Krajowe Ramy Interoperacyjności – obowiązkowe wyzwanie dla JST w ujęciu norm ISO

JANUSZ CZAUDERNA
tel. 505 328 1oo
janusz@czauderna.pl

Krajowe Ramy Interoperacyjności

stanowią zbiór zasad i sposobów postępowania podmiotów w celu zapewnienia systemom informatycznym interoperacyjności działania, rozumianej jako zdolność tych systemów oraz wspieranych przez nie procesów do wymiany danych oraz do dzielenia się informacjami i wiedzą

opisanych w

rozporządzeniu 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 r., poz. 526 ze zm.)*

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

Celem kontroli NIK była ocena wdrażania wybranych wymagań określonych w rozporządzeniu KRI.

Ocenie poddano następujące, wybrane kwestie: (...)

- działania burmistrzów oraz prezydentów miast w celu realizacji wymagań wprowadzonych rozporządzeniem KRI, dotyczących w szczególności:

  – dostosowania posiadanych systemów informatycznych do współpracy z innymi systemami/rejestrami informatycznymi,

  – stopnia wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

Najwyższa Izba Kontroli, pozytywnie ocenia działania podjęte przez burmistrzów i prezydentów miast w celu dostosowania objętych kontrolą systemów teleinformatycznych do współpracy z innymi systemami/rejestrami, jednakże NIK sformułowała wiele uwag w tym zakresie.

Większość z kontrolowanych systemów informatycznych (72 z 77) współpracowało z innymi systemami informatycznymi urzędów i tym samym spełniało minimalne wymogi interoperacyjności, o których mowa w § 5 ust. 3 pkt 3 rozporządzenia KRI. Niemniej tylko dwanaście (16,7%) systemów współpracowało z innymi systemami urzędu w sposób w pełni zautomatyzowany, tj. na poziomie najbardziej pożądanym, a pięć systemów (6,9%) bezpośrednio korzystało z danych gromadzonych w zewnętrznych systemach/rejestrach publicznych (zasada referencji), takich jak np. rejestr centralny PESEL czy też System Informacji Przestrzennej.

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

NIK, ze względu na liczne nieprawidłowości, ogólnie negatywnie ocenia działania burmistrzów i prezydentów miast w zakresie zarządzania bezpieczeństwem informacji w urzędach, o którym mowa w

§ 20 rozporządzenia KRI.

NIK stwierdziła nieprawidłowości w tym obszarze w 21 z 24 (87,5%) skontrolowanych urzędów miast, z których sześć oceniła negatywnie.

Zdaniem NIK, stwierdzone nieprawidłowości mogą skutkować utratą dostępności, integralności i poufności informacji przetwarzanych w systemach informatycznych urzędów wykorzystywanych do elektronicznej komunikacji i świadczenia usług

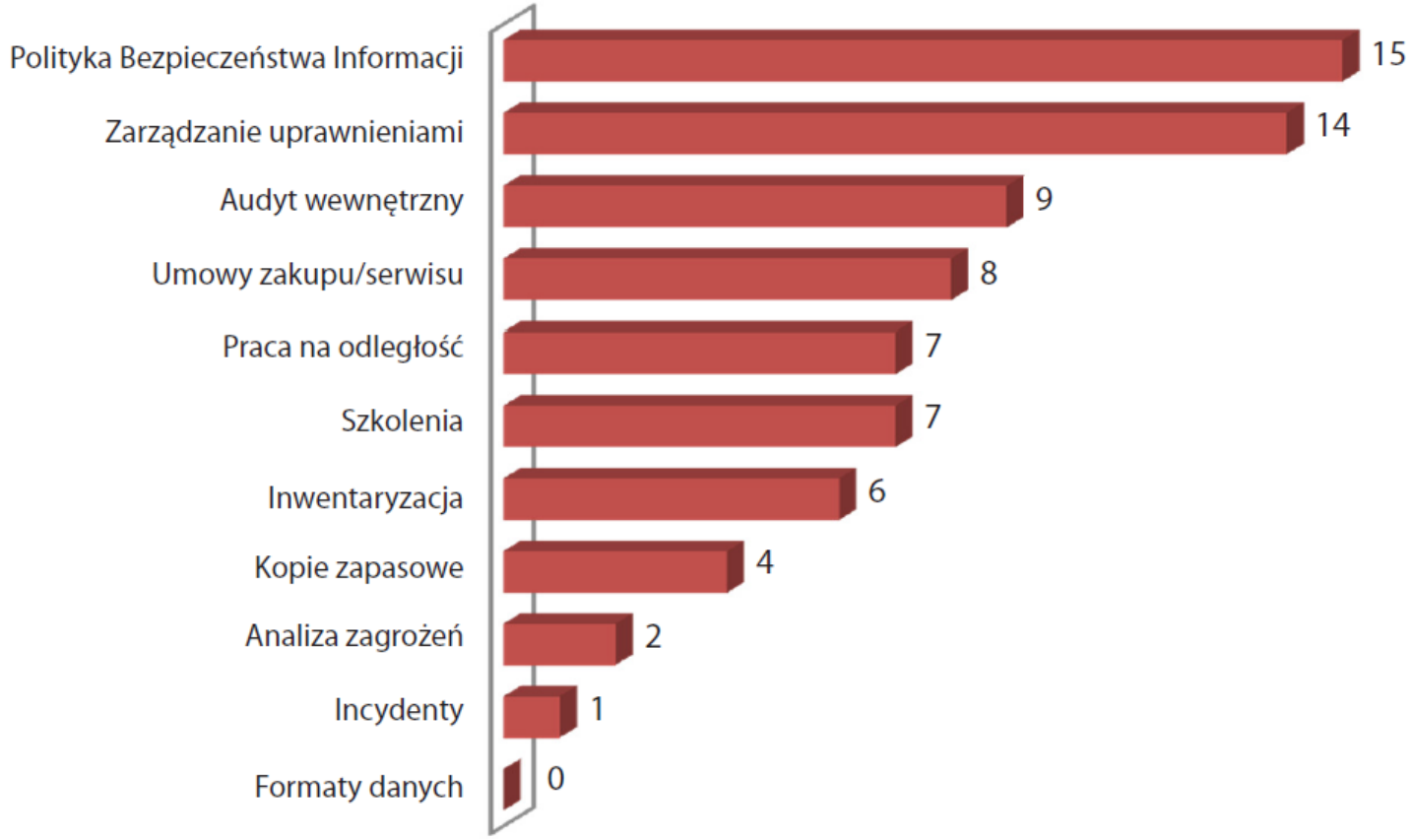
Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

Nieprawidłowości dotyczyły przede wszystkim:

- braku w kontrolowanych urzędach całościowej Polityki Bezpieczeństwa Informacji (poza bezpieczeństwem danych osobowych), która jest wymagana przepisami § 20 ust. 1 i 3 rozporządzenia KRI;
- niewłaściwego zarządzania uprawnieniami użytkowników w zakresie dostępu do systemów informatycznych, co było niezgodne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI;
- nieprzeprowadzania corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KR I;
- Braku w umowach na zakup lub serwis sprzętu komputerowego/oprogramowania zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych w związku z realizacją tych umów przez wykonawców, co było niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

Liczba kontrolowanych urzędów, w których stwierdzono nieprawidłowości przy realizacji poszczególnych zadań w obszarze zarządzania bezpieczeństwem informacji



Źródło: Wyniki kontroli.

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

W 15 urzędach, tj. 62,5% objętych kontrolą nie opracowano i nie wdrożono Polityki Bezpieczeństwa Informacji (dalej PBI), która jest elementem systemu zarządzania bezpieczeństwem informacji.

Przepis § 20 ust. 1 rozporządzenia KR I zobowiązuje podmioty realizujące zadania publiczne m.in. do opracowania, ustanowienia, wdrożenia, monitorowania i dokonywania przeglądów systemu zarządzania bezpieczeństwem informacji. W myśl § 20 ust. 3 tego rozporządzenia wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione, jeżeli system ten został opracowany na podstawie Polskich Norm

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

Nie opracowano pisemnych procedur zarządzania uprawnieniami użytkowników do pracy w systemach informatycznych w jednym urzędzie32, a w 13 innych urzędach (54,2%) stwierdzono nieprawidłowości polegające na niedochowaniu wymogów określonych w § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI.

Stwierdzono:

– w przypadku 18 osób (z 421 pracowników objętych badaniem) stwierdzono, że wystąpiły nieprawidłowości w zakresie nadawania uprawnień do realizowanych zadań

– konta w systemach informatycznych 20 byłych pracowników (z 310 objętych badaniem) nie zostały zablokowane i pozostawały wciąż aktywne

– w przypadku 82 pracowników wykonujących zadania w systemach informatycznych (z 350 objętych badaniem) stwierdzono, że mieli oni możliwość zainstalowania na użytkowanych przez nich komputerach dowolnego oprogramowania. Sytuacja taka wystąpiła w dziewięciu urzędach (37,5%), a w czterech z nich wszyscy badani użytkownicy systemów informatycznych niebędący pracownikami służb informatycznych posiadali uprawnienia administratora systemu, w związku z czym mogli samodzielnie instalować dowolne oprogramowanie

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

W ośmiu skontrolowanych urzędach (33,3%) w umowach na zakup lub serwis sprzętu komputerowego/oprogramowania dotyczących badanych systemów informatycznych, brak było zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych przez wykonawców w związku z realizacją tych umów, co było niezgodne z przepisem § 20 ust. 2 pkt 10 rozporządzenia KRI.

Zapisów takich nie zawarto w umowach spośród 63 umówo bjętych badaniem (44,4%). Wskazywane przez kontrolowanych „uzgodnienia nieformalne" bez wprowadzenia odpowiednich zapisów w umowach, zdaniem NIK mogą istotnie utrudniać zamawiającemu skuteczne dochodzenie odpowiedzialności usługodawcy w przypadku niedochowania tajemnicy informacji, do jakich miał on dostęp w związku z realizowaniem umowy

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

W dziewięciu urzędach (tj. 37,5%) w okresie objętym kontrolą nie przeprowadzono audytu w zakresie bezpieczeństwa informacji w systemach informatycznych, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI.

Powyższą nieprawidłowość tłumaczono m.in. faktem, że audyt o podobnej tematyce został przeprowadzony w latach wcześniejszych, a także brakiem pracowników posiadających niezbędną wiedzę i doświadczenia dla przeprowadzenia takiego audytu

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

Burmistrzowie i Prezydenci miast powinni:

1. Przeprowadzać , przy zakupie nowych lub modernizacji już funkcjonujących systemów informatycznych, analizy zapewnienia interoperacyjności (współdziałania) z innymi systemami w celu optymalnego wykorzystywania danych już zgromadzonych we własnych i zewnętrznych systemach/rejestrach informatycznych.

2. Rozważyć możliwość wprowadzenia systemu elektronicznego zarządzania dokumentacją jako podstawowego sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw.

3. Opracować i wdrożyć PB I oraz konsekwentnie stosować procedury zarządzania bezpieczeństwem informacji przetwarzanych w urzędzie, obejmujące wszystkie elementy, o których mowa w § 20 rozporządzenia KR I.
(...)

4. Zapewnić do 31 maja 2015 r. dostosowanie prezentowanych informacji w systemach teleinformatycznych urzędów, w tym na stronach internetowych i BIP do odbioru przez osoby niepełnosprawne, stosownie do wymagań określonych w § 19 rozporządzenia KRI.

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

W 13 urzędach (54,2%) nie ustanowiono zasad (procedur) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI.

W siedmiu urzędach jako przyczynę nieopracowania i niewdrożenia procedur bezpiecznej pracy na urządzeniach mobilnych poza urzędem wskazywano m.in., że nie wykorzystywano urządzeń do pracy poza urzędem, jak również brak możliwości realizowania zdalnie zadań z wykorzystaniem systemów informatycznych jednostki.

