1. Zarządzanie bezpieczeństwem informacji wymaga jako minimum

Udziału w nim wszystkich pracowników organizacji

2. Wymagania dotyczące bezpieczeństwa powinny być określone w oparciu

- szacowanie ryzyka dotyczącego organizacji
- zbiór wymagań prawnych statutowych, regulacyjnych i kontraktowych
- specyficzny zbiór zasad celów i wymagań dotyczących przetwarzania informacji opracowane przez organizację w celu wspomagania swojej działalności

3. W definicji Zarządzania znajdują się następujące pojęcia

Skoordynowane działania w celu kierowania i kontroli organizacji z uwzględnieniem ryzyka, risk management

4. Koło Deminga składa się z następujących czynności

Planowanie, wykonanie, sprawdzenie, działanie

5. System zarządzania bezpieczeństwem informacji odnosi się do

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

6. Zabezpieczenie to

- Odseparowane domeny logiczne
- Kontrolowanie ruchu pomiędzy domenami
- Zapory (firewall)
- Uwzględniać
    - politykę kontroli dostępu i
    - koszt
    - wydajność

7. Źródła zagrożeń to

- brak mechanizmu lub nieskuteczne mechanizmy kontroli dostępu do sprzętu oprogramowani i danych
- niewłaściwa administracja systemem informatycznym
- zaniedbania i błędy użytkowników
- niezadowolenie pracowników z warunków pracy
- programy wirusowe, bomy logiczne, konie trojańskie, robaki komputerowe
- ingerencja intruzów specjalizujących się w przełamywaniu zabezpieczeń
- możliwość podsłuchiwania aktywnego i pasywnego
- retransmisja informacji

8. Znamy następujące rodzaje audytów w bezpieczeństwie informacji

- wewnętrzny (pierwszej strony)
- drugiej strony (klienta, innej zainteresowanej strony)
- trzeciej strony (jednostki certyfikacyjnej)

9. Rodzaje zagrożeń to

- nieuprawniona modyfikacja informacji
- kradzież istotnych informacji
- zniszczenie fizyczne
- powielenie komunikatu
- podszycie się pod inna osobę
- zaprzeczenie wykonania informacji
- sabotaż zasobów
- niedbalstwo użytkowników

10. Obraźliwa i nielegalna treść to

- pornografia i pedofila
- promowanie brutalności, terroryzmu, rasizmu a nawet anoreksji
- edukacja anarchistyczna
- nielegalne transakcje

11. Przykładowymi zagrożeniami jest

1. Rozmyślne (ludzkie)
    - podsłuch
    - modyfikacja informacji
    - włamanie do systemu
    - złośliwy kod
    - kradzież
2. Przypadkowe (ludzkie)
    - pomyłki i pominięcia
    - skasowanie pliku
    - nieprawidłowe skierowanie
    - wypadki fizyczne
3. Środowiskowe
    - trzęsienia ziemi
    - piorun
    - powódź
    - pożar

12. Zagrożenia przypadkowe to

j.w.

13. Najgroźniejsze wycieki informacji w 2008 i 2009r to

- 2008
    - Problemy z fuzją PKO S.A. i BPH
    - Życiorysy i listy motywacyjne kandydatów do pracy PKO S.A
    - BRE 3mln zł –kradzież tradycyjna z wrzutni (ale pewnie był przeciek)
    - Fishing (WZB, PKO ....)
    - Karta VISA problemy 2 razy w roku
    - Nieuznawanie reklamacji (rekordzista Lukas Bank)
    - Zniknięcie 500tys L.Wałęsy z Multibanku?
    - 50tys. Pobranych z kont w czasie awarii połączenia do Bankomatu
- 2009
    - 10 mln $ z jednego banku przez kilkadziesiąt bankomatów
    - Penetracje ambasad kilkudziesięciu krajów,
    - Dostęp do serwerów myśliwca F35
    - Awaria serwerów autoryzacji bankowej
    - Awaria google – złe uaktualnienie
    - Awaria sieci T-Mobile
    - Problem Microsoftu z Zumi (nie istniejący dzień)
    - 75% zwolnionych pracowników wynosi dane (ankieta)
    - Sprytniejsi donoszą na nielegalne oprogramowanie
    - BSA się cieszy
    - Ostatnio w jednym z banków w Polsce na godzinę konta zostały wyzerowane

