Polskie normy dotyczące ochrony informacji - najbliższe zmiany i dalsze potrzeby w tym zakresie

Wdrożenie SZBI w podmiocie publicznym

Janusz Cendrowski, Janusz Żmudziński

Komitet Techniczny 182

Polski Komitet Normalizacyjny

Warszawa, dnia 2013.10.03

Agenda prezentacji

- Polskie Normy dotyczące ochrony informacji
- Potrzeby w zakresie nowych PN
- Wdrożenie SZBI w podmiotach publicznych
- Nowe normy w ISO/IEC

Komitet Techniczny 182 w PKN –

Polskie Normy dotyczące bezpieczeństwa informacji

- Systemy zarządzania bezpieczeństwem informacji – 6 szt.
- Kryptograficzne i niekryptograficzne techniki i mechanizmy zabezpieczeń – 21 szt.
- Kryteria oceny bezpieczeństwa oraz metodyki testów bezpieczeństwa - 3 szt.
- Usługi i aplikacje wspierające wdrożenie celów stosowania zabezpieczeń i zabezpieczeń – 1 szt.
- Aspekty bezpieczeństwa w zarządzaniu tożsamością, w biometrii oraz ochronie danych osobowych – 2 szt.
- Terminologia – 1 szt.

Polskie Normy w obszarze SZBI

Numer	Nazwa
PN-I-13335-1:1999	Technika informatyczna -- Wytyczne do zarządzania bezpieczeństwem systemów informatycznych -- Pojęcia i modele bezpieczeństwa systemów informatycznych
PN-ISO/IEC 17799:2007	Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zarządzania bezpieczeństwem informacji
PN-ISO/IEC 27001:2007	Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania
PN-ISO/IEC 27005:2010	Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji
PN-ISO/IEC 27006:2009	Technika informatyczna -- Techniki bezpieczeństwa -- Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji
PN-ISO/IEC 27000:2012	Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia
PN-EN ISO 27799:2010	Informatyka w ochronie zdrowia – Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002

Przywołanie Polskich Norm w przepisach

Nazwa aktu prawnego	Normy
Rozporządzenie MSWiA z 10.09.2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych Załącznik – Wykaz certyfikatów …	PN-ISO/IEC 27001
Rozporządzenie MSWiA z 21.04.2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników	PN-ISO/IEC 27001
Rozporządzenie Prezesa RM z 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych	PN-ISO/IEC 27001
Rozporządzenie RM z 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych	PN-ISO/IEC 27001 PN-ISO/IEC 17799 PN-ISO/IEC 27005 PN-ISO/IEC 24762 PN-ISO/IEC 20000
Rozporządzenie RM z 7.08.2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.	PN-ISO/IEC 15408 ISO/IEC 15946-2
Rozporządzenie Prezesa RM z 14.09.2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych	ISO/IEC 26300

Przywołanie Polskich Norm w przepisach

Nazwa aktu prawnego	Normy
Rozporządzenie Ministra Zdrowia z dnia 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej	PN-EN ISO 27799:2010 Ustawa o informatyzacji => Rozporządzenie KRI=> PN-ISO/IEC 27001 i pozostałe Inne normy dotyczące informatyki w ochronie zdrowia
Rozporządzenie Ministra Zdrowia z dnia 19 kwietnia 2013 r. w sprawie Systemu Rejestru Usług Medycznych Narodowego Funduszu Zdrowia	
Rozporządzenie Ministra Zdrowia z dnia 6 czerwca 2013 r. w sprawie Systemu Monitorowania Kosztów Leczenia i Sytuacji Finansowo-Ekonomicznej Podmiotów Leczniczych	
Rozporządzenie Ministra Zdrowia z dnia 6 czerwca 2013 r. w sprawie Systemu Ewidencji Zasobów Ochrony Zdrowia	
Rozporządzenie Ministra Zdrowia z dnia 25 czerwca 2013 r. w sprawie Systemu Statystyki w Ochronie Zdrowia	
Rozporządzenie Ministra Zdrowia z dnia 9 lipca 2013 r. w sprawie Systemu Monitorowania Zagrożeń	
Rozporządzenie Ministra Zdrowia z dnia 14 sierpnia 2013 r. w sprawie minimalnych wymagań dla niektórych systemów teleinformatycznych funkcjonujących w ramach systemu informacji w ochronie zdrowia	
Rozporządzenie Ministra Zdrowia z dnia 14 sierpnia 2013 r. w sprawie opisu, minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania Platformy Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych oraz Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych	

