących się do bezpieczeństwa,**
    - **przed przyznaniem klientom dostępu do**
      - jakichkolwiek aktywów organizacji:
    - **ochrony aktywów, w tym:**
      - procedury **ochrony aktywów** organizacji,
        - *w tym* **informacji** *i*
        - **oprogramowania***, oraz*
        - **zarządzania** *znanymi* **podatnościami***;*

6. Organizacja bezpieczeństwa informacji (23a)
6.2 – Zewnętrzne strony

- **procedury**
  - **wykrywania naruszenia** aktywów, tzn.
    - **utraty** *lub*
    - **modyfikacji** *danych;*
- **integralność;**
- **ograniczenia**
  - **kopiowania** i
  - **ujawniania** informacji;

6. Organizacja bezpieczeństwa informacji (24)
6.2 – Zewnętrzne strony

- **opisu dostarczanego produktu lub usługi;**
- **różnych przyczyn,**
  - **wymagań i**
  - **korzyści wynikających z dostępu klientów;**
- **polityki kontroli dostępu, w tym:**
  - **dozwolone metody dostępu oraz**
    - kontroli i korzystania z unikalnych identyfikatorów, takich jak
    - identyfikator i hasło użytkownika;
  - **proces autoryzacji**
    - praw dostępu i
    - przywilejów dla użytkownika;
  - **stwierdzenie, że jeśli**
    - jakikolwiek dostęp **nie został jawnie** przyznany,
    - to **jest zabroniony**;
  - **proces odbierania**
    - **praw dostępu** lub
    - przerywania **połączeń** pomiędzy systemami;

6. Organizacja bezpieczeństwa informacji (24a)
6.2 – Zewnętrzne strony

- **ustalenia dotyczące**
  - **raportowania,**
  - **zawiadamiania i**
  - **śledzenia nieścisłości informacji**
    - (np. szczegółów danych osobowych),
  - **incydentów naruszenia bezpieczeństwa informacji oraz**
  - **naruszeń bezpieczeństwa;**

6. Organizacja bezpieczeństwa informacji (25)
6.2 – Zewnętrzne strony

- **opis każdej udostępnianej usługi;**
- **docelowy poziom usług i**
  - **nieakceptowalny poziom usług;**
- **prawo do monitorowania i**
  - **zablokowania wszelkich działań związanych z aktywami organizacji;**
- **odpowiedzialność organizacji i klienta;**
- **odpowiedzialność wynikająca z przepisów prawa oraz**
  - **sposoby zapewniania, że wymagania prawne są spełniane,**
    - np. prawo ochrony **danych osobowych**,
- **prawo do własności intelektualnej i**
  - **prawo autorskie (patrz 15.1.2) oraz**
  - **ochrona wspólnej pracy (patrz 6.1.5).**

6. Organizacja bezpieczeństwa informacji (26)
6.2 – Zewnętrzne strony

- **A.6.2.3. Wymagania bezpieczeństwa w umowach ze stroną trzecią**
  - **Umowy ze stronami trzecim dotyczące**
    - **dostępu,**
    - **przetwarzania,**
    - **przekazywania lub**
    - **zarządzania**
      - informacją lub
      - środkami służącymi do przetwarzania informacji,
    - **organizacji lub**
    - **dodania produktów lub**
      - usług do środków służących do przetwarzania informacji,
    - **powinny być obejmować wszystkie**
      - stosowne wymagania bezpieczeństwa.