Jakkolwiek NIK nie formułowała w tych przypadkach wniosków o opracowanie takich procedur, to jednak jest zdania, że **podstawową funkcją urządzeń mobilnych, takich jak posiadane przez urzędy laptopy jest praca w dowolnym miejscu z wykorzystaniem technik komunikacyjnych. A zatem nie można wykluczyć, że praca może być niekiedy wykonywana również poza siedzibą urzędu, co powoduje szereg zagrożeń dla bezpieczeństwa danych zapisanych w tych urządzeniach (np. kradzież, modyfikacja danych).**

Wyniki kontroli NIK stanu wdrożenia wymagań KRI w JST wg stanu na 2014 r

Termin „istotna modernizacji", § 23 rozporządzenia KRI

(…) w piśmie z dnia 10 sierpnia 2011 r. nr DS I-WP ISI-0230-9-1/2011 przedstawiono wyjaśnienie, że „Poprzez istotną Modernizację" należy rozumieć modernizację co najmniej na poziomie 10% ogólnej wartości systemu".

W opinii NIK, brak precyzyjnego określenia pojęcia „istotnej modernizacji" może utrudniać interpretację tego pojęcia przez podmioty realizujące zadania publiczne. Ma to znaczenie w aspekcie realizacji obowiązku określonego w § 23 rozporządzenia KRI, który zobowiązuje ww. podmioty do dostosowania użytkowanych systemów teleinformatycznych do wymogów zawartych w rozdziale IV rozporządzenia KRI, nie później niż w dniu ich pierwszej istotnej modernizacji.

Rozporządzenie

DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 16 maja 2012 r.

Poz. 526

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[1)]

Interoperacyjność

Interoperacyjność

Interoperacyjność oznacza zdolność systemów ICT i procesów biznesowych przez nie wspieranych do wymiany danych i wspierania udostępniania informacji i wiedzy.

Ramy interoperacyjności (*interoperability framework*) można zdefiniować jako zestaw standardów i wytycznych opisujących sposób, w który organizacje zgodziły się - lub zgodzą się - współdziałać ze sobą.

Rozporządzenie określa

- Krajowe Ramy Interoperacyjności
- Minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej
- Minimalne wymagania dla systemów teleinformatycznych

Minimalne wymagania dla systemów teleinformatycznych

Specyfikacja formatów danych oraz protokołów komunikacyjnych i szyfrujących, które mają być stosowane w oprogramowaniu interfejsowym

Sposoby zapewnienia bezpieczeństwa przy wymianie informacji

Standardy techniczne zapewniające wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgenicznej

Sposoby zapewnienia dostępu do informacji podmiotów publicznych dla osób niepełnosprawnych

Interoperacyjność osiąga się przez:

UJEDNOLICENIE

(zastosowanie kompatybilnych norm, standardów i procedur)

WYMIENNOŚĆ

(możliwość zastąpienia produktu, procesu lub usługi bez zakłócenia wymiany informacji)

ZGODNOŚĆ

(przydatność produktów, procesów lub usług przeznaczonych do wspólnego użytkowania)

Interoperacyjność:

- organizacyjna
- semantyczna
- technologiczna

Interoperacyjność organizacyjna

- umożliwia efektywne współdziałanie podmiotów publicznych, obywatela i biznesu;

- określa w jaki sposób organizacje takie jak ministerstwa, biura i rządy definiują swoje cele, modelują procesy biznesowe i w inny sposób współdziałają na polu wymiany informacji w celu zrealizowania określonych zadań;

- zapewnia:
  - współpracę wszystkich instytucji które będą dokonywać wymiany informacji;
  - stosowanie ustaleń wielostronnych;
  - określenie granic swobody dla poszczególnych organizacji;
  - określenie jakości informacji przekazywanych przez poszczególne organizacje.

Interoperacyjność semantyczna

- oznacza zdolność dwóch lub więcej systemów komputerowych do wymiany informacji oraz precyzyjnego i automatycznego określania *znaczenia* tych informacji – zarówno przez nadawcę jak i odbiorcę;
- umożliwia efektywną wymianę informacji pomiędzy, podmiotami publicznymi, obywatelem i biznesem;
- zapewnia:
  - usunięcie konfliktów na poziomie danych (różna interpretacja podobnych danych – semantyka),
  - usunięcie konfliktów na poziomie struktury danych (logika, niespójność metadanych – synktatyka);
- umożliwia zarządzanie konfliktami semantycznymi w sposób automatyczny.

Interoperacyjność technologiczna

- zapewnia technologię wymiany danych pomiędzy systemami teleinformatycznymi administracji publicznej, obywatelem i biznesem

- zapewnia wspólnie funkcjonowanie pod względem technicznym systemów informatycznych współpracujących organizacji

Czynniki warunkujące prawidłowe funkcjonowanie interoperacyjności

- dostępność informacji/usług,
- wielojęzyczność i urządzenia wieloplatformowe,
- bezpieczeństwo, ochrona prywatności,
- wolne oprogramowanie i otwarte standardy,
- subsydiarność,
- wspólne definicje,
- upowszechnianie wspólnych definicji,
- zaufanie, wiarygodność co do wspólnych definicji,
- utrzymanie i rozwój wspólnych definicji,
- zarządzanie interoperacyjnością.

Zarządzanie interoperacyjnością

koordynacja i uzgadnianie procesów administracyjnych i architektury informacji;

identyfikacja i likwidacja wszelkich możliwych barier (prawnych, kulturowych, innych) w celu agregacji usług i wymiany informacji;

dostosowanie przepisów prawnych.

Obecna rola systemów ICT administracji:

1. Służą usprawnieniu wewnętrznego funkcjonowania urzędów. To najstarsza i (teoretycznie) najmniej skomplikowana forma wsparcia administracji IT obejmująca np. systemu obiegu dokumentów, wewnętrzne systemy informacyjne (intranety) itp.
2. Służą realizacji usług funkcji elektronicznej administracji (eGovernment), czyli umożliwiają obywatelom i firmom załatwianie spraw urzędowych przez Internet.
3. Dostarczają sferze politycznej informacji umożliwiających sprawne i skuteczne rządzenie Państwem (ang. Governance) obejmuje to w szczególności hurtownie danych i systemy klasy Bussiness Intelligence.
4. Służą zapewnieniu przejrzystości funkcjonowania administracji . To najnowsza, ale dynamicznie rozwijająca się funkcja.

We wszystkich wariantach kluczowa jest wymiana informacji pomiędzy systemami.

Zmiana roli systemów IT w administracji

Ewolucja modelu dojrzałości eGovermnent

Poziom 1	
Informacja	Komunikacja jednokierunkowa. Strona WWW obejmuje informacje ogólne (np. kontaktowe)

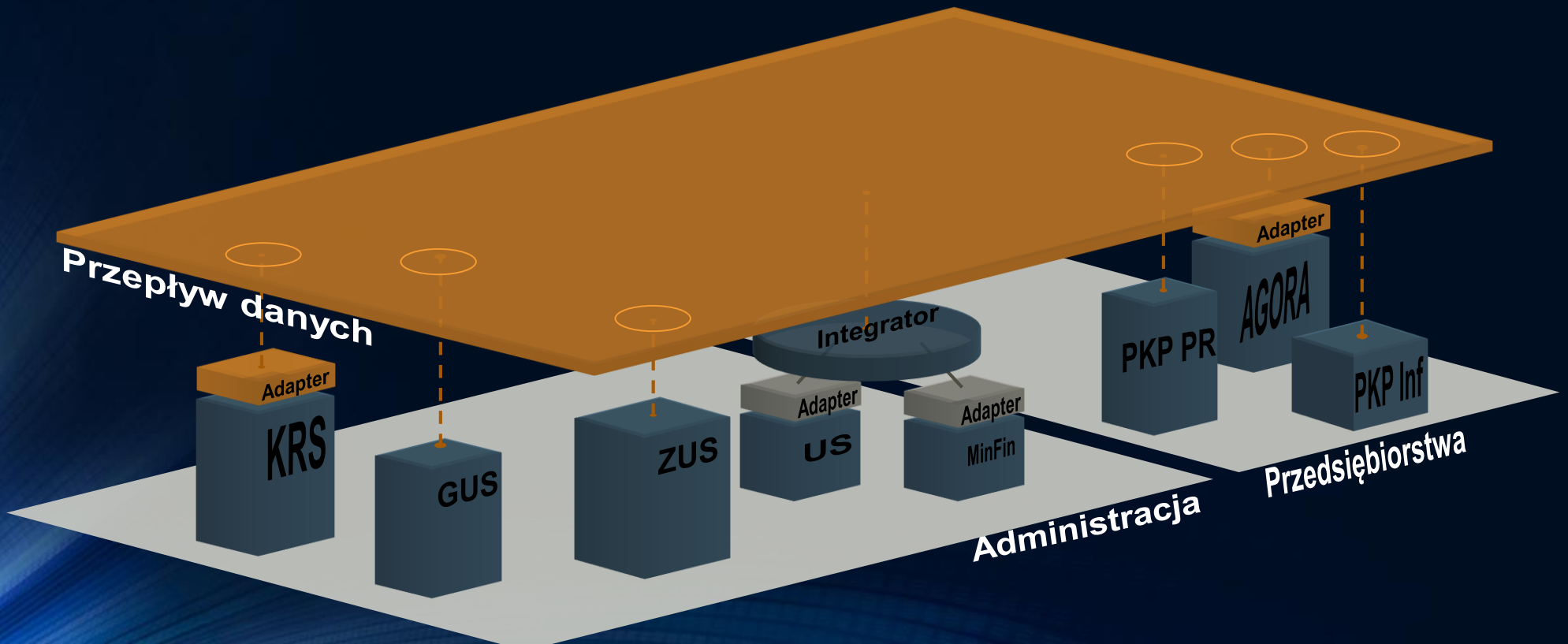
Poziom 2	
Interakcja	Strona WW Urzędu zawiera informacje niezbędne do załatwiania konkretnych spraw np. linki do formularzy elektronicznych

Poziom 3	
Transakcja	Sprawa może być już całkowicie załatwiona poprzez złożenie wniosku poprzez Sieć na podstawie danych które już ma Urząd

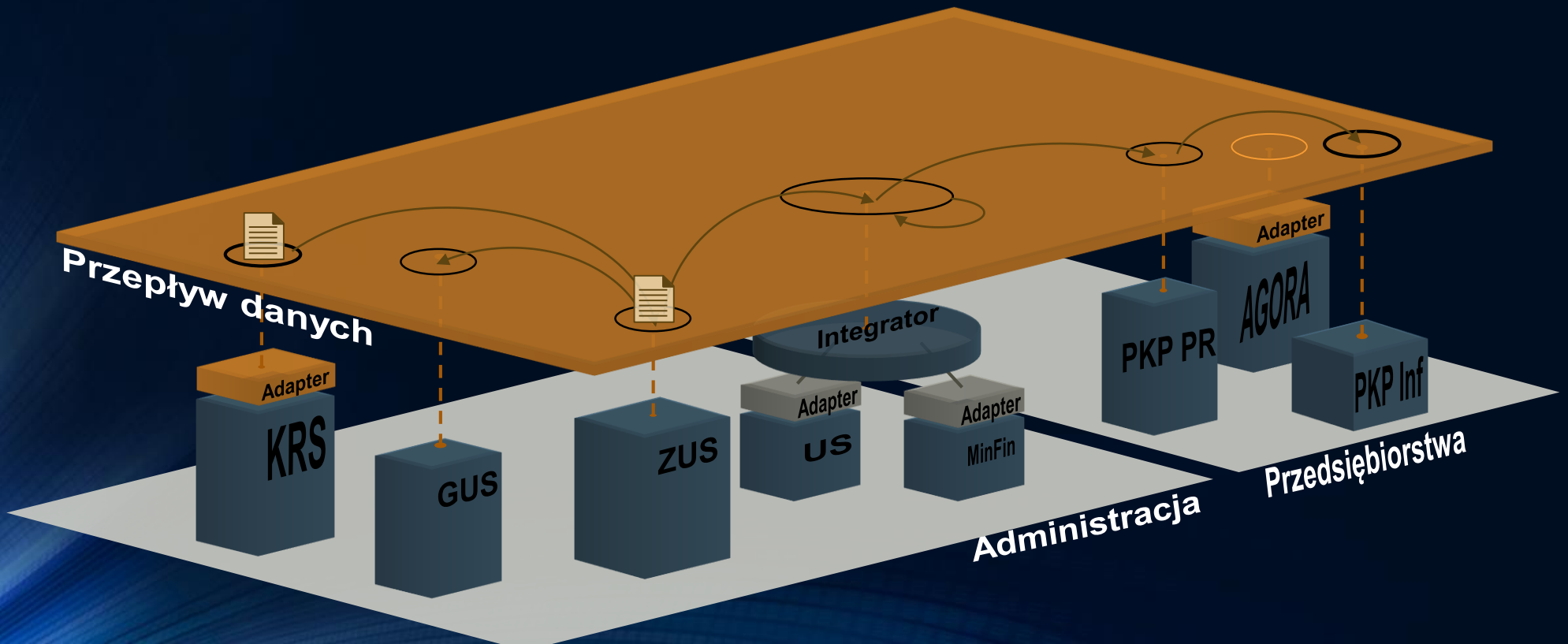
Poziom 4	
Transformacja	Sprawa może być załatwiona całkowicie via Internet, w komunikacji dwukierunkowej pomiędzy urzędem a klientem