14. Ustanowienie SZBI obejmuje

- Ustanowienie SZBI
    - Organizacja powinna określić zakres i granice SZBI uwzględniając charakterystyki:
        - Prowadzonej działalności
        - Organizacji
        - Lokalizacji
        - Aktywów
        - Technologii
        - Zawierający
            - Dokładny opis i decyzję dla każdego wyłączenia z zakresu
    - Określić politykę SZBI, uwzględniającą charakter prowadzonej działalności, organizacji, jej lokalizacji, aktywów i technologii która:
        - Zawiera ramy ustalania celów, oraz
            - wyznacza ogólny kierunek i
            - zasady działania dotyczące bezpieczeństwa informacji
        - Bierze pod uwagę
            - wymagania biznesowe,
            - prawne i
            - Charakterze regulacyjnym
            - oraz kontraktowe
            - dotyczące bezpieczeństwa informacji
        - Ustanawia
            - kontekst strategiczny
            - związany z zarządzaniem ryzykiem
            - dający obszar
            - ustanowienia i
            - utrzymania SZBI

- Określa kryteria oceny ryzyka i strukturę oceny ryzyka
- Została zaakceptowana przez kierownictwo
    - Uwaga polityka SZBI może być zestawem wszystkich polityk bezpieczeństwa, może być w jednym dokumencie

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

- Określić ryzyko
- Określić aktywa w zakresie SZBI i ich właścicieli
- Określić zagrożenia dla tych aktywów
- Określić podatności, które mogą być wykorzystane przez zagrożenia
- Określić skutki utraty poufności, integralności i dostępności w odniesieniu do aktywów

- Analizować i ocenić ryzyko
- Oszacować szkody i straty dla biznesu wynikające z naruszenia bezpieczeństwa, biorąc pod uwagę konsekwencje utraty: poufności integralności i dostępności aktywów
- Oszacować realne prawdopodobieństwo naruszenia bezpieczeństwa w świetle istotnych zagrożeń i podatności oraz konsekwencji związanych z tymi aktywami oraz aktualnie wdrożonymi zabezpieczeniami
- Wyznaczyć poziomy ryzyka
- Stwierdzić kiedy ryzyko jest akceptowane lub wymaga odpowiedniego postępowania
    - Opierając się na
    - Kryteriach zaakceptowania ryzyka

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

- Wybrać cele stosowania zabezpieczania i zabezpieczenia.
- Uzyskać akceptację kierownictwa dla ryzyk szczątkowych
- Uzyskać autoryzację kierownictwa dla wdrożenia i eksploatacji SZBI
- Przygotować deklarację stosowania (SoA)

15. Dokumentacja powinna obejmować

- Udokumentowaną politykę bezpieczeństwa oraz
    - celów stosowania zabezpieczeń
- Zakres SZBI
- procedury i zabezpieczenia służące realizacji SZBI
- Opis metodologii szacowania ryzyka
- Raport z szacowania ryzyka
- Plan postępowania z ryzykiem
- Udokumentowane procedury potrzebne organizacji aby efektywnie
    - Planować
    - Wykonywać
    - Sterować
    - procesami bezpieczeństwa informacji
    - Oraz
    - Określenie jak mierzyć skuteczność zabezpieczeń
- Zapisy wymagane przez normę
- Deklarację stosowania

16. Utrzymywanie i doskonalenie SZBI obejmuje

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

17. Dokumentacja powinna obejmować

- Udokumentowaną politykę bezpieczeństwa oraz
    - celów stosowania zabezpieczeń
- Zakres SZBI
- procedury i zabezpieczenia służące realizacji SZBI
- Opis metodologii szacowania ryzyka
- Raport z szacowania ryzyka
- Plan postępowania z ryzykiem
- Udokumentowane procedury potrzebne organizacji aby efektywnie
    - Planować
    - Wykonywać
    - Sterować
    - procesami bezpieczeństwa informacji
    - Oraz
    - Określenie jak mierzyć skuteczność zabezpieczeń