6. Organizacja bezpieczeństwa informacji (26)
6.2 – Zewnętrzne strony

- **Zaleca się, aby**
  - **umowa zapewniała, że**
  - **nie ma żadnych nieporozumień**
    - **pomiędzy organizacją i**
    - **stroną trzecią.**
- **Zaleca się włączenie**
  - **klauzul odpowiedzialności odszkodowawczej**
  - **od strony trzeciej.**
- **Zaleca się, aby włączyć do umowie następujące zagadnienia:**
  - **polityki bezpieczeństwa informacji;**

6. Organizacja bezpieczeństwa informacji (27)
6.2 – Zewnętrzne strony

- **zabezpieczeń chroniących aktywa, w tym:**
  - **procedury ochrony aktywów organizacji,**
    - w tym informacji, oprogramowania i sprzętu;
  - **wszelkie wymagane zabezpieczenia i**
    - mechanizmy ochrony fizycznej;
  - **zabezpieczenia chroniące przed złośliwym oprogramowaniem (patrz 10.4.1);**
  - **procedury wykrywania naruszenia aktywów,**
    - tzn. utraty lub modyfikacji danych, oprogramowania lub sprzętu;
  - **zabezpieczenia zapewniające zwrot lub**
    - **niszczenie** informacji i aktywów
    - w chwili **zakończenia** umowy lub w innym uzgodnionym w umowie czasie;
  - **poufność, integralność, dostępność oraz**
    - wszystkie inne odpowiednie własności aktywów (patrz 2.1.5);
  - **ograniczenia kopiowania i ujawniania informacji oraz**
    - korzystania z umów **poufności** (patrz 6.1.5);

6. Organizacja bezpieczeństwa informacji (28)
6.2 – Zewnętrzne strony

- **szkolenia dla użytkowników i administratorów**
  - **w zakresie metod, procedur i bezpieczeństwa;**
- **zapewnienia świadomości użytkowników**
  - **w zakresie ich odpowiedzialności za**
    - bezpieczeństwo informacji oraz
    - inne sprawy z tym związane;
- **zabezpieczenia na wypadek**
  - **przenosin personelu**
  - **wszędzie, gdzie należy to wziąć pod uwagę;**
- **odpowiedzialności związane z**
  - **instalacją i utrzymaniem oprogramowania i sprzętu;**
- **jasnej struktury raportowania oraz**
  - **uzgodnionych formularzy raportów;**
- **określonego i**
  - **jasnego procesu**
  - **zarządzania zmianami;**

6. Organizacja bezpieczeństwa informacji (29)
6.2 – Zewnętrzne strony

- **polityki kontroli dostępu, obejmującej:**
  - **różne przyczyny,**
    - **wymagania i**
    - **korzyści określające potrzebę udzielenia dostępu stronie trzeciej;**
  - **dozwolone metody dostępu,**
    - **zabezpieczenia oraz**
    - **korzystanie z unikalnych identyfikatorów takich jak**
      - identyfikator i hasło użytkownika;
  - **proces autoryzacji dostępu i**
    - **przywilejów dla użytkowników;**
  - **wymaganie prowadzenia**
    - **listy osób uprawnionych do korzystania z udostępnianych usług**
      - wraz z ich prawami;
  - **stwierdzenie, że**
    - **jeśli jakikolwiek dostęp nie został jawnie przyznany,**
    - **to jest zabroniony;**

6. Organizacja bezpieczeństwa informacji (29)
6.2 – Zewnętrzne strony

- wymagania prawne są spełniane,
  - np. prawo ochrony danych osobowych,
- proces odbierania uprawnień lub
  - przerywania połączeń pomiędzy systemami;
- planów
  - raportowania,
  - zawiadamiania i
  - śledzenia
  - incydentów naruszenia bezpieczeństwa informacji oraz
  - naruszeń bezpieczeństwa jak również
  - naruszeń wymagań określonych w umowie;
- opisu dostarczanych produktów lub
  - usług oraz
  - opisu udostępnianej informacji wraz z
  - jej klasyfikacją bezpieczeństwa (patrz 7.2.1);
- docelowego poziomu usług i
  - nieakceptowalnego poziomu usług;