Poziom 5	
Personalizacja	W administracji (NIE w jednym urzędzie) funkcjonują mechanizmy bezpośredniej interakcji i współpracy z klientem przy załatwianiu jego spraw

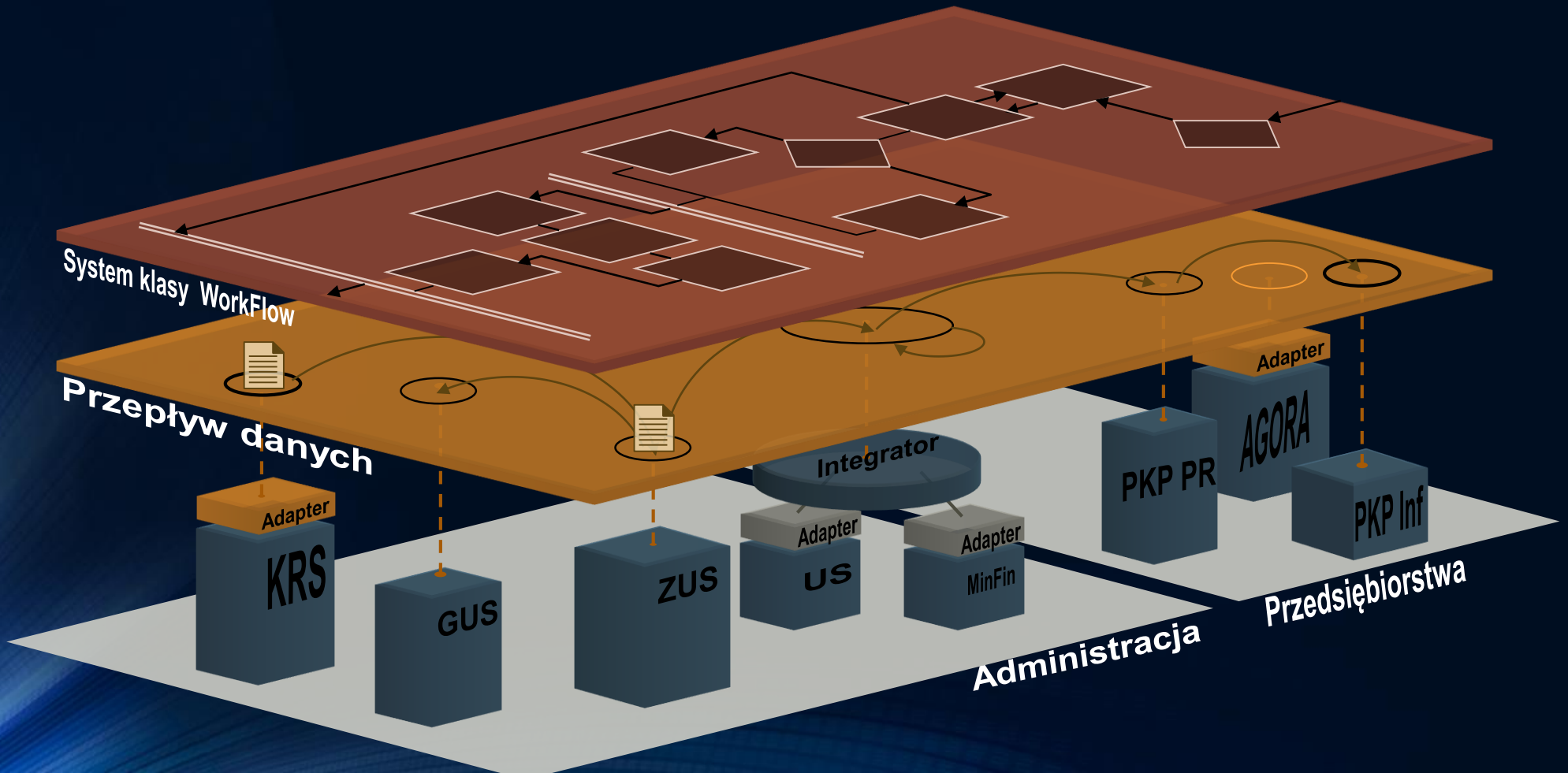
Rozproszona struktura (e-)administracji



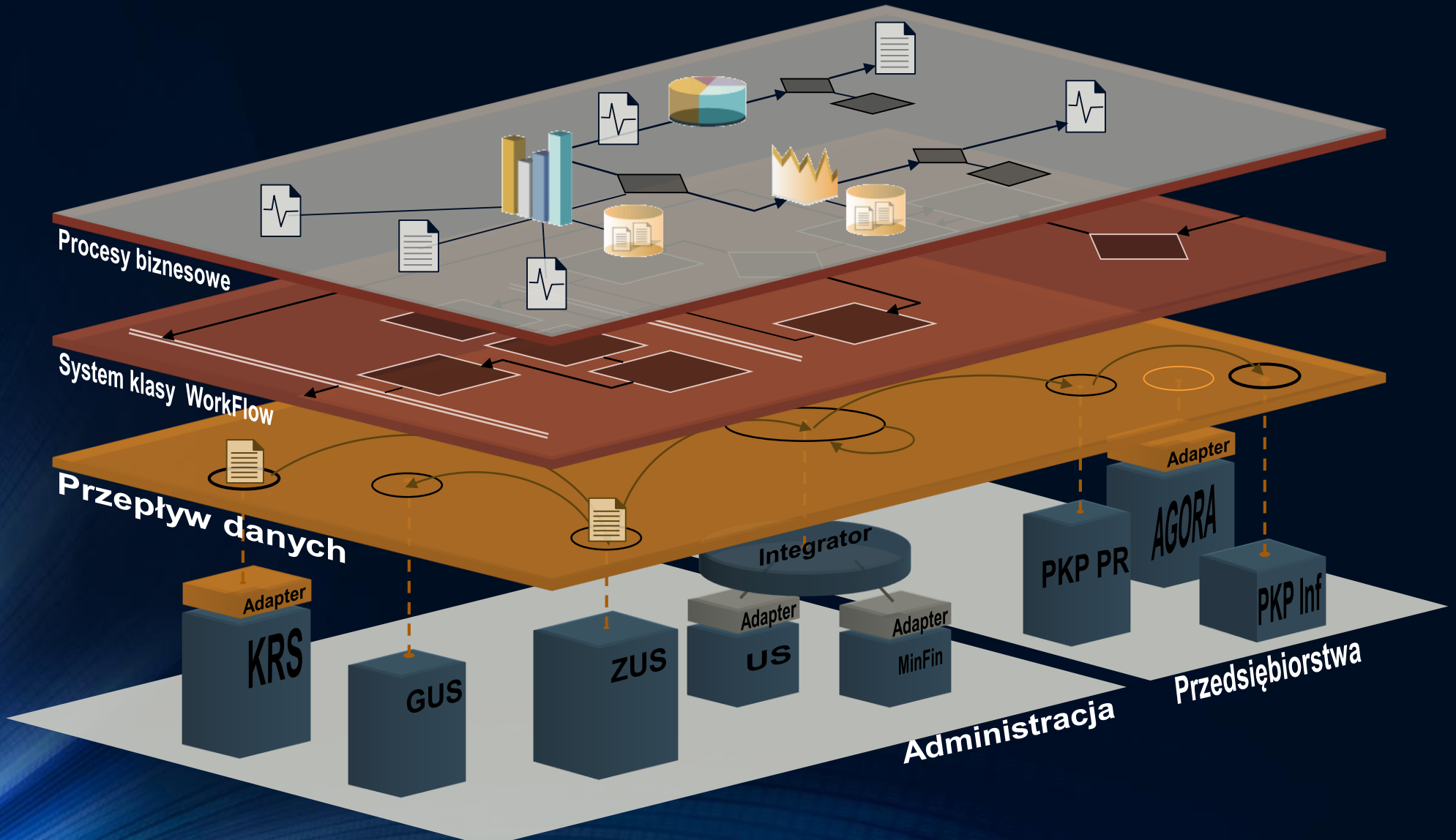
Rozproszona struktura (e-)administracji



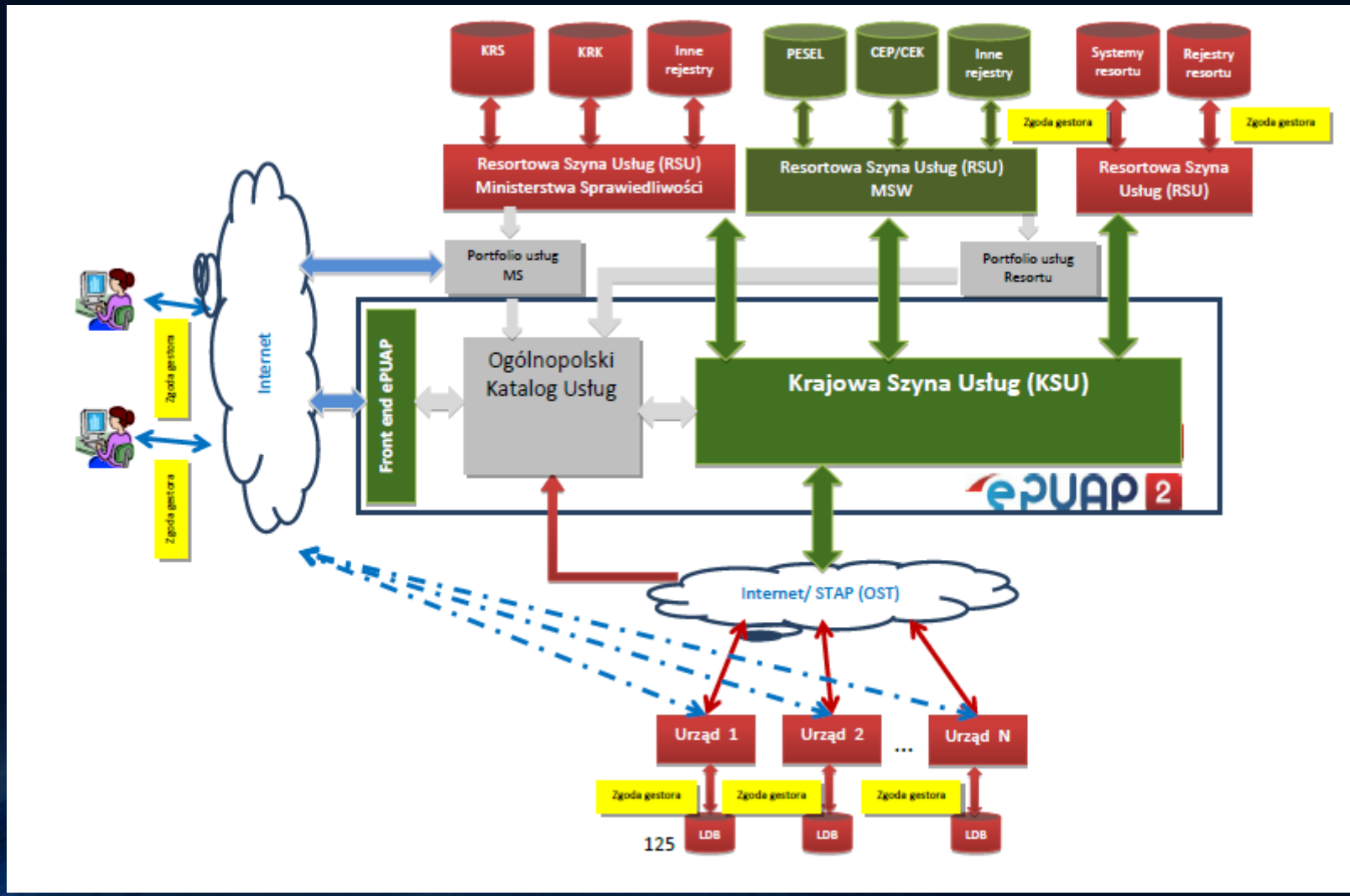