- Zapisy wymagane przez normę
- Deklarację stosowania

18. Zapisy powinny dotyczyć

Realizacji procesów zgodnie z opisem zawartym w 4.2 oraz wszystkich incydentów związanych bezpieczeństwem w odniesieniu do SZBI

- Przykłady
- Lista gości,
- Raporty z audytów,
- Autoryzacja dostępu

19. Odpowiedzialność kierownictwa obejmuje

- Zaangażowanie kierownictwa
    - Kierownictwo powinno przedstawić świadectwo zaangażowania w ustanowienie, eksploatację, monitorowanie, przeglądy, utrzymanie obsługę i doskonalenie SZBI.
- Zarządzanie zasobami
- Zapewniania zasobów
- Szkolenie, uświadomienie i kompetencje

20. Szkolenie, uświadamianie i kompetencje obejmują

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

21. Dane wejściowe do przeglądu to

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

22. Dane wyjściowe z przeglądu to

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

23. Procedury wymagane przez ISO/IEC 27001:2005

- Procedura nadzoru nad dokumentacją [4.3.2]
- Procedura audytu wewnętrznego [6]
- Procedury działania korygującego [8.2]
- Procedury działań zapobiegawczych [8.3]
- Procedury natychmiastowego wykrycia i reakcji na incydenty oraz wykrywania błędów w wynikach przetwarzania [4.2.2g] [4.2.3a]:
- Procedury oznaczania informacją i postępowania z informacją [A.7.2.2]
- Procedury zarządzania incydentami związanymi z bezpieczeństwem [A.13.1.2]
- Procedury uświadamiania użytkowników o szkodliwym oprogramowaniu [A.10.4.1.]
- Procedury postępowania z informacją [A.10.7.3]
- Procedury dotyczące wymiany informacji [A.10.8.1]
- Formalna procedura rejestrowania i wyrejestrowania użytkowników [A 11.2.1].
- Procedury pracy na odległość [A11.7.2]
- Formalne procedury kontroli zmian [A12.5.1]
- Procedura zapewnianie zgodności z prawem do własności intelektualnej [A.15.1.2.]

24 Doskonalenie SZBI powinno być realizowane przez

- Stosowanie polityki bezpieczeństwa informacji
- Cele bezpieczeństwa
- Wyniki audytów
- Analizę monitorowanych zdarzeń
- Działania korygujące
- Działania zapobiegawcze
- Przeglądy realizowane przez kierownictwo

25 Rola kierownictwa w ISO/IEC 27001:2005

- Zaangażowanie kierownictwa

  Kierownictwo powinno przedstawić świadectwo zaangażowania w ustanowienie, eksploatację, monitorowanie, przeglądy, utrzymanie obsługę i doskonalenie SZBI poprzez

  - Ustanowienie polityki SZBI
  - Zapewnienie że cele i plany bezpieczeństwa informacji zostały ustanowione
  - Określenie ról i zakresów odpowiedzialności za bezpieczeństwo informacji
  - Informowanie organizacji o znaczeniu realizacji celów bezpieczeństwa informacji oraz zgodności z polityką bezpieczeństwa, odpowiedzialności wobec prawa oraz potrzeby ciągłego doskonalenia
  - Dostarczanie wystarczających zasobów dla opracowania, wdrożenia, monitorowania, przeglądów, eksploatacji i utrzymania SZBI
  - Decydowanie o kryteriach akceptowania ryzyka i akceptowanym poziomie ryzyka
  - Zapewnienia przeprowadzania wewnętrznych audytów SZBI
  - Przeprowadzanie przeglądów SZBI realizowanych przez kierownictwa