Przywołanie norm ISO/IEC w aktach UE

Nazwa aktu prawnego	Normy
Rozporządzenie WYKONAWCZE KOMISJI (UE) NR 1179/2011 z dnia 17 listopada 2011 r. ustanawiające specyfikacje techniczne w odniesieniu do systemów zbierania deklaracji on-line na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 211/2011 w sprawie inicjatywy obywatelskiej	ISO/IEC 27001 (PN-ISO/IEC 27001) ISO/IEC 27002 (PN-ISO/IEC 17799) ISO/IEC 27005 (PN-ISO/IEC 27005) ISO/IEC 27033
Rozporządzenie KOMISJI (WE) NR 885/2006 z dnia 21 czerwca 2006 r. ustanawiające szczegółowe zasady stosowania rozporządzenia Rady (WE) nr 1290/2005 w zakresie akredytacji agencji płatniczych i innych jednostek, jak również rozliczenia rachunków EFGR i EFRROW	ISO/IEC 27002 (PN-ISO/IEC 17799)
Rozporządzenie KOMISJI (UE) NR 73/2010 z dnia 26 stycznia 2010 r. ustanawiające wymagania dotyczące jakości danych i informacji lotniczych dla jednolitej europejskiej przestrzeni powietrznej	ISO/IEC 27002 (PN-ISO/IEC 17799)

Nowe projekty i propozycje polskich norm

- W opracowaniu nowe wersje
  - Pr PN-ISO/IEC 27006
  - Pr PN-ISO/IEC 27005
  - Pr PN-ISO/IEC 27013 Technika informatyczna - Techniki bezpieczeństwa -Wytyczne do zintegrowanego wdrożenia ISO/IEC 27001 oraz ISO/IEC 20000-1
  - Pr PN-ISO/IEC 20000-1 - Technika informatyczna - Zarządzanie usługami - Część 1: Wymagania dla systemu zarządzania usługami

Nowe projekty i propozycje polskich norm

- Celowe byłoby szybko opracować odpowiedniki dla
  - FDIS ISO/IEC 27001:2013 – nowa wersja 27001
  - FDIS ISO/IEC 27002:2013 – nowa wersja 27002 (dawniej 17799)
  - Normy dotyczące zarządzania ciągłością działania
    - ISO/IEC 22300:2012 Societal security - Terminology
    - ISO/IEC 22301:2012 Societal security - Business continuity management systems – Requirements
    - ISO/IEC 22313:2012 Societal security - Business continuity management systems - Guidance

Znaczenie norm

- Zalety norm
  - Suma doświadczeń – dobrych praktyk w określonym zakresie
  - Integracja, kompatybilność, współpraca
  - Uzgodnione w szerokim gronie specjalistów
  - Obejmujące cały zakres danego obszaru
    - Normy ogólne i normy szczegółowe
    - Normy wieloczęściowe, odwołania z norm ogólnych do szczegółowych
- Wady norm
  - Czasami nieaktualność (czas powstawania i uaktualniania - 5 lat)
  - Powolne usuwanie niespójności (jw.)
- Inne cechy
  - Neutralne technologicznie

Przykłady norm

- PN-ISO/IEC 17799 (27002)
  - Zalecenia we wszystkich obszarach bezpieczeństwa Systemów Informacyjnych
  - Podstawa opracowania PBI
- PN-ISO/IEC 27001
  - Wymagania na SZBI - spełnienie zapewni certyfikat
- PN-ISO/IEC 27005
  - Pełne podejście szacowania ryzyka w bezpieczeństwie informacji
- PN-ISO/IEC 24762
  - Kompendium zaleceń dot. zabezpieczeń organizacji świadczącej usługi DRP