Rozproszona struktura (e-)administracji



Rozproszona struktura (e-)administracji



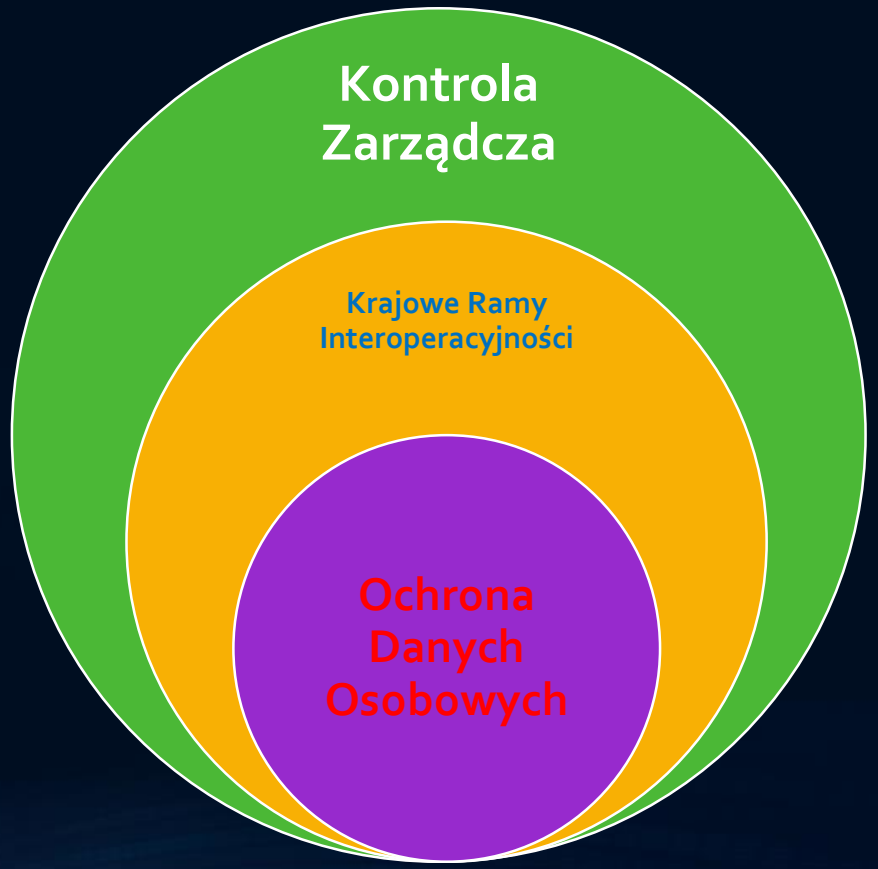
Informatyzacja Zintegrowana



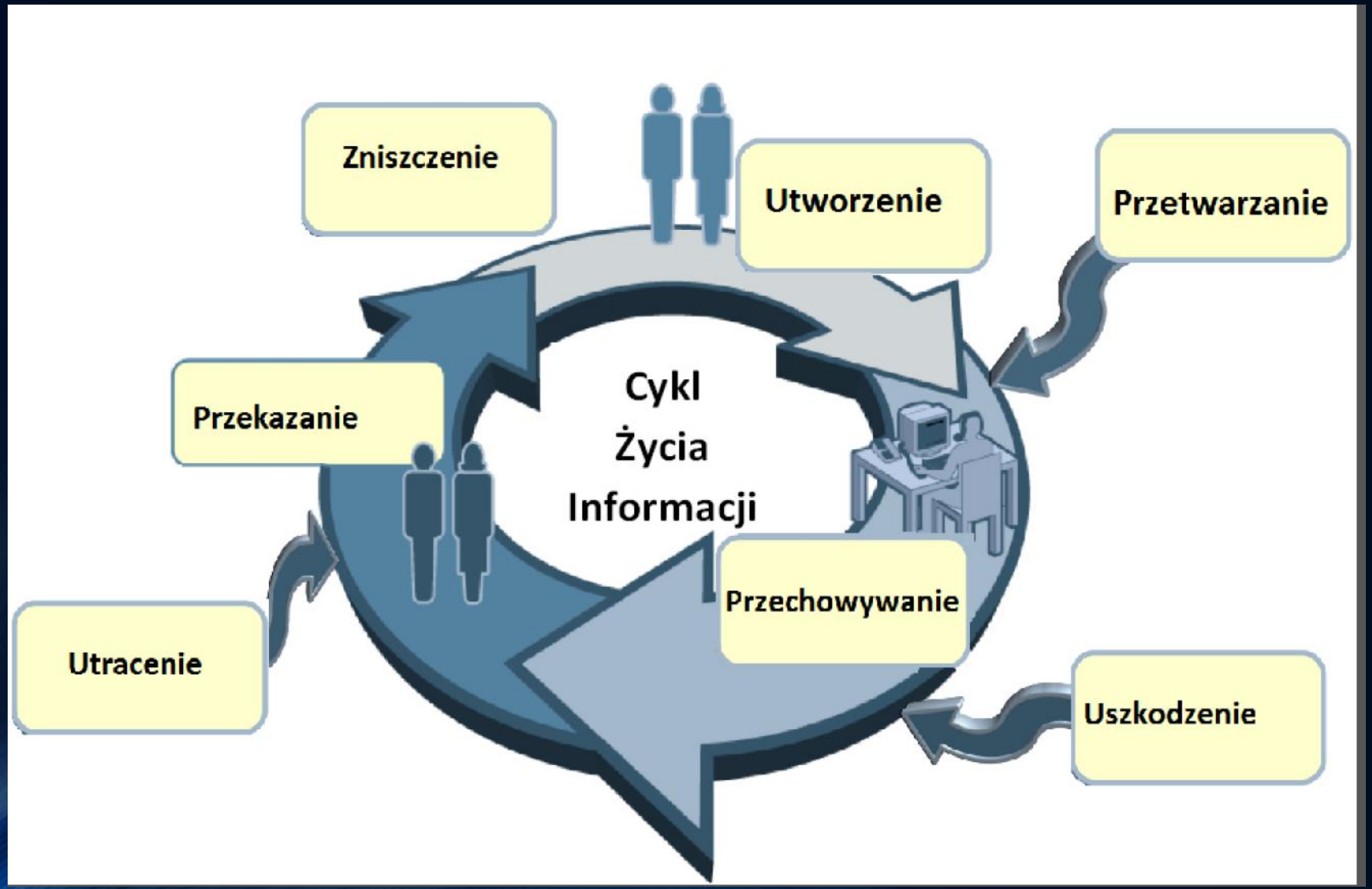
Zródło: MAiC 2014

INFORMACJA *(udokumentowana)*

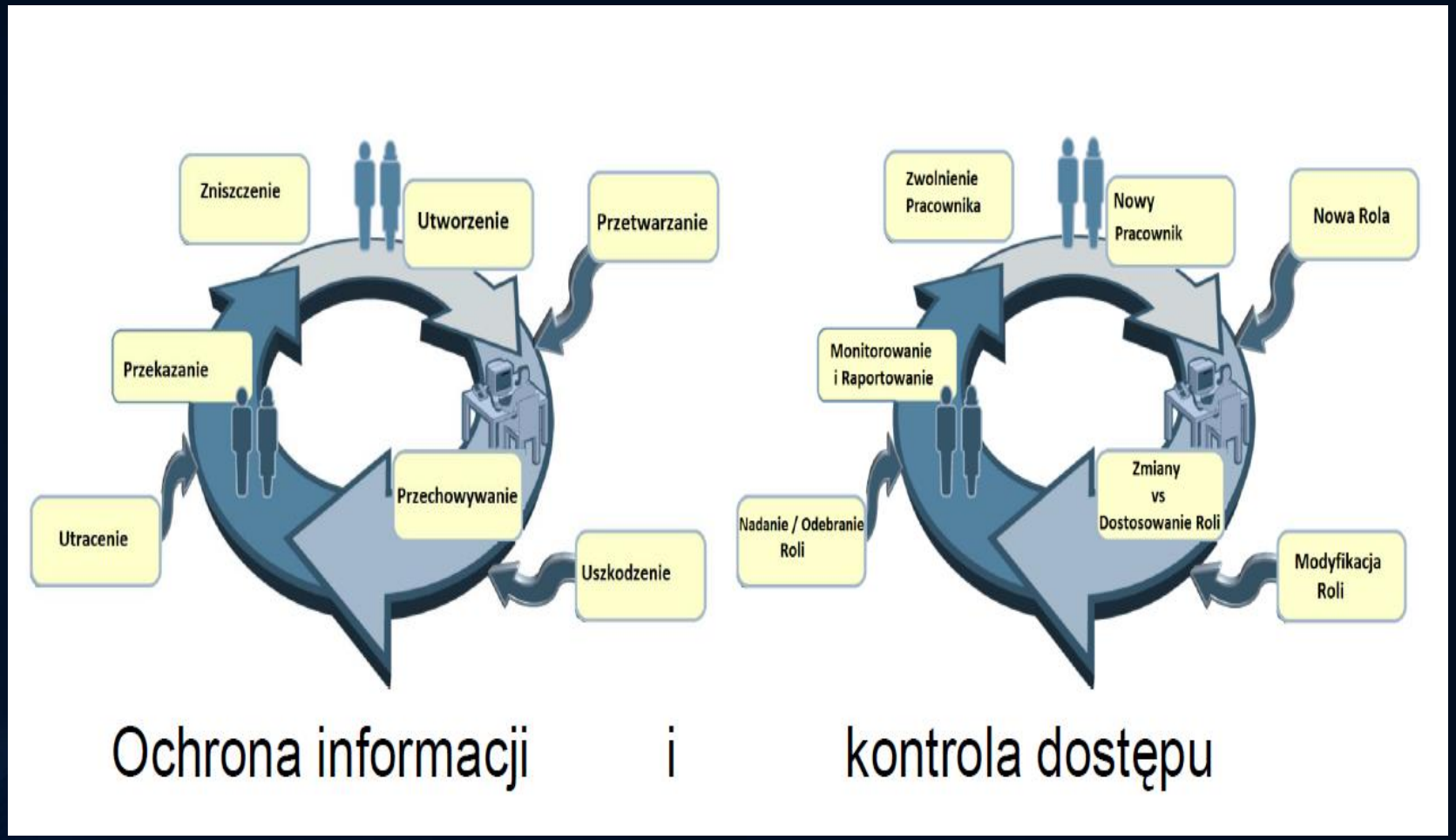
Ochrona informacji – założenia systemowe JFP