- Zarządzanie zasobami

  - Zapewniania zasobów

  Organizacja powinna określić i zapewnić zasoby potrzebne dla

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

  - Szkolenie, uświadomienie i kompetencje

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

26. Działania zapobiegawcze

- Organizacja powinna wskazywać działanie podejmowane w celu ochrony przed przyszłymi niezgodnościami tak, aby przeciwdziałać ich wystąpieniu.
- Działania zapobiegawcze powinny być dostosowane do wagi potencjalnych problemów
- Udokumentowana procedura działań zapobiegawczych powinna określić wymagania dla:
    - zidentyfikowania potencjalnych niezgodności i
        - ich przyczyn,
    - Oceny potrzeby działania zapobiegawczego
        - w celu zapobieżeniu niezgodnościom
    - wskazania i
        - wdrożenia
        - potrzebnego działania zapobiegawczego
    - zapisu rezultatów podjętych działań
    -przeglądu podjętych działań zapobiegawczych.
- Organizacja powinna zidentyfikować zmienione ryzyka o zwracając uwagę na znacząco zmienione ryzyka
- Należy wskazać priorytety działań zapobiegawczych w oparciu o wyniki szacowania ryzyka
    - Uwaga działania zapobiegające niezgodnościom są często bardziej efektywne kosztowo niż działania korygujące

27. Polityka SZBI

- Polityka SZBI, uwzględnia charakter prowadzonej działalności, organizacji, jej lokalizacji, aktywów i technologii która:
    - Zawiera ramy ustalania celów, oraz
        - wyznacza ogólny kierunek i
        - zasady działania dotyczące bezpieczeństwa informacji
    - Bierze pod uwagę
        - wymagania biznesowe,
        - prawne i
        - Charakterze regulacyjnym
        - oraz kontraktowe
        - dotyczące bezpieczeństwa informacji
    - Ustanawia
        - kontekst strategiczny
        - związany z zarządzaniem ryzykiem
        - dający obszar
        - ustanowienia i
        - utrzymania SZBI
    - Określa kryteria oceny ryzyka i strukturę oceny ryzyka
    - Została zaakceptowana przez kierownictwo

28. Norma ISO/IEC 27001 wymaga następujących działań w odniesieniu do ryzyka

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

29. Doskonalenie

30. Warianty postępowania z ryzykiem obejmują

- redukowanie ryzyka
- zachowanie ryzyka
- unikanie ryzyka
- przeniesienie ryzyka

31. Przeglądy ryzyka akceptowalnego powinny brać pod uwagę

- Kontekst prawny i środowiskowy
- Kontekst związany z konkurencją
- Podejście do szacowania ryzyka
- Wartość i kategorie aktywów
- Kryteria skutków
- Kryteria oceny ryzyka
- Kryteria akceptowania ryzyka
- Całkowity koszt utrzymania
- Konieczne zasoby

32. Przykładowe aktywa to

- 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
- aktywa fizyczne
    - sprzęt komputerowy
        - procesory
        - monitory

        - laptopy
        - modemy
    - sprzęt komunikacyjny
        - routery
        - centrale abonenckie
        - telefaksy
        - automatyczne sekretarki
    - nośniki magnetyczne
        - dyski
        - cd i dvd
    - inny sprzęt techniczny
        - zasilacze
        - klimatyzatory
    - meble
    - pomieszczenia
- usługi
    - usługi obliczeniowe i telekomunikacyjne
    - inne usługi infrastruktury technicznej
        - ogrzewanie
        - oświetlenie
        - zasilanie
        - klimatyzacja
- ludzie i ich kwalifikacje, umiejętności i doświadczenie, wartości niematerialne jak reputacja i wizerunek

33. Usługi wchodzące w skład aktywów to

- usługi obliczeniowe i telekomunikacyjne
- inne usługi infrastruktury technicznej
    - ogrzewanie
    - oświetlenie
    - zasilanie
    - klimatyzacja

34. Przykładowe podatności to

- 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
- 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
- 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

- 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
- 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
- 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

- 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
  - 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
  - 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

35. Przykładowe podatności dotyczące oprogramowania to

Odpowiedź wyżej

36. W przykładowej metodzie analizy ryzyka stosowane są następujące terminy

- 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.