PN-ISO/IEC 17799:2007

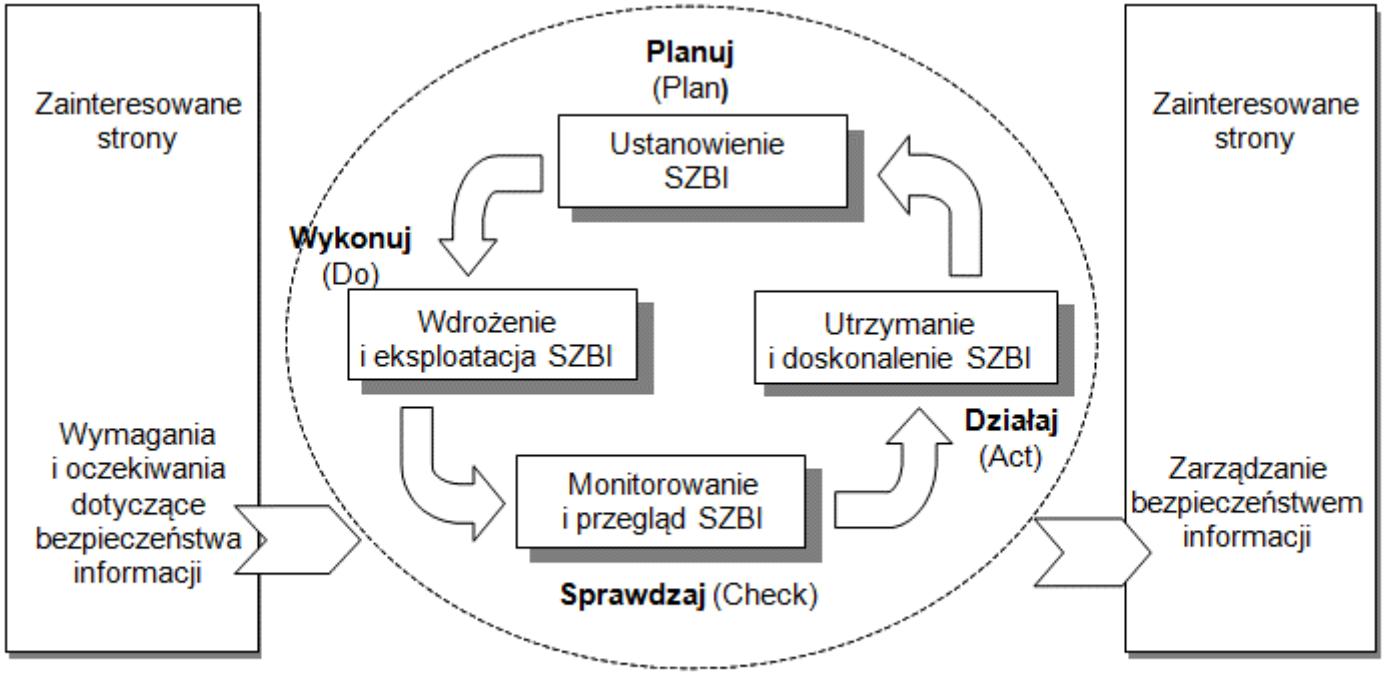
- Główne zalecenie
  - Wybór i wprowadzanie zabezpieczeń powinno być skutkiem szacowania ryzyka
- OBSZARY
  - Szacowanie ryzyka i postępowanie z ryzykiem,
  - Polityka bezpieczeństwa informacji,
  - Organizacja bezpieczeństwa informacji,
  - Zarządzanie aktywami,
  - Bezpieczeństwo zasobów ludzkich,
  - Bezpieczeństwo fizyczne i środowiskowe,

PN-ISO/IEC 17799:2007

- OBSZARY - cd
  - Zarządzanie systemami i sieciami
  - Kontrola dostępu
  - Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych
  - Zarządzanie incydentami związanymi z bezpieczeństwem informacji
  - Zarządzanie ciągłością działania
  - Zgodność

PN-ISO/IEC 27001:2007

- Część główna
  - ciągłe doskonalenie zarządzania bezpieczeństwem – wg cyklu PDCA



PN-ISO/IEC 27001:2007

- Cel wdrożenia Cyklu PDCA
  - Zmuszenie organizacji do ciągłego doskonalenia
  - Zmuszenie do stosowania środków wewnętrznej i zewnętrzne kontroli (monitorowanie, audyty, przeglądy)
    - Audyt – środek uzyskania dowodu na doskonalenie SZBI
- Opracowanie, wdrożenie i utrzymanie SZBI
  - Etap planowania (dokumentacja)
  - Etap wdrożenia (zapisy)
  - Etap monitorowania (ocena skuteczności)
  - Etap doskonalenia

PN-ISO/IEC 27001:2007

- Opracowanie, wdrożenie i utrzymanie SZBI cd
  - Wymagana dokumentacja i zapisy
  - Rola Kierownictwa
  - Audyty i przeglądy
  - Działania korygujące i zapobiegawcze
- Załącznik A
  - 132 wymagania - odwzorowanie rozdziałów PN-ISO/IEC 17799
  - Wymagania opisują zabezpieczenia
    - Fizyczne
    - Organizacyjno-proceduralne
    - Logiczne (mechanizmy w oprogramowaniu i urządzeniach)