6.0 Organizacja bezpieczeństwa informacji (30)
6.2 – Zewnętrzne strony

- określenia weryfikowalnych kryteriów wykonania,
  - ich monitorowania i
  - raportowania;
- prawa do monitorowania i
  - zablokowania wszelkich działań związanych z aktywami organizacji;
- prawa do przeprowadzenia audytów
  - odpowiedzialności określonych w umowie,
  - zlecania tych czynności stronie trzeciej,
  - określenia praw audytorów;
- ustanowienia procesu eskalacji dla rozwiązywania problemów;
- wymagań dla ciągłości usług,
  - w tym pomiaru ich dostępności i niezawodności w powiązaniu
  - z potrzebami biznesowymi organizacji;
- odpowiedzialności stron umowy;
- odpowiedzialność wynikająca
  - z przepisów prawa oraz
  - sposoby zapewniania, że jest przestrzegana

6. Organizacja bezpieczeństwa informacji (31)
6.2 – Zewnętrzne strony

- prawo do własności intelektualnej i
  - prawo autorskie (patrz 15.1.2) oraz
  - ochrona wspólnej pracy (patrz 6.1.5).
- zasad współpracy strony trzeciej
  - z podwykonawcami oraz
    - zabezpieczeń, jakie
    - podwykonawcy mają wdrożyć;
- warunki renegocjacji lub zakończenia umowy:
  - zaleca się przygotowanie planu ciągłości działania na wypadek,
    - gdy któraś ze stron będzie chciała zakończyć umowę **przed terminem**;
  - renegocjacja umowy ze względu
    - na **zmianę wymagań** bezpieczeństwa w organizacji;
  - aktualna dokumentacja listy aktywów,
    - licencji,
    - umów oraz
    - praw z nimi związanych.

7 - Zarządzanie aktywami
7.1 – Odpowiedzialność za aktywa **(1)**

- **A.7.1 – Odpowiedzialność za aktywa**
- Cel: ***Osiągnięcie i utrzymanie odpowiedniego poziomu ochrony aktywów organizacji***
- *A.7.1.1 Inwentaryzacja aktywów*
  - **Wszystkie aktywa**
    - **powinny być**
  - **jasno zidentyfikowane**
    - oraz
  - należy sporządzić i utrzymywać spis
  - wszystkich ważnych aktywów

7 - Zarządzanie aktywami

7.1 – Odpowiedzialność za aktywa (1)

- **Zalecenia**
  - **Inwentarz aktywów**
    - **w postaci przydatnej**
  - **do odtworzenia aktywu po katastrofie**
  - **Własność i klasyfikacja udokumentowana**
    - **dla każdego aktywu**
  - **Nie powielać innych wykazów**

7 - Zarządzanie aktywami

7.1 – Odpowiedzialność za aktywa (2)

- **Przykładowe aktywa:**
  - **aktywa informacyjne:**
    - **zbiory danych i**
    - **pliki z danymi,**
    - **dokumentacja systemu,**
    - **instrukcje użytkownika,**
    - **materiały szkoleniowe,**
    - **procedury eksploatacyjne i**
      - wsparcia,
    - **plany utrzymania ciągłości działania,**
    - **przygotowania awaryjne,**
    - **informacje zarchiwizowane;**
  - **aktywa oprogramowania:**
    - **oprogramowanie aplikacyjne,**
    - **oprogramowanie systemowe,**
    - **programy narzędziowe i**
    - **użytkowe;**

7 - Zarządzanie aktywami

7.1 – Odpowiedzialność za aktywa (3)

- **aktywa fizyczne:**
  - **sprzęt komputerowy**
    - procesory,
    - monitory,
    - laptopy,
    - modemy,
  - **sprzęt komunikacyjny**
    - rutery,
    - **centrale** abonenckie,
    - **telefaksy**,
    - automatyczne **sekretarki**,
  - **nośniki magnetyczne**
    - taśmy i
    - Dyski
    - **CD** i **DVD**,

7 - Zarządzanie aktywami

7.1 – Odpowiedzialność za aktywa (4)

  - **inny sprzęt techniczny**
    - zasilacze,
    - **klimatyzatory**,
  - **meble,**
  - **pomieszczenia;**
- **usługi:**
  - **usługi obliczeniowe i**
  - **telekomunikacyjne,**
  - **inne usługi infrastruktury technicznej**
    - ogrzewanie,
    - oświetlenie,
    - **zasilanie**,
    - **klimatyzacja**.