37. Norma ISO/IEC 27001 (poprzednio o nazwie ISO/IEC 17799) zawiera w rozdziale organizacja wewnętrzna następujące punkty

- Zaangażowanie kierownictwa w bezpieczeństwo informacji
- Koordynacja bezpieczeństwa informacji
- Przydział odpowiedzialności w zakresie bezpieczeństwa informacji
- Proces autoryzacji urządzeń służących do przetwarzania informacji
- Umowy o zachowaniu poufności
- Kontakty z organami władzy
- Kontakty z grupami zainteresowania Bezpieczeństwem
- Niezależne przeglądy bezpieczeństwa informacji

38. W przypadku kontaktu ze stronami zewnętrznymi podstawą jest

Utrzymanie bezpieczeństwa informacji należących do organizacji oraz środków przetwarzania informacji,

- do których mają dostęp,
- Za pomocą których
- przetwarzają,
- komunikują się
- lub którymi o zarządzają strony zewnętrzne.

39. Bezpieczeństwa zasobów ludzkich obejmuje

- Bezpieczeństwo przed zatrudnieniem
- Bezpieczeństwo podczas zatrudnienia
- Bezpieczeństwo po zakończeniu lub zmianie zatrudnienia

40. Audyt systemu zarządzania bezpieczeństwem informacji to

Proces zbierania i oceniania dowodów w celu określenia czy system informatyczny i związane z nim zasoby właściwie chronią majątek, utrzymują integralność danych i dostarczają odpowiednich i rzetelnych informacji, osiągają efektywnie cele organizacji, oszczędnie wykorzystują zasoby i stosują mechanizmy kontroli wewnętrznej, tak aby dostarczyć rozsądnego zapewnienia, że osiągane są cele operacyjne i kontrolne, oraz że

chroni się przed niepożądanymi zdarzeniami lub są one na czas wykrywane a ich skutki na czas korygowane.

41. Audyt certyfikacyjny obejmuje

- Wdrożenie SZBI
- Ewentualnie Ocena wstępna
- Audyt certyfikacyjny
- Etap 1
- Etap 2
- Działania po audytowe
- Audyty nadzoru

42. Drugi etap audytu certyfikacyjnego koncentruje się na

- ocenie ryzyka związanego z bezpieczeństwem informacji i wynikające z tego zaleceniach SZBI;
- Deklaracji Stosowania;
- celach wynikających z polityki;
- monitorowaniu, pomiarach, sporządzaniu raportów i przeglądach celów;
- przeglądach bezpieczeństwa i zarządzania;
- odpowiedzialności kierownictwa za politykę bezpieczeństwa informacji;
- związkach pomiędzy polityką wynikami oceny zagrożenia bezpieczeństwa, informacji, celami, odpowiedzialnością, programami, procedurami, danymi o wynikach i przeglądami bezpieczeństwa.

43. Programy antywirusowe można ocenić ze względu na

- Wydajność
    - Stopień wykrycia wirusów
- Obsługa
- Funkcjonalność
    - Czas reakcji na nowe zagrożenia
    - Szybkość skanowania
    - Obsługa techniczna
    - wsparcie
- Nie brano pod uwagę
    - Możliwości błędów w oprogramowaniu
    - Wielkości plików łatek
    - Możliwości używania bez połączenia z internetem
    - Interakcji z innymi programami antywirusowymi

44. Programy antyspamowe można instalować

- Zalecana instalacja
    - Na serwerze
    - I na stacjach roboczych
- Zwykle nie da się zainstalować 2 na jednej stacji
    - Chociaż niektóre mają 2 skanery

45. Komponenty firewall

- Filtry pakietów
- Działają na poziomie warstwy IP

- Bramy na poziomie warstwy transportowej
- Circuit level gataway
- Bramy na poziomie aplikacji
- Wielopoziomowe zapory z badaniem stanu połączeń