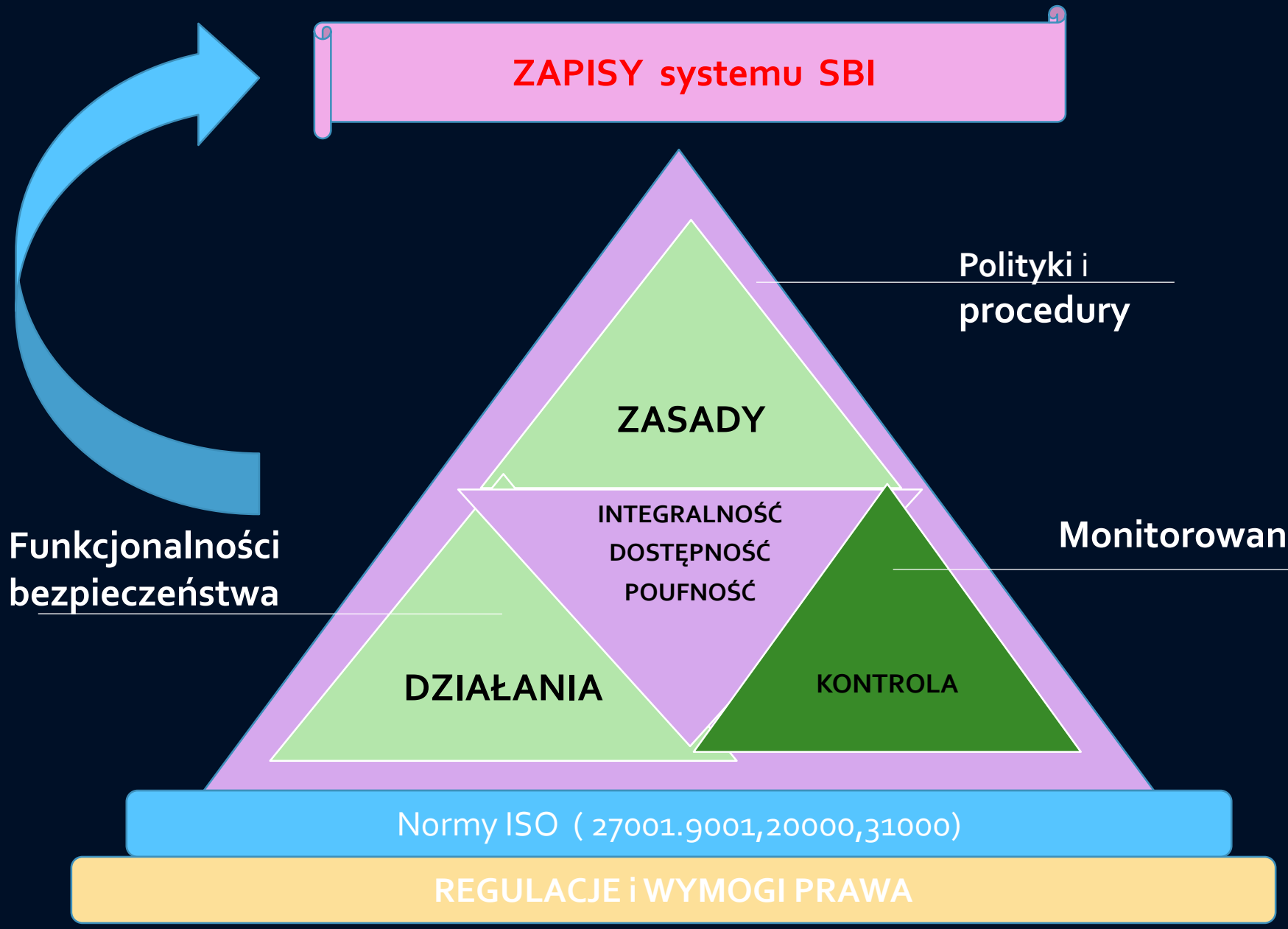


Cykl życia informacji



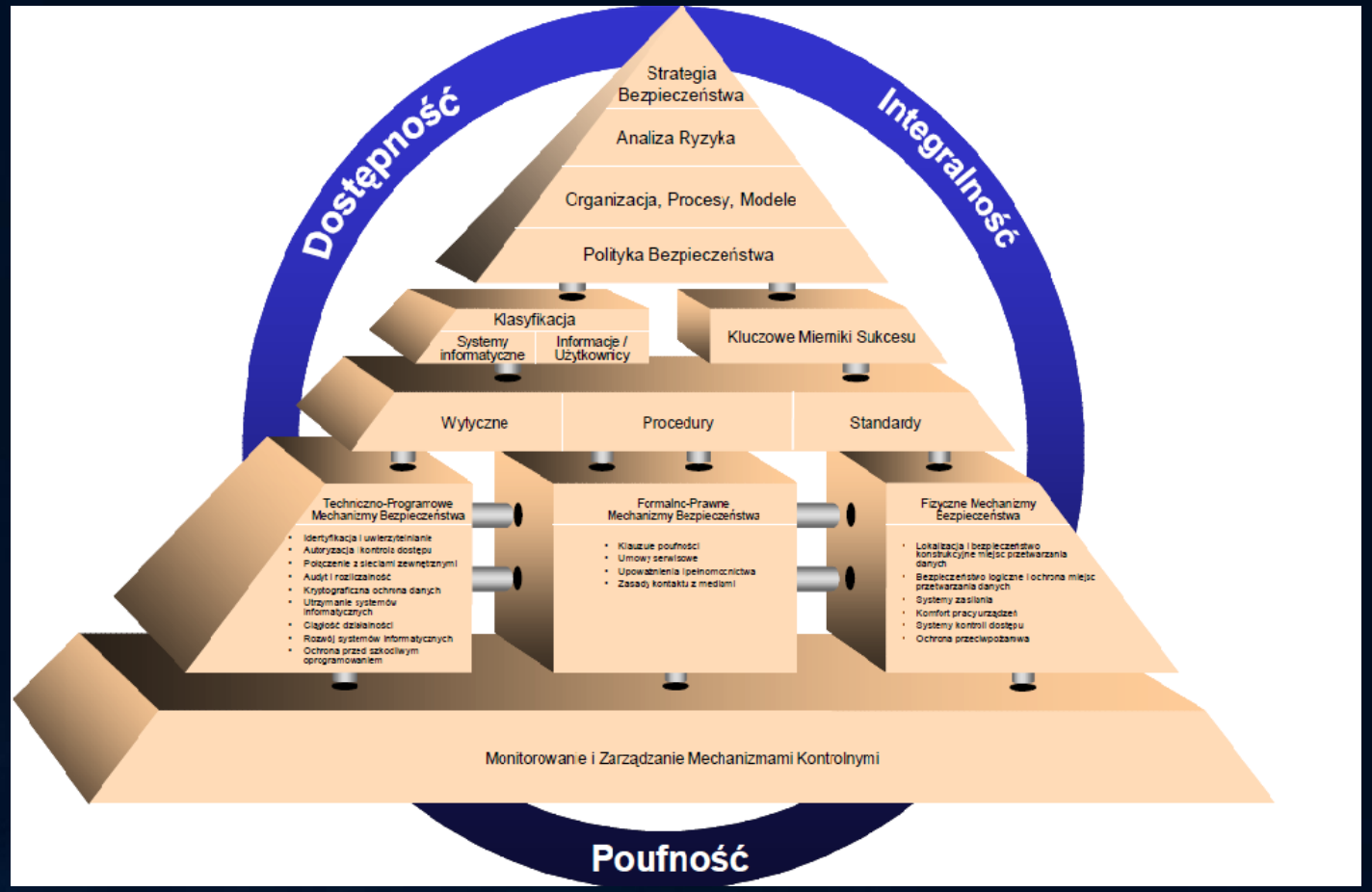
Zarządzanie Informacją w organizacji





SYSTEM MONITOROWANIA BEZPIECZEŃSTWA

Model zarządzania Systemem Bezpieczeństwa Informacji w organizacji



DZ.U. poz. 526 z 12 kwietnia 2012

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

Rozdział I: **Przepisy ogólne**

§ 1. Rozporządzenie określa:

1) Krajowe Ramy Interoperacyjności;

2) minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej;

3) minimalne wymagania dla systemów teleinformatycznych, w tym:

a) **specyfikację formatów** danych oraz protokołów komunikacyjnych i szyfrujących, które mają być stosowane w oprogramowaniu interfejsowym,

b) sposoby zapewnienia bezpieczeństwa przy wymianie informacji,

c) **standardy techniczne zapewniające** wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgranicznej,

d) sposoby zapewnienia dostępu do zasobów informacji podmiotów publicznych dla osób niepełnosprawnych.

Rozdział II: **Krajowe Ramy Interoperacyjności**

§ 3. 1. Krajowe Ramy Interoperacyjności określają:

1) sposoby postępowania podmiotu realizującego zadania publiczne w zakresie doboru środków, metod i standardów wykorzystywanych do **ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalania** systemu teleinformatycznego wykorzystywanego do realizacji zadań tego podmiotu oraz procedur organizacyjnych.

Rozdział II : **Krajowe Ramy Interoperacyjności**

4. Interoperacyjność na poziomie technologicznym osiągana jest przez:

1) stosowanie minimalnych wymagań dla systemów teleinformatycznych, określonych w rozdziale IV;

2) stosowanie regulacji zawartych w przepisach odrębnych, a w przypadku ich braku uwzględnienia **postanowień odpowiednich**

Polskich Norm, norm międzynarodowych lub standardów uznanych w drodze dobrej praktyki przez organizacje międzynarodowe.

Rozdział III: Minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej

6. Podmioty realizujące zadania publiczne z wykorzystaniem wymiany informacji za pomocą środków komunikacji elektronicznej lub za pomocą pism w formie dokumentów elektronicznych sporządzonych według wzorów elektronicznych, w których mają zastosowanie obiekty, o których mowa w ust. 1, stosują strukturę danych cech informacyjnych tych obiektów zgodną ze strukturą publikowaną przez ministra właściwego do spraw informatyzacji w postaci schematów XML w repozytorium interoperacyjności na podstawie wniosków organu prowadzącego rejestr referencyjny właściwy dla danego typu obiektu.

Rozdział III: Minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej

§ 11. 1. Podmiot publiczny prowadzący rejestr publiczny, wydając informacje z tego rejestru w drodze wymiany, jest obowiązany zapewnić rozliczalność takiej operacji.

2. Podmiot otrzymujący informacje z rejestru publicznego w drodze wymiany jest obowiązany do jej ochrony na poziomie nie mniejszym niż ten, który ma zastosowanie w tym rejestrze.

Rozdział IV: **Minimalne wymagania dla systemów teleinformatycznych**

§15. 1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

2. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: **PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.**

Rozdział IV: **Minimalne wymagania dla systemów teleinformatycznych**

§ 16. 1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne **wyposaża się w składniki sprzętowe lub** oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

2. W przypadku gdy w danej sprawie brak jest przepisów, norm lub standardów, o których mowa w ust. 1, stosuje sięstandardy uznane na poziomie międzynarodowym, w szczególności opracowane przez:

1) Internet Engineering Task Force (IETF) i publikowane w postaci Request For Comments (RFC),

2) World Wide Web Consortium (W3C) i publikowane w postaci W3C Recommendation (REC)

– **adekwatnie do potrzeb wynikających z realizowanych zadań oraz bieżącego stanu technologii informatycznych**.

Rozdział IV: **Minimalne wymagania dla systemów teleinformatycznych**

§ 17. 1. Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego **przez normę ISO/IEC 10646** wraz ze zmianami lub normę ją zastępującą.

2. W uzasadnionych przypadkach dopuszcza się kodowanie znaków według standardu Unicode UTF-16 określonego przez normę, o której mowa w ust. 1.

3. Zastosowanie kodowania, o którym mowa w ust. 2, **nie może negatywnie wpływać na współpracę z systemami teleinformatycznymi** używającymi kodowania określonego w ust. 1.

§ 18. 1. Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia.

Rozdział IV: **Minimalne wymagania dla systemów teleinformatycznych**

§ 20. 1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający **poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność**.

2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez **kierownictwo podmiotu publicznego** warunków umożliwiających **realizację i egzekwowanie następujących działań:**

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania

służącego do przetwarzania informacji obejmującej

ich rodzaj i konfigurację;

Rozdział IV: **Minimalne wymagania dla systemów teleinformatycznych**

§ 20. 2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

2) utrzymywania **aktualności inwentaryzacji sprzętu i oprogramowania** służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;

3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji **posiadają stosowne uprawnienia** i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

5) *bezzwłocznej zmiany uprawnień*, w przypadku zmiany zadań osób, o których mowa w pkt 4;

6) zapewnienia **szkolenia osób zaangażowanych** w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

a) zagrożenia bezpieczeństwa informacji,

b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym **urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;**

Rozdział IV: **Minimalne wymagania dla systemów teleinformatycznych**

§ 20. 2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo *…ciag dalszy….*

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

a) monitorowanie dostępu do informacji,

b) czynności zmierzające do **wykrycia nieautoryzowanych** działań związanych z przetwarzaniem informacji,

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) zabezpieczenia informacji w sposób **uniemożliwiający** nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10) **zawierania w umowach serwisowych** podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

11) **ustalenia zasad postępowania z informacjami**, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

Rozdział IV: **Minimalne wymagania dla systemów teleinformatycznych**

§ 20. 2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo *…ciąg dalszy….*

zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

Rozdział IV
Minimalne wymagania dla systemów teleinformatycznych

§ 20. 2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo *…ciąg dalszy….*

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Rozdział IV: **Minimalne wymagania dla systemów teleinformatycznych**

§ 21. 1. Rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

2. W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:

1) systemu z uprawnieniami administracyjnymi;

2) konfiguracji systemu, w tym konfiguracji zabezpieczeń;

3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

Rozdział IV: **Minimalne wymagania dla systemów teleinformatycznych**

§15. 1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

2. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.