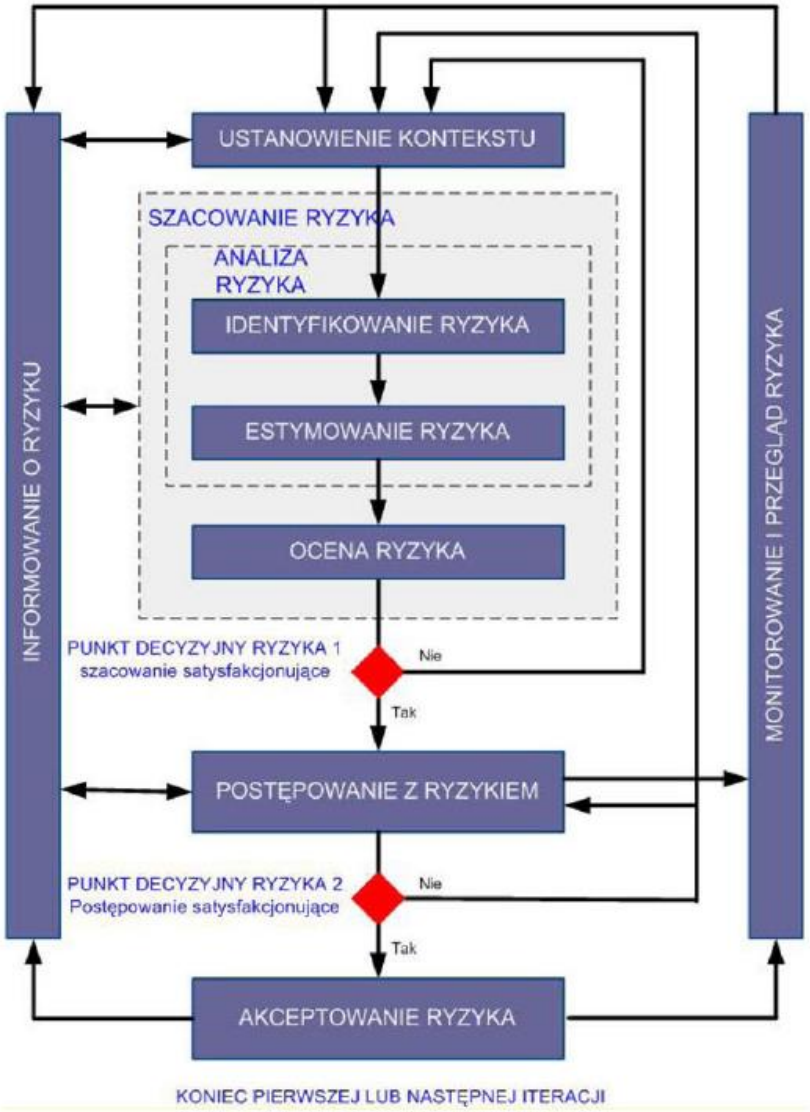
SZBI – czynniki sukcesu

- Struktura organizacyjna
- Audyt bezpieczeństwa
- Szacowanie ryzyka
  - Metodyka
  - Identyfikacja aktywów, zagrożeń, podatności, wpływów
  - Analiza i ocena ryzyka
  - Wybór zabezpieczeń
- Opracowanie dokumentów wymaganych przez PN ISO/IEC 27001
  - Deklaracji Stosowania, polityk, procedur
  - Plan Postępowania z Ryzykiem

SZBI – czynniki sukcesu

- Dobór i przeszkolenie Pełnomocnika
- Przeszkolenie pracowników
- Rozpoczęcie funkcjonowania, monitorowanie
- Tworzenie zapisów
- Audyty wewnętrzne
- Przegląd (min. 1 w roku)
- Realizacja Działań korygujących i zapobiegawczych
- Pozytywny audyt certyfikacyjny (akredytowana jednostka certyfikująca)

PN-ISO/IEC 27005:2010



Rysunek 1 – Proces zarządzania ryzykiem w bezpieczeństwie informacji

- Postępowanie z ryzykiem
  - Redukowanie
  - Zachowanie
  - Unikanie
  - Transfer

PN-ISO/IEC 27005:2010

- Analiza ryzyka
  - Wartość aktywów (wrażliwość, krytyczność)
  - Zagrożenia (prawdopodobieństwo , siła oddziaływania)
  - Podatności
  - Istniejące zabezpieczenia
  - Wpływy