- **Ludzie ich kwalifikacje, umiejętności i doświadczenie**
- **Wartości niematerialne takie jak reputacja i wizerunek organizacji**

7 - Zarządzanie aktywami

7.1 – Odpowiedzialność za aktywa (4)

- **A 7.1.2 Własność aktywów**
  - **Wszystkie informacje**
  - **i aktywa związane**
    - **ze środkami służącymi do przetwarzania informacji**
  - **powinny mieć właściciela ***
  - **w postaci wyznaczonej części organizacji.**

* **Właściciel określa osobę lub podmiot, który ma zatwierdzoną przez zarząd odpowiedzialność za sterowanie produkcją, rozwój utrzymanie, użytkowanie i bezpieczeństwo aktywu.**
- **Pojęcie to nie oznacza że osoba ta posiada jakiekolwiek prawa własności do aktywu**

7 - Zarządzanie aktywami

7.1 – Odpowiedzialność za aktywa (4)

- **Zaleca się, aby właściciel aktywu był odpowiedzialny za:**
  - **zapewnienie, że**
    - **informacja i aktywa powiązane ze środkami służącymi do przetwarzania informacji są**
    - **poprawnie sklasyfikowane;**
  - **zdefiniowanie i okresowy**
  - **przegląd ograniczeń dostępu oraz klasyfikacji,**
    - **uwzględniając odpowiednie polityki kontroli dostępu.**
  - **Przedmiotem własności może być:**
    - **proces biznesowy;**
    - **określony zbiór działań;**
    - **aplikacja;**
    - **określony zbiór danych.**

7 - Zarządzanie aktywami

7.1 – Odpowiedzialność za aktywa (5)

- **A 7.1.3. Akceptowalne użycie aktywów**
  - **Zasady dopuszczalnego korzystania**
  - **z informacji**
    - **oraz**
    - **aktywów związanych**
      - z środkami służącymi do przetwarzania informacji.
  - **powinny zostać**
    - **określone,**
    - **udokumentowane i**
    - **wdrożone**

7 - Zarządzanie aktywami

7.1 – Odpowiedzialność za aktywa (5)

- **Zaleca się, aby wszyscy**
  - **pracownicy,**
  - **współpracownicy oraz**
  - **użytkownicy reprezentujący stronę trzecią**
  - **stosowali się do zasad akceptowalnego korzystania z informacji oraz**
  - **aktywów związanych z środkami służącymi do przetwarzania informacji, w tym:**
    - **zasad korzystania z poczty elektronicznej i Internetu (patrz 10.8);**

7 - Zarządzanie aktywami

7.1 – Odpowiedzialność za aktywa (6)

- zaleceń dotyczących korzystania z urządzeń przenośnych,
  - w szczególności korzystania z nich poza siedzibą organizacji (patrz 11.7.1).

❑ **Zaleca się, aby**
- określone zasady i zalecenia były
- wprowadzone przez odpowiednie kierownictwo.

❑ **Zaleca się, aby**
- pracownicy,
- współpracownicy oraz
- użytkownicy reprezentujący stronę trzecią
- korzystający lub
- mający dostęp do aktywów organizacji byli świadomi
- ograniczeń korzystania z informacji,
- zasobów oraz
- aktywów związanych ze środkami służącymi do przetwarzania informacji należących do organizacji.

7 - Zarządzanie aktywami 7.2 - Klasyfikacja informacji (1)

A.7.2 - *Cel :* *Zapewnianie informacje uzyskują ochronę na odpowiednim poziomie*

❑ A.7.2.1 Wytyczne w zakresie klasyfikacji
- Informacje powinny być klasyfikowane
  - przy uwzględnieniu ich wartości,
  - wymagań prawnych,
  - wrażliwości i
  - krytyczności dla organizacji.