§ 3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie **Polskiej Normy PN-ISO/IEC 27001**, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;

2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;

3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Rozdział IV
Minimalne wymagania dla systemów teleinformatycznych

3. Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:

1) działań użytkowników nieposiadających uprawnień administracyjnych,

2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,

3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka.

4. Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych,

a w przypadku braku przepisów odrębnych przez dwa lata.

Norma ISO 27001

AKTUALNA norma to:

PN-ISO/IEC 27001:2014-12

która **zastąpiła** normę PN-ISO/IEC 27001:2007

czyli musimy zrealizować nowe wydanie dokumentacji systemu bezpieczeństwa informacji z uwzględnieniem wymagań ustawy o Ochronie danych osobowych

Rozdział V P**rzepisy przejściowe i końcowe**

§ 22. Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia należy dostosować do wymagań określonych **w § 19,** nie później niż w **terminie 3 lat od** dnia wejścia w życie niniejszego rozporządzenia.

§ 23. Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia na podstawie dotychczas obowiązujących przepisów należy dostosować do wymagań, o których mowa w rozdziale IV rozporządzenia, nie później niż w dniu ich pierwszej istotnej modernizacji przypadającej po wejściu w życie rozporządzenia.

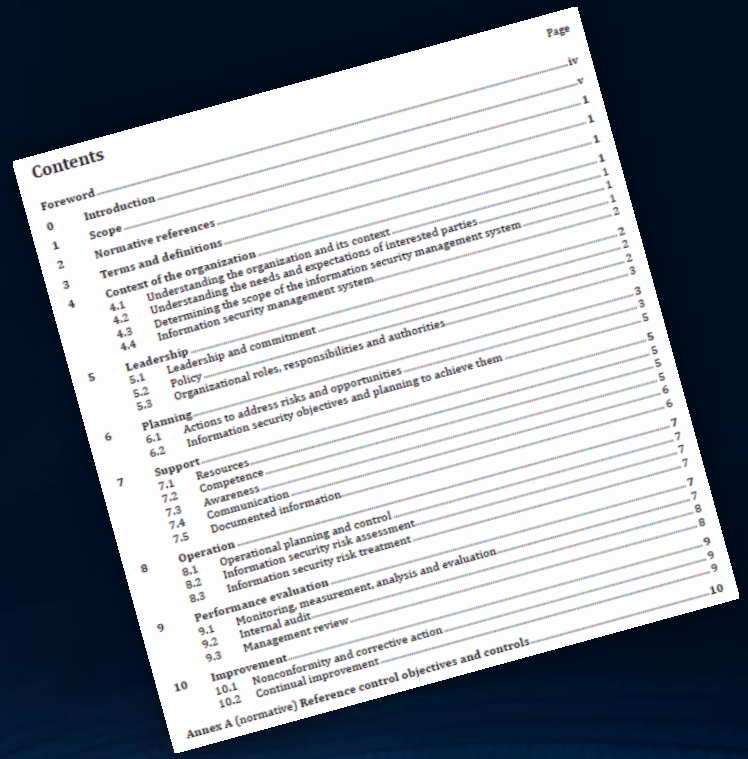
Norma PN-ISO/IEC 27001:2014-12

Wymagania ISO/IEC 27001:2014-12
Technika informacyjna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania

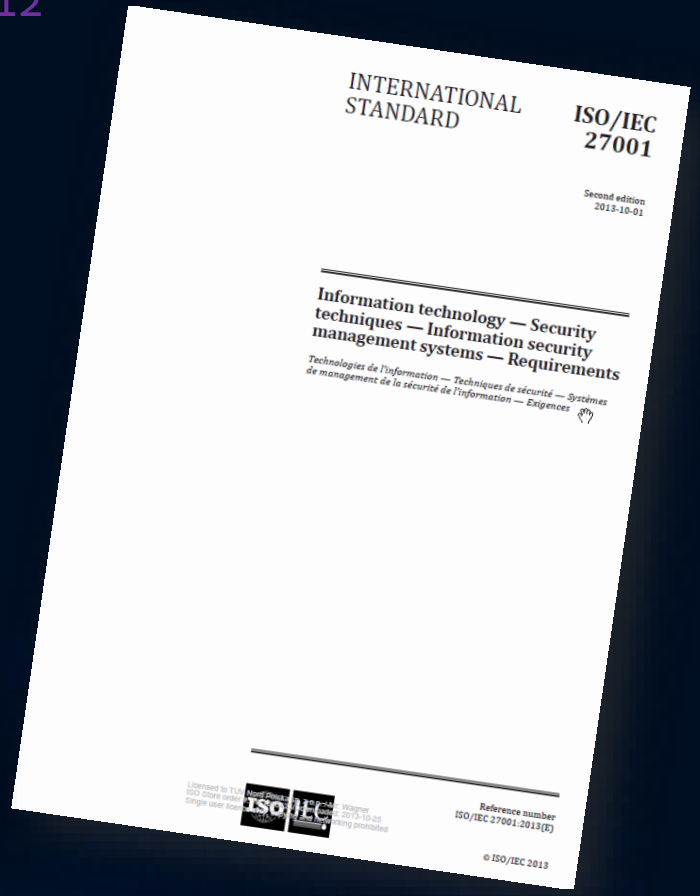
Information technology — Security techniques — Information security management systems — Requirements

Agenda

1. Wymagania normy ISO/IEC 27001:2014-12
2. Załącznik A – normatywny



Contents



INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

Spis treści

Contents Page

Spis treści

Contents

Page

Forewo iv

0 v

1 1

2 1

3 1

4 1

..... 1

..... 1

..... 1

..... 2

5 2

..... 2

..... 2

..... 3

6 3

..... 3

..... 5

7 5

..... 5

..... 5

..... 5

..... 6

..... 6

8 7

..... 7

..... 7

..... 7

9 7

..... 7

..... 8

..... 8

10 9

..... 9

..... 9

Annex 10

Bibliography 23

0 Wprowadzenie

1 Zakres normy

2 Powołania normatywne

3 Terminy i definicje

4 Kontekst organizacji

5 Przywództwo

6 Planowanie

7 Wsparcie

8 Eksploatacja

9 Ocena działań

10 Doskonalenie

Załącznik A

Nowe zagadnienia wprowadzone (uzupełnione)

Nowe zagadnienie/korekta	Wyjaśnienie
Kontekst organizacji	Środowisko, w którym działa organizacja (kontekst zewnętrzny i wewnętrzny).
Problemy, ryzyko i szansa	Zastępuje „działania zapobiegawcze”
Zainteresowane strony	Zastępuje „wymagania nadzoru”
Przywództwo	Wymagania wobec kierownictwa w aspekcie BI
Komunikacja	Wyraźne wymagania dotyczące zakomunikowania zarówno wewnątrz organizacji jak i do organizacji współpracujących.
Cele Bezpieczeństwa Informacji	Cele Bezpieczeństwa informacji są określone pod kątem stopnia zabezpieczenia jak i funkcji jakie mają spełnić (co chcemy osiągnąć).
Ocena ryzyka	Identyfikacja aktywów, zagrożeń i luk w zabezpieczeniach nie jest już warunkiem wstępnym identyfikacji zagrożeń bezpieczeństwa informacji
Właściciel ryzyka	Zastępuje „właściciela aktywów”
Postępowanie z ryzykiem	Skuteczność planu postępowania z ryzykiem (minimalizacja ryzyka) jest teraz uważany jest ważniejsze niż skuteczności kontroli.
Kontrola	Sposób kontroli określany jest na poziomie minimalizacji ryzyka a nie na podstawie aneksu A.
Udokumentowana informacja	Zastępuje „dokumenty i zapisy”
Ocena zmian	Obejmuje pomiar skuteczności SZBI oraz minimalizacji ryzyka
Ciągłe doskonalenie	Mogą być stosowane inne metodologie niż PDCA (Plan-Do-Check-Act)

Udokumentowana informacja

4.3	**Zakres SZBI.** Określanie zakresu działania system u zarządzania bezpieczeństwem informacji.	**8.1**	**Planowanie operacyjne i kontrola** Planowanie i nadzór nad działaniami eksploatacyjnymi.
5.2	**Polityka.** Ustanowienie polityki w zakresie Zarządzania Bezpieczeństwem Informacji	**8.2**	**Wyniki oceny ryzyka Bezpieczeństwa Informacji** Ocena ryzyka związanego z bezpieczeństwem informacji.
6.1.2	**Ustanowienie procesów oceny ryzyka.** Ocena ryzyka związanego z Bezpieczeństwem Informacji.	**8.3**	**Wyniki postępowania z ryzykiem Bezpieczeństwa Informacji** Postępowanie z ryzykiem związanym z Bezpieczeństwem Informacji, plany postępowania, rezultaty działań.
6.1.3	**Zdefiniowanie i zastosowanie procedur postępowania z ryzykiem.** Postępowanie z ryzykiem związanym z Bezpieczeństwem Informacji	**9.1**	**Dowody z wyników monitorowania i pomiarów** Monitorowanie , pomiar y , analiza i ocena wydajności BI, skuteczności działania SZBI
6.1.3 d)	**Deklaracja stosowania** Opracowania deklaracji stosowania zawierającej niezbędne zabezpieczenia oraz uzasadnienie wyboru, ustanowienia i wyłączenia zabezpieczeń.	**9.2 g)**	**Ewidencjonowanie przeprowadzonych audytów oraz wyników z nich wynikających.** Zachować dokumentację jako dowód przedstawiający program audytów i ich wyniki.
6.2	**Cele Bezpieczeństwa Informacji** Cele w zakresie bezpieczeństwa informacji i planowanie działań umożliwiających ich osiągnięcie, funkcje i poziomy działania.	**9.3**	**Ewidencja oraz wyniki przeglądu zarządzania** Przegląd zarządzania - w zaplanowanych odstępach czasu w celu zapewnienia jego ciągłej odpowiedniości, adekwatności i skuteczności.
7.2 d)	**Dowód kompetencji** Zachować odpowiednią udokumentowaną informację jako dowód posiadanych kompetencji.	**10.1 f)**	**Ewidencja charakteru niezgodności oraz wszystkich działań podjętych w celu jej usunięcia**
7.5.1 b)	**Dokumentacja konieczna aby SZBI było skuteczne** Zachować udokumentowaną informację określoną przez organizację konieczną do uzyskania skuteczności systemu zarządzania Bezpieczeństwem Informacji	**10.1 g)**	**Ewidencja wszystkich działań podjętych w celu usunięcia niezgodności.**

Tabela odwzorowania głównych punktów normy PN ISO/IEC 27001:2014 w odniesieniu do PN ISO/IEC 27001:2007

	27001 wersja 2014		27001 wersja2005/2007
0	Wprowadzenie	0	Wprowadzenie
1	Zakres normy	1	Zakres normy
2	Odniesienia normatywne	2	Odniesienia normatywne
3	Terminy i definicje	3	Terminy i definicje
4.1	Kontekst organizacji	8.3	Działania zapobiegawcze
4.2	Rozumienie potrzeb i oczekiwań zainteresowanych stron	5.2.1(c)	zidentyfikowania i odniesienia się do wymagań przepisów prawa i wymagań nadzoru oraz zobowiązań związanych z bezpieczeństwem, a wynikających z zawartych umów
4.3	Określanie zakresu działania systemu zarządzania bezpieczeństwem informacji	4.2.1 a)	Zdefiniować zakres i granice SZBI, uwzględniając charakterystykę prowadzonej działalności, organizacji: jej lokalizację, aktywa i technologie, i dołączając dokładny opis oraz uzasadnienie każdego wyłączenia z zakresu
		4.2.3 f)	W regularnych odstępach czasu wykonywać przeglądy SZBI realizowane przez kierownictwo, aby zapewnić, że zakres jest odpowiedni oraz udoskonalenia procesu SZBI są identyfikowane
4.4	System zarządzania bezpieczeństwem informacji	4.1	Wymagania ogólne
5.1	Kierownictwo i jego zaangażowanie	5.1	Zaangażowanie kierownictwa
5.2	Polityka	4.2.1 b)	Zdefiniować politykę SZBI, uwzględniającą charakterystykę prowadzonej działalności, organizacji, jej lokalizacji, aktywów i technologii
5.3	Role organizacyjne, zakresy odpowiedzialności i organy władzy	5.1 c)	Określenie ról i zakresów odpowiedzialności w odniesieniu do bezpieczeństwa informacji
6.1.1	Działania w zakresie zarządzania ryzykiem i możliwości	8.3	Działania zapobiegawcze
6.1.2	Cele w zakresie bezpieczeństwa informacji i planowanie działań umożliwiających ich osiągnięcie	4.2.1 c)	Zdefiniować podejście do szacowania ryzyka w organizacji
6.1.2		4.2.1 d)	Określenie (identyfikacja) ryzyka
6.1.2		4.2.1 e)	Analiza ocena, przemiana ryzyka