PN-ISO/IEC 27005:2010

- Przykład z normy

Tablica E.1 a)

	Prawdopodobieństwo urzeczywistnienia się – Zagrożenie	Niskie (L)			Średnie (M)			Wysokie (H)		
	Łatwość wykorzystania	L	M	H	L	M	H	L	M	H
Wartość aktywów	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

- Inny przykład

$$R = (W+K) * pZ * P$$

gdzie

- W – wrażliwość (1-3)
- K – Krytyczność aktywów (1-3)
- pZ – „prawdopodobieństwo” zagrożenia (1-3)
- Podatności (0 lub 1)

Praktyka wdrażania SZBI w podmiocie publicznym

Wdrażanie SZBI w podmiotach publicznych

- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U. z 2012 poz. 526 /dalej R526/

- Bardzo długo konsultowane
  - Administracja publiczna, organizacje społeczne i zawodowe
- Intencja
  - Oparcie bezpieczeństwa systemów poza obszarem UOIN i UODO na bazie Polskich Norm

Wdrażanie SZBI w podmiotach publicznych

- Par. 20
  - Ust. 1 – konieczność opracowania, wdrożenia, monitorowania i doskonalenia SZBI
    - Cel – uzyskanie pożądanych atrybutów informacji
  - Ust. 3 – w oparciu o PN-ISO/IEC 27001 oraz inne polskie normy
  - Ust. 2 – zapewnienie przez kierownictwo podmiotu warunków zarządzania bezpieczeństwem
  - Ust. 4 – inne zabezpieczenia wynikające z analizy ryzyka

- Większy nacisk na systemy teleinformatyczne
- Termin – „w dniu pierwszej istotnej modernizacji systemów TI”
- Brak konieczności certyfikacji na zgodność z 27001

Wdrażanie SZBI w podmiotach publicznych

- Rekomendacja – połączyć wdrożenie SZBI z projektem wdrożenia nowego systemu IT

- Konieczna osoba wspierająca projekt z grona kierownictwa podmiotu

- Wyznaczyć pracownika odpowiedzialnego za SZBI
  - Administrator Bezpieczeństwa Informacji
  - Inspektor BTI
  - Pełnomocnik SZJ
  - Dyrektor Departamentu Informatyki – najmniej perspektywiczny

Kontrola wdrożenia SZBI

- Możliwe kontrole wdrożenia SZBI
  - NIK
  - Ustawa o informatyzacji
    - Naczelne organy administracji rządowej
      - W ramach swoich resortów
    - Ministerstwo Administracji i Cyfryzacji
      - Wszystkie inne podmioty publiczne
    - Kontrolerzy
      - Obszar jeszcze nie do końca uregulowany
        - ALE
      - Rozporządzenie MSWiA z dn. 10.09.2010 w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych (Dz.U. z 2010 nr 177 poz. 1195)

Nowe normy w ISO/IEC
Zmiany w stosunku do obecnych

FDIS ISO/IEC 27001:2013

- Część główna normy - struktura
  - 1 Scope
  - 2 Normative references
  - 3 Terms and definitions
  - 4 Context of the organization
  - 5 Leadership
  - 6 Planning
  - 7 Support
  - 8 Operation
  - 9 Performance evaluation
  - 10 Improvement

FDIS ISO/IEC 27001:2013

- Część główna normy - zmiany
  - PDCA
  - Interesariusze – muszą być określone wszystkie zainteresowane strony
  - „udokumentowane informacje” vs „dokumenty” i „zapisy”
  - Szacowanie ryzyka i postępowanie z ryzykiem
  - Cele, monitorowanie i pomiary
  - Komunikacja
  - Działania korygujące i zapobiegawcze

FDIS ISO/IEC 27001:2013

- Część główna normy - implementacja
  - Łatwiejsza integracja z ISO 9001, ISO 22301, ISO 20000
  - Lepsza skalowalność

FDIS ISO/IEC 27001:2013

- Załącznik A – uwagi ogólne
  - Wymagania nie zmienione lub zmienione stylistycznie
  - Wymagania zmienione
    - Nowe elementy istotne dla późniejszej oceny czy wymaganie jest spełnione
  - Wymaganie nowe lub zupełnie zmienione
  - Wymaganie usunięte
    - Większość pozornie usunięta ! => ukryte w innych wymaganiach