7 - Zarządzanie aktywami

7.2 - Klasyfikacja informacji (2)

❑ Zaleca się
- brać pod uwagę wymagania biznesowe dla
  - współużytkowania i
  - **ograniczania** dostępu do informacji oraz
  - **biznesowe konsekwencje** wynikające z tych potrzeb.

❑ **Zalecanie umiaru przy klasyfikowaniu;**
- Uwzględnienie zmiany wartości informacji w różnych fazach życia informacji.

❑ **Zaleca się, aby**
  - zalecenia do klasyfikacji zawierały
- zasady wstępnej klasyfikacji oraz
- późniejszych jej modyfikacji;
  - według z góry
- ustalonej polityki kontroli dostępu (patrz 11.1.1).

7 - Zarządzanie aktywami

7.2 - Klasyfikacja informacji (2)

❑ **Do obowiązków właściciela aktywu (patrz 7.1.2) należy**
- określenie klasyfikacji aktywu, jej
  - okresowy przegląd oraz
- zapewnienie aktualności tej klasyfikacji i właściwego poziomu tej klasyfikacji.

❑ **Zaleca się, aby klasyfikacja brała pod uwagę**
- efekt agregacji opisany w 10.7.2.

❑ **Zaleca się zwrócenie uwagi na**
- ilość kategorii oraz
- korzyści z nich wynikające.

❑ **Zaleca się na zwrócenie uwagę na**
- interpretację oznaczeń pochodzących z innych organizacji

7 - Zarządzanie aktywami

7.2 - Klasyfikacja informacji (2)

- **A.7.2.2. Oznaczanie i postępowanie z informacją**
  - **Odpowiedni zbiór procedur**
    - **do oznaczania informacji i**
    - **postępowania z nimi,**
    - **powinien zostać opracowany i wdrożony**
      - według
    - **schematu klasyfikacji**
  - **przyjętego w organizacji**

7 - Zarządzanie aktywami

7.2 - Klasyfikacja informacji (2)

- **Elektroniczna i**
  - **fizyczna postać informacji;**
- **Zaleca się, aby**
  - **oznaczanie odzwierciedlało**
  - **klasyfikację według zasad wprowadzonych w 7.2.1.**
- **Dotyczy to**
  - **drukowanych raportów,**
  - **ekranów,**
  - **zapisanych nośników (np. taśm, dysków, dysków CD),**
  - **wiadomości elektronicznych oraz**
  - **przesyłanych plików.**

7 - Zarządzanie aktywami

7.2 - Klasyfikacja informacji (2)

- **Dla każdego poziomu klasyfikacji należy określić**
  - **procedury postępowania, które obejmują**
    - **przetwarzanie,**
    - **przechowywanie,**
    - **przesyłanie,**
    - **zmianę klasyfikacji oraz**
    - **niszczenie.**
- **Zaleca się także uwzględnienie procedur**
  - **tworzenia powiązań uprawnień i**
  - **rejestrowania zdarzeń związanych z bezpieczeństwem.**

7 - Zarządzanie aktywami

7.2 - Klasyfikacja informacji (3)

- **Zaleca się, aby**
  - **umowy z innymi organizacjami, które**
  - **uwzględniają współużytkowanie informacji,**
  - **zawierały procedury opisujące**
    - **klasyfikację tej informacji oraz**
    - **umożliwiające interpretację oznaczeń innych organizacji.**
- **Jakie przyjąć oznaczenia?**
  - **Nie stosować**
    - ściśle tajne,
    - tajne,
    - poufne,
    - zastrzeżone lecz
    - **tajemnica firmy,**
    - **tajemnica spółki,**
    - **poufne firmy,**
    - **poufne bankowe itp.**