6 Planowanie

Należy przygotować deklarację stosowania SoA:

Deklaracja Stosowania Wydanie z: 22.04.2014

Objaśnienia (dla wybranych zabezpieczen i powodów stosowania)

WR: wymagania regulacyjne, **WK**: wymagania kontraktowe, zapisy umów, W**B/BP**: wymagania biznesowe/stosowanie dobrych praktyk, **RRA**: wdrożone jako element postępowania z ryzykiem

ISO 27001:2013 Zabezpieczenia			Bieżące zabezpieczenia	Opis (uzasadnienie wyłączenia)	Wybrane zabezpieczenia i powód stosowania				Uwagi (przegląd realizacji)
					WR	WK	WB/BP	RRA	
Klauzula	Sekcja	Cel zabezpieczenia/zabezpieczenie							
5 Polityki bezpieczeństwa	5.1	Wskazówki dla kierownictwa o bezpieczeństwie informacji							
	5.1.1	Polityki bezpieczeństwa infrormacji	Polityka Bezpieczeństwa - dane osobowe		x	x	x	x	
	5.1.2	Przegląd polityk bezpieczeństwa infromacji	brak					x	
6 Organizacja bezpieczeństwa informacji	6.1	Organizacja wewnętrzna							
	6.1.1	Role i odpowiedzialności w bezpieczeństwie informacji	Wyznaczony Pełnomocnik SZBI					x	wyznaczyć auditorów i forum BI
	6.1.2	Podział obowiązków	brak					x	
	6.1.3	Kontakt z organami władzy	brak	brak zidentyfikowanych komunikacji, oprócz niezapowiedzianych wizyt: Urząd Skarbowy, Inspekcja Pracy					
	6.1.4	Kontakty z grupami zaangażowanymi w zapewnienie bezpieczeństwa	przegląd portali tematycznych					x	
	6.1.5	Bezpieczeństwo infromacji w zarządzaniu projektami	każdy projekt jest poprzedzony analiża ryzyka wykonalności					x	
	6.2	Urządzenia mobilne i telepraca							
	6.2.1	Polityka dla urządzeń mobilnych	brak					x	wdrożenie do 2015
	6.2.2	Telepraca	brak					x	wdrożenie do 2015

Wartość dodana SoA (*informacje nie wymagane przez normę*):

Wyraźne określenie wymagań powiązanych z prawem

Opis metody implementacji zabezpieczenia, „spis treści" dla stosowanych zabezpieczeń

Załącznik A funkcjonuje jako lista kontrolna a nie jako zestaw zabezpieczeń do zastosowania !

Załącznik A – normatywny załącznik

A.5 – A.18 **14 domen zabezpieczeń**

A.5.1
A.6.1
A.6.2
A.7.1
A.7.2
A.7.3
A.8.1
A.8.2
A.8.3
A.9.1
A.9.2
A.9.3
A.9.4
A.10.1
A.11.1
A.11.2
A.12.1
A.12.2
A.12.3
A.12.4
A.12.5
A.12.6
A.12.7
A.13.1
A.13.2
A.14.1
A.14.2
A.14.3
A.15.1
A.15.2
A.16.1
A.17.1
A.17.2
A.18.1
A.18.2

35 celów zabezpieczeń

ZAŁĄCZNIK A jest listą otwartą, ma służyć jako model do sprawdzenia wdrożonych zabezpieczeń, ma zapobiegać aby żaden z obszarów nie został pominięty. NIE JEST listą do zastosowania na starcie systemu, ale wskazówką ! Można i należy stosować własne zabezpieczenia, jeżeli te w załączniku nie są wystarczające dla organizacji

114 zabezpieczeń

Załącznik A: A.5 Polityka Bezpieczeństwa Informacji

Przykłady polityk:

Polityka kontroli dostępu – patrz klauzula A.9
Polityka klasyfikacji informacji i postępowania z aktywami – patrz A.8.2
Polityka bezpieczeństwa fizycznego i środowiskowego – patrz A.11
Przykłady polityk zorientowanych na końcowego użytkownika:

- Akceptowalne użycie aktywów A.8.1.3
- Polityka czystego biurka i ekranu A.11.29
- Polityki i procedury przekazywania informacji A.13.2.1
- Polityka dla urządzeń mobilnych i telepracy patrz A.6.2
- Polityka ograniczeń dotyczących instalacji oprogramowania A.12.6.2

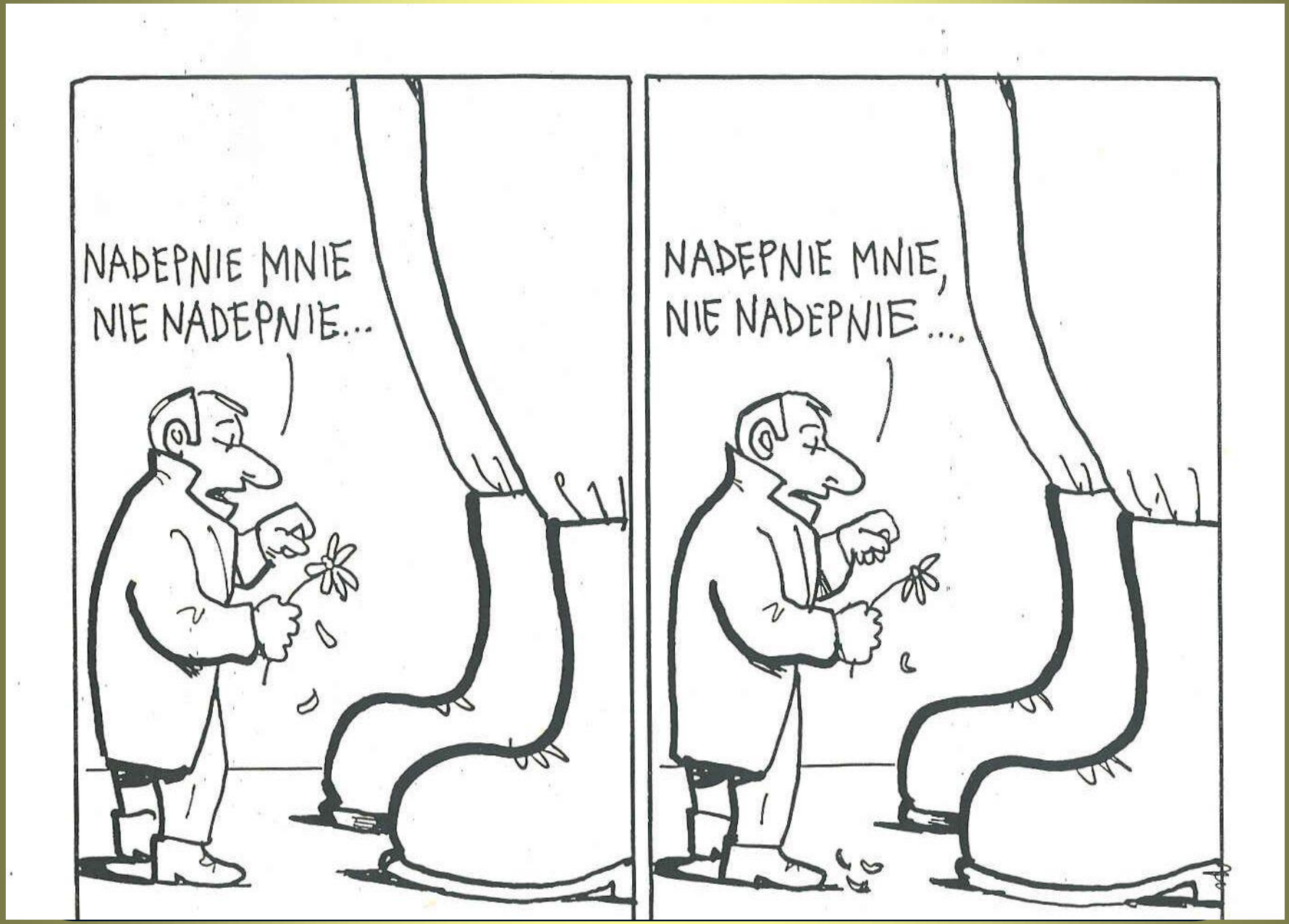
Polityka kopii zapasowych A.12.3
Polityka przekazywania informacji A.13.2
Polityka ochrony przed malware A.12.2
Polityka zarządzania podatnościami technicznymi A.12.6.1
Polityka stosowania kryptografii A.10
Polityka bezpieczeństwa komunikacja A.13
Polityka prywatności oraz ochrony danych osobowych A.18.1.4
Polityka relacji z poddostawcami A.15

Załącznik A – normatywny załącznik

Atrybut	Opis
A.5	Polityki bezpieczeństwa informacji
A.6	Organizacja bezpieczeństwa informacji
A.7	Bezpieczeństwo zasobów ludzkich
A.8	Zarządzanie aktywami
A.9	Kontrola dostępu
A.10	Kryptografia
A.11	Bezpieczeństwo fizyczne i środowiskowe
A.12	Bezpieczna eksploatacja
A.13	Zarządzanie bezpieczeństwem sieci
A.14	Pozyskiwanie, rozwój i utrzymanie systemów
A.15	Relacje z dostawcami
A.16	Zarządzanie incydentami związanymi z bezpieczeństwem informacji
A.17	Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
A.18	Zgodność

Tabela odwzorowania punktów kontrolnych załącznika A

Mapa kontrolna załącznika A		ISO 27001 - 2005/2007										
		Polityka bezpieczeństwa	Organizacja bezpieczeństwa informacji	Zarządzanie aktywami	Bezpieczeństwo zasobów ludzkich	Bezpieczeństwo fizyczne i środowiskowe	Zarządzanie systemami i sieciami	Kontrola dostępu	Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych	Zarządzanie incydentami związanymi z bezpieczeństwem informacji	Zarządzanie ciągłością działania	Zgodność
ISO 27001 - 2013		A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15
A.5.1	Wsparcie kierownictwa dla bezpieczeństwa informacji (2)	X										
A.6.1	Organizacja wewnętrzna (5)		X		X		X					
A.6.2	Urządzenia mobilne i telepraca (2)							X				
A.7.1	Przed zatrudnieniem (2)				X							
A.7.2	Podczas zatrudnienia (3)				X							
A.7.3	Zakończenie lub zmiana zatrudnienia (1)				X							
A.8.1	Odpowiedzialność za aktywa (4)			X	X							
A.8.2	Klasyfikacja informacji (3)			X			X					
A.8.3	Obsługa nośników (3)						X					
A.9.1	Wymagania biznesowe wobec kontroli dostępu (2)							X				
A.9.2	Zarządzanie dostępem użytkowników (6)				X			X				
A.9.3	Odpowiedzialność użytkowników (1)							X				
A.9.4	Kontrola dostępu do systemu i aplikacji (5)							X	X			


NADEPNIE MNIE
NIE NADEPNIE...
NADEPNIE MNIE,
NIE NADEPNIE....


CHOLERA, TEGO
NIE PRZEWIDZIAŁEM!