46. Celami audytu systemu zarządzania bezpieczeństwem informacji jest

- Przegląd zgodności SZBI z ISO 27001:2005
- Przegląd poziomu wdrożenia ISO 27001:2005
- Przegląd skuteczności i stosowalności SZBI w odniesieniu do polityki i celów bezpieczeństwa
- identyfikacja luk i słabości
- Wskazanie możliwości doskonalenia SZBI

49. Odpowiedzialność audytora dotyczy

- Spełnienie wymagań związanych z audytem
- Przekazywanie i wyjaśnianie wymagań związanych z audytem
- Planowanie oraz sprawne i skuteczne wykonywanie powierzonych im zadać
- Dokumentowanie spostrzeżeń
- Przedstawianie wyników audytu
- Ochronę dokumentów dotyczących audytu
- Współpracę z audytorem wiodącym

50. Zadania audytora i audytora wiodącego

Zadania audytora:

- Nie wykraczanie poza zakres audytu
- Obiektywizm
- Zebranie i przeanalizowanie wystarczającej liczby dowodów
- Postępowanie w sposób etyczny
- Ochrona poufności
- Ochrona wszystkich dokumentów
- Niezależna i obiektywna ocena SZBI
- Nie uleganie uprzedzeniom i wpływom
- Skuteczność w odniesieniu do SZBI
- Poziom wdrożenia
- Planowanie i zarządzanie audytem
- Rejestrowanie i raportowanie spostrzeżeń
- Zapewnienie integralności i niezależności audytu

Zadania audytora wiodącego:

- Ponosi ostateczną odpowiedzialność za wszystkie fazy audytu
- Bierze udział w doborze pozostałych członków zespołu audytu
- Przygotowuje plan audytu
- Reprezentuje zespół audytowy wobec kierownictwa audytowanej jednostki
- Przedstawia raport z audytu
- Określenie wymagań dotyczące zadań audytu
- Stosowanie się do wymagań
- Zaplanowanie audytu
- Przygotowanie dokumentacji
- Dokonanie przeglądu dokumentacji
- Informowanie audytowanego o krytycznych nie zgodnościach

- Informowanie o przeszkodzie w realizacji audytu
- Przedstawianie wyniki audytu w sposób jasny i bez opóźnień

51. Plan audytu obejmuje

- Przygotowany przez audytora wiodącego
- Zaaprobowany przez klienta
- Elastyczny
- Zawierający cele audytu z jego zakres
- Określający osoby odpowiedzialne za realizację celów
- Identyfikujący powiązane dokumenty
- Określający zespół audytowy
- Określający czas trwania wszystkich działań
- Harmonogram spotkań
- Umowa o zachowaniu poufności (jeżeli nie była zawarta wcześniej)
- Termin dostarczenia raportu z audytu
- Rozwiązujący wszelkie wątpliwości związane z audytem

52. Programy antywirusowe

- G-Data
- McAffe
- Kasparski lab
- Fsecure
- Symantec
- Panda
- Antivir
- NOD 32
- Trend micro

53. Bezpieczeństwo informacji oznacza

Bezpieczeństwo informacji oznacza, że jest ona chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby

- zapewnić ciągłość prowadzenia działalności,
- zminimalizować straty
- maksymalizować zwrot nakładów na inwestycje i działania o charakterze biznesowym.

Bezpieczeństwo informacji oznacza :

- dostępność
  - Właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu, czyli ochronę przed utratą chwilową lub trwałą
- integralność
  - Właściwość zapewnia dokładności i kompletności aktywów, czyli ochronę przed celową lub przypadkową modyfikacją
- poufność
  - Właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom, czyli ochronę przed kradzieżą lub ujawnieniem informacji

- dodatkowo, mogą być brane pod uwagę inne własności takie, jak autentyczność, rozliczalność, niezaprzeczalnąść i niezawodność.