FDIS ISO/IEC 27001:2013

- Załącznik A – OBSZARY
  - 5. Polityka bezpieczeństwa informacji
  - 6. Organizacja bezpieczeństwa informacji
    - uszczegółowione „urządzenia mobilne i telepraca”
  - 7. Bezpieczeństwo zasobów ludzkich
    - Zapisy uszczegółowione
  - 8. Zarządzanie aktywami
    - Zapisy skrócone
  - 9. Kontrola dostępu
    - Dużo zmian np.:
      - „Authentication information” zamiast „password”
      - Dodano „User access provisioning”
      - Połączono dostęp do systemu i aplikacji

FDIS ISO/IEC 27001:2013

- OBSZARY - cd
  - 10. Ochrona kryptograficzna
    - Dawniej w rozdziale 12; uszczegółowienie „key management”.
  - 11. Bezpieczeństwo fizyczne i środowiskowe
    - Zmiany i uogólnienia („asset” zamiast „equipment”)
  - 12. Bezpieczeństwo utrzymania (bezpieczeństwo operacyjne)
    - Zarządzanie zmianą – podejście procesowe
    - Logi – jeden uogólniony zapis
    - Nowy zapis - „Restrykcje przy instalacji oprogramowania”
    - Usunięto „handel elektroniczny”, „transakcje on-line” i „www”
      - Usługi i aplikacje Webowe => są w wielu rozdziałach 27002 (mobilność, szkolenia, malware, testy stron webowych)

FDIS ISO/IEC 27001:2013

- OBSZARY – cd
  - 13. Bezpieczeństwo sieciowe (bezpieczeństwo sieciowe)
    - Wymagania z różnych sekcji poprzedniej wersji
    - Usunięto „Kontrola połączeń sieciowych” i „kontrola rutingu w sieciach” (zapory)
      - Włączono do 13.1.3 „Rozdzielenie sieci”
  - 14. Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych
    - Nowe
      - Zabezpieczenie usług aplikacyjnych w sieciach publicznych (również fraudy!)
      - Ochrona transakcji (kryptografia, trzecie zaufane strony)
      - Polityka bezpiecznego rozwoju oprogramowania (środowisko, kontrola wersji itp.)
      - Zasady bezpiecznej inżynierii systemowej - bezpieczeństwo we wszystkich obszarach:
        - Biznes, dane, aplikacje, technologia
      - Bezpieczne środowisko rozwoju oprogramowania

FDIS ISO/IEC 27001:2013

- OBSZARY – cd
  - 15. Relacje z dostawcami
    - Rozwiniecie 3 wymagań z poprzedniej wersji => 6 zupełnie nowych
  - 16. Zarządzanie incydentami związanymi z bezpieczeństwem informacji
    - Nowe
      - Ocena zdarzenia związanego z bezpieczeństwem
      - Reagowanie na incydent związanego z bezpieczeństwem (wydzielony z 13.2.1)
    - Zbieranie materiału dowodowego - procedura
  - 17. Aspekty bezpieczeństwa w zarządzaniu ciągłością działania
    - Zapisy bardzo uogólnione, brak szczegółów nt. BCP/DRP
    - Dodano – redundancję (komponenty, systemy)

FDIS ISO/IEC 27001:2013

OBSZARY – cd

- 18 Zgodność
  - Uszczegółowienie
  - Przeniesiono – niezależny przegląd bezpieczeństwa informacji

Podsumowanie

- Skrócenie i uogólnienie istniejących wymagań
- Dodanie wymagań z nowych obszarów (zbliżenie do ISO/IEC 20000)
- Konieczność znajomości nowej ISO/IEC 27002
  - klucz do zrozumienia załącznika A z ISO/IEC 27001

Kompetencje Asseco

Kompetencje Asseco

- Możliwe wsparcie podmiotów publicznych przez Pion Integracji Asseco Poland SA
  - Wdrażanie systemów zabezpieczeń
    - Ochrona kryptograficzna w urządzeniach sieciowych
    - FW, IPS, WAF, DBF, SIEM, Systemy dwuskładnikowego uwierzytelnienia, IdM, SSO
  - Wdrażanie SZBI
    - Projektowanie wdrożenia SZBI
      - Zdefiniowanie procesów i potrzebnych zasobów
    - Szacowanie ryzyka
    - Opracowanie dokumentacji
    - Audyty bezpieczeństwa
    - Projekty technicznych systemów bezpieczeństwa

Dziękujemy

KONTAKT
Janusz.cendrowski @asseco.pl
Janusz.zmudzinski@asseco.pl