- rozliczalność:
  - Właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2: 1989)
  - accountability
- autentyczność:
  - Właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana. Autentyczność dotyczy takich podmiotów jak: użytkownicy, procesy, systemy i informacja
  - authenticity

- niezawodność:
  - Właściwość oznaczająca spójne, zamierzone zachowanie i skutki
  - Reliability
- niezaprzeczalność
  - Zdolność do potwierdzenia wystąpienia określonego zdarzenia lub działania i jego oryginalnych podmiotów w przypadku konieczności rozwiązania sporów o wystąpienie lub nie wystąpienie zdarzenia lub działania i brania w nim udziału podmiotów w tym zdarzeniu

54. Bezpieczeństwo informacji można osiągnąć stosując

Bezpieczeństwo informacji można osiągnąć, wprowadzając odpowiedni zestaw środków:

- Politykę bezpieczeństwa
- Dobre praktyki,
- Procedury,
- Struktury organizacyjne
- Funkcje oprogramowania i sprzęt.

55. Normy rodziny ISO 27000 to

- Information technology -- Security techniques Information security management system
- fundamentals and vocabulary
- Będzie tłumaczona

56. Przykłady zagrożeń to

Pytanie 11

57. Kod złośliwy to

- Bomba logiczna
- Backdoor
- Wirus
- Robak internetowy
- Koń trojański
- keylogger
- rootkit

58. PN ISO/IEC 27001 składa się z następujących rozdziałów

- Przedmowa
- 0 Wprowadzenie
- 1 Zakres normy
- 2 Powołania normatywne
- 3 Terminy i definicje
- 4 Skróty
- 5 Usługi odtwarzania techniki teleinformatycznej po katastrofie
- 6 Obiekty związane z usługami odtwarzania techniki teleinformatycznej po katastrofie
- 7 Funkcje zapewniane przez zewnętrznego dostawcę usług
- 8 Wybór miejsc odtwarzania po katastrofie
- 9 Ciągłe doskonalenie
- Załącznik A (informacyjny) Powiązanie pomiędzy ISO/IEC 27002:2005 z niniejszą Normą Międzynarodową
- Bibliografia

59. Wdrożenie i eksploatacja SZBI obejmuje

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

60. Wymagane procedury w SZBI to

- Procedury oznaczania informacją i postępowania z informacją [A.7.2.2]
- Procedury zarządzania incydentami związanymi z bezpieczeństwem [A.13.1.2]
- Procedury uświadamiania użytkowników o szkodliwym oprogramowaniu [A. 10.4.1.]
- Procedury postępowania z informacją [A. 10.7.3]
- Procedury dotyczące wymiany informacji [A.10.8.1]

- Formalna procedura rejestrowania i wy rejestrowania użytkowników [A 11.2.1].
- Procedury pracy na odległość [Al 1.7.2]
- Formalne procedury kontroli zmian [A12.5.1]
- Procedura zapewnianie zgodności z prawem do własności intelektualnej [A.15.1.2.]

61. Przykładowe definicje związane z zarządzaniem ryzykiem to

- Ryzyko
    - kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji
        - W niektórych standardach
        - ryzyko może się wiązać zarówno z
            - aspektami pozytywnymi (szanse) jak i
            - negatywnymi (zagrożenia)
- 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
- 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 o “prawdopodobieństwo matematyczne”
- identyfikowanie ryzyka
    - proces znajdowania, zestawiania i charakteryzowania elementów ryzyka
- redukowanie ryzyka
    - działania, podejmowane w celu zmniejszenia prawdopodobieństwa
    - negatywnych następstw
        o 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
- akceptowanie ryzyka
    - decyzja, aby zaakceptować ryzyko

orisk acceptance

- analiza ryzyka
  - systematyczne korzystanie z informacji w celu zidentyfikowania źródeł i oceny ryzyka.

    orisk analizys
- Szacowanie ryzyka
  - całościowy proces analizy ryzyka i oceny ryzyka

    orisk assessment

62. Model zarządzania ryzykiem wg ISO/IEC 27005 obejmuje

- 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