Pytania


Zapewnić równowagę
Dziękuję

Załącznik A – normatywny załącznik

A.5	Polityki bezpieczeństwa informacji
A.5.1	Kierunki bezpieczeństwa informacji określane przez kierownictwo
A.5.1.1	Polityki bezpieczeństwa informacji
A.5.1.2	Przegląd polityk bezpieczeństwa informacji

Załącznik A – normatywny załącznik

A.6	Organizacja bezpieczeństwa informacji
A.6.1	Organizacja wewnętrzna
A.6.1.1	Role i odpowiedzialność za bezpieczeństwo informacji
A.6.1.2	Rozdzielanie obowiązków
A.6.1.3	Kontakty z organami władzy
A.6.1.4	Kontakty z grupami zainteresowanych specjalistów
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami
A.6.2	Urządzenia mobilne i telepraca
A.6.2.1	Polityka stosowania urządzeń mobilnych
A.6.2.2	Telepraca

Załącznik A – normatywny załącznik

A.7	Bezpieczeństwo zasobów ludzkich
A.7.1	Przed zatrudnieniem
A.7.1.1	Postępowanie sprawdzające
A.7.1.2	Warunki zatrudnienia
A.7.2	Podczas zatrudnienia
A.7.2.1	Odpowiedzialność kierownictwa
A.7.2.2	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
A.7.2.3	Postępowanie dyscyplinarne
A.7.3	Zakończenie i zmiana zatrudnienia
A.7.3.1	Zakończenie zatrudnienia lub zmiana zakresu obowiązków

Załącznik A – normatywny załącznik

A.8	Zarządzanie aktywami
A.8.1	**Odpowiedzialność za aktywa**
A.8.1.1	Inwentaryzacja aktywów
A.8.1.2	Własność aktywów
A.8.1.3	Akceptowalne użycie aktywów
A.8.1.4	Zwrot aktywów
A.8.2	Klasyfikacja informacji
A.8.2.1	Klasyfikowanie informacji
A.8.2.2	Oznaczanie informacji
A.8.2.3	Postępowanie z aktywami
A.8.3	Postępowanie z nośnikami
A.8.3.1	Zarządzanie nośnikami wymiennymi
A.8.3.2	Wycofywanie nośników
A.8.3.3	Przekazywanie nośników

Załącznik A – normatywny załącznik

A.9	Kontrola dostępu
A.9.1	Wymagania biznesowe wobec kontroli dostępu
A.9.1.1	Polityka kontroli dostępu
A.9.1.2	Dostęp do sieci i usług sieciowych
A.9.2	Zarządzenie dostępem użytkowników
A.9.2.1	Rejestrowanie i wyrejestrowywanie użytkowników
A.9.2.2	Przydzielanie dostępu użytkownikom
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników
A.9.2.5	Przegląd praw dostępu użytkowników
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu
A.9.3	Odpowiedzialność użytkowników
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających
A.9.4	Kontrola dostępu do systemów i aplikacji
A.9.4.1	Ograniczanie dostępu do informacji
A.9.4.2	Procedury bezpiecznego logowania
A.9.4.3	System zarządzania hasłami
A.9.4.4	Użycie uprzywilejowanych programów narzędziowych
A.9.4.5	Kontrola dostępu do kodów źródłowych programów

Załącznik A – normatywny załącznik

A.10	Kryptografia
A.10.1	Zabezpieczenia kryptograficzne
A.10.1.1	Polityka stosowania zabezpieczeń kryptograficznych
A.10.1.2	Zarządzanie kluczami

Załącznik A – normatywny załącznik

A.11	Bezpieczeństwo fizyczne i środowiskowe
A.11.1	Obszary bezpieczne
A.11.1.1	Fizyczna granica obszaru bezpiecznego
A.11.1.2	Fizyczne zabezpieczenie wejść
A.11.1.3	Zabezpieczenie biur, pomieszczeń i obiektów
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi
A.11.1.5	Praca w obszarach bezpiecznych
A.11.1.6	Obszary dostaw i załadunku
A.11.2	Sprzęt
A.11.2.1	Lokalizacja i ochrona sprzętu
A.11.2.2	Systemy wspomagające
A.11.2.3	Bezpieczeństwo okablowania
A.11.2.4	Konserwacja sprzętu
A.11.2.5	Wynoszenie aktywów
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia
A.11.2.8	Pozostawianie sprzętu użytkownika bez opieki
A.11.2.9	Polityka czystego biurka i czystego ekranu

Załącznik A – normatywny załącznik

A.12	Bezpieczna eksploatacja
A.12.1	Procedury eksploatacyjne i odpowiedzialność
A.12.1.1	Dokumentowanie procedur eksploatacyjnych
A.12.1.2	Zarządzanie zmianami
A.12.1.3	Zarządzanie pojemnością
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych
A.12.2	Ochrona przed szkodliwym oprogramowaniem
A.12.2.1	Zabezpieczenia przed szkodliwym oprogramowaniem
A.12.3	Kopie zapasowe
A.12.3.1	Zapasowe kopie informacji
A.12.4	Rejestrowanie zdarzeń i monitorowanie
A.12.4.1	Rejestrowanie zdarzeń
A.12.4.2	Ochrona informacji w dziennikach zdarzeń
A.12.4.3	Rejestrowanie działań administratorów i operatorów
A.12.4.4	Synchronizacja zegarów
A.12.5	Nadzór nad oprogramowaniem produkcyjnym
A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych
A.12.6	Zarządzanie podatnościami technicznymi
A.12.6.1	Zarządzanie podatnościami technicznymi
A.12.6.2	Ograniczenia w instalowaniu oprogramowania
A.12.7	Rozważania dotyczące audytu systemów informacyjnych
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych

Załącznik A – normatywny załącznik

A.13	Bezpieczeństwo komunikacji
A.13.1	Zarządzanie bezpieczeństwem sieci
A.13.1.1	Zabezpieczenia sieci
A.13.1.2	Bezpieczeństwo usług sieciowych
A.13.1.3	Rozdzielanie sieci
A.13.2	Przesyłanie informacji
A.13.2.1	Polityki i procedury przesyłania informacji
A.13.2.2	Porozumienia dotyczące przesyłania informacji
A.13.2.3	Wiadomości elektroniczne
A.13.2.4	Umowy o zachowaniu poufności

Załącznik A – normatywny załącznik

A.14	Pozyskiwanie, rozwój i utrzymanie systemów
A.14.1	Wymagania związane z bezpieczeństwem systemów informacyjnych
A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji
A.14.1.2	Zabezpieczanie usług aplikacyjnych w sieciach publicznych
A.14.1.3	Ochrona transakcji usług aplikacyjnych
A.14.2	Bezpieczeństwo w procesach rozwoju i wsparcia
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych
A.14.2.2	Procedury kontroli zmian w systemach
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej
A.14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania
A.14.2.5	Zasady projektowania bezpiecznych systemów
A.14.2.6	Bezpieczne środowisko rozwojowe
A.14.2.7	Prace rozwojowe zlecane podmiotom zewnętrznym
A.14.2.8	Testowanie bezpieczeństwa systemów
A.14.2.9	Testy akceptacyjne systemów
A.14.3	Dane testowe
A.14.3.1	Ochrona danych testowych

Załącznik A – normatywny załącznik

A.15	Relacje z dostawcami
A.15.1	Bezpieczeństwo informacji w relacjach z dostawcami
A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z dostawcami
A.15.1.2	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami
A.15.1.3	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych
A.15.2	Zarządzanie usługami świadczonymi przez dostawców
A.15.2.1	Monitorowanie i przegląd usług świadczonych przez dostawców
A.15.2.2	Zarządzenie zmianami w usługach świadczonych przez dostawców

Załącznik A – normatywny załącznik

A.16	Zarządzanie incydentami związanymi z bezpieczeństwem informacji
A.16.1	Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami
A.16.1.1	Odpowiedzialność i procedury
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
A.16.1.5	Reagowanie na incydenty związane z bezpieczeństwem informacji
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
A.16.1.7	Gromadzenie materiału dowodowego

Załącznik A – normatywny załącznik

A.17	Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
A.17.1	Ciągłość bezpieczeństwa informacji
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji
A.17.1.2	Wdrożenie ciągłości bezpieczeństwa informacji
A.17.1.3	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji
A.17.2	Nadmiarowość
A.17.2.1	Dostępność środków przetwarzania informacji

Załącznik A – normatywny załącznik

A.18	Zgodność
A.18.1	**Zgodność z wymaganiami prawnymi i umownymi**
A.18.1.1	Określenie stosownych wymagań prawnych i umownych
A.18.1.2	Prawa własności intelektualnej
A.18.1.3	Ochrona zapisów
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych
A.18.2	**Przeglądy bezpieczeństwa informacji**
A.18.2.1	Niezależny przegląd bezpieczeństwa informacji
A.18.2.2	Zgodność z politykami bezpieczeństwa i standardami
A.18.2.3	Sprawdzanie zgodności technicznej

Norma PN ISO/IEC 20000-1:2014

Obszary/dziedziny procesów informatycznych norma ISO 20000

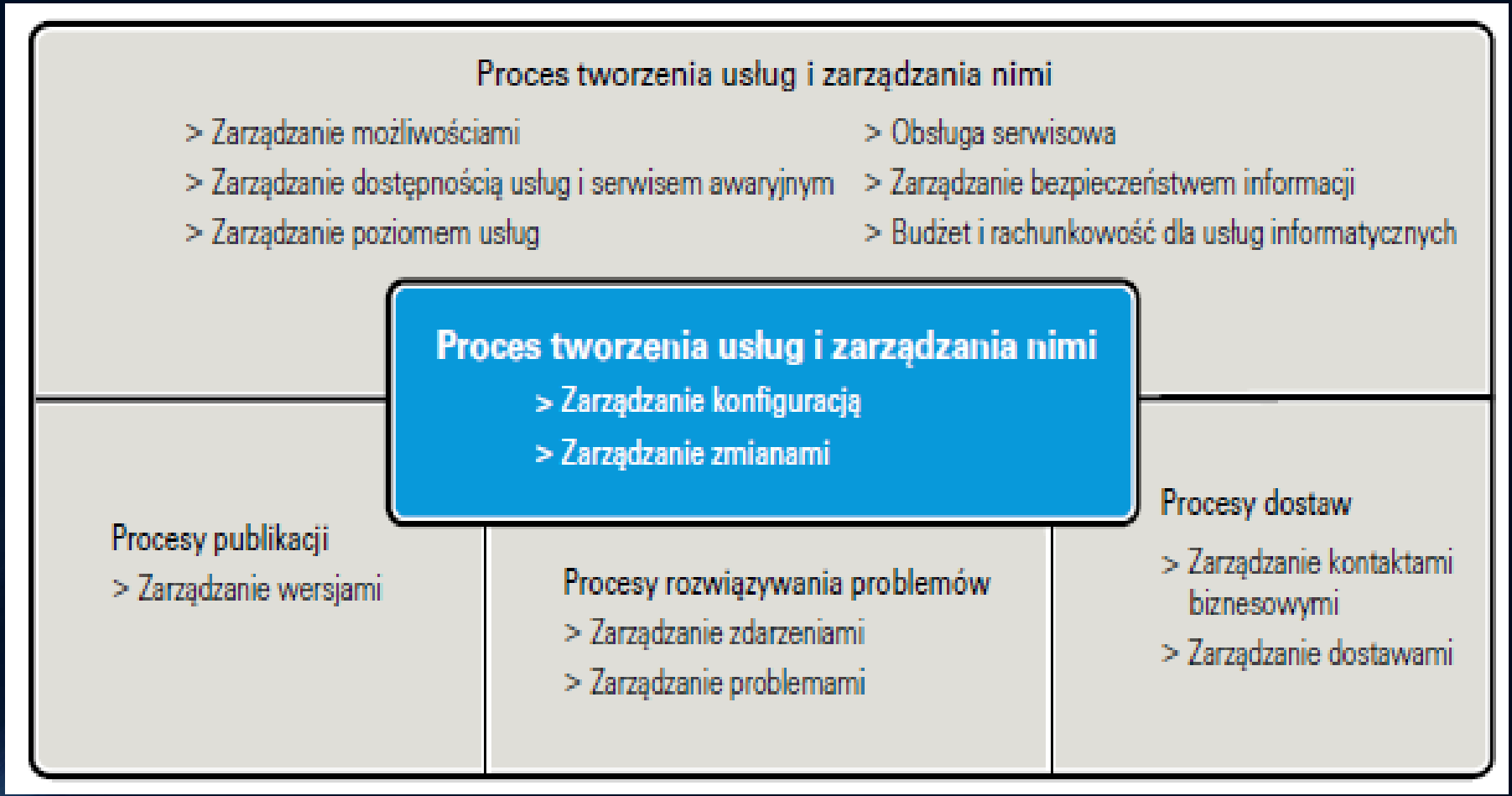
Zawartość normy

Treść normy ISO 20000 opiera się na następujących dokumentach, będących częścią normy BS 15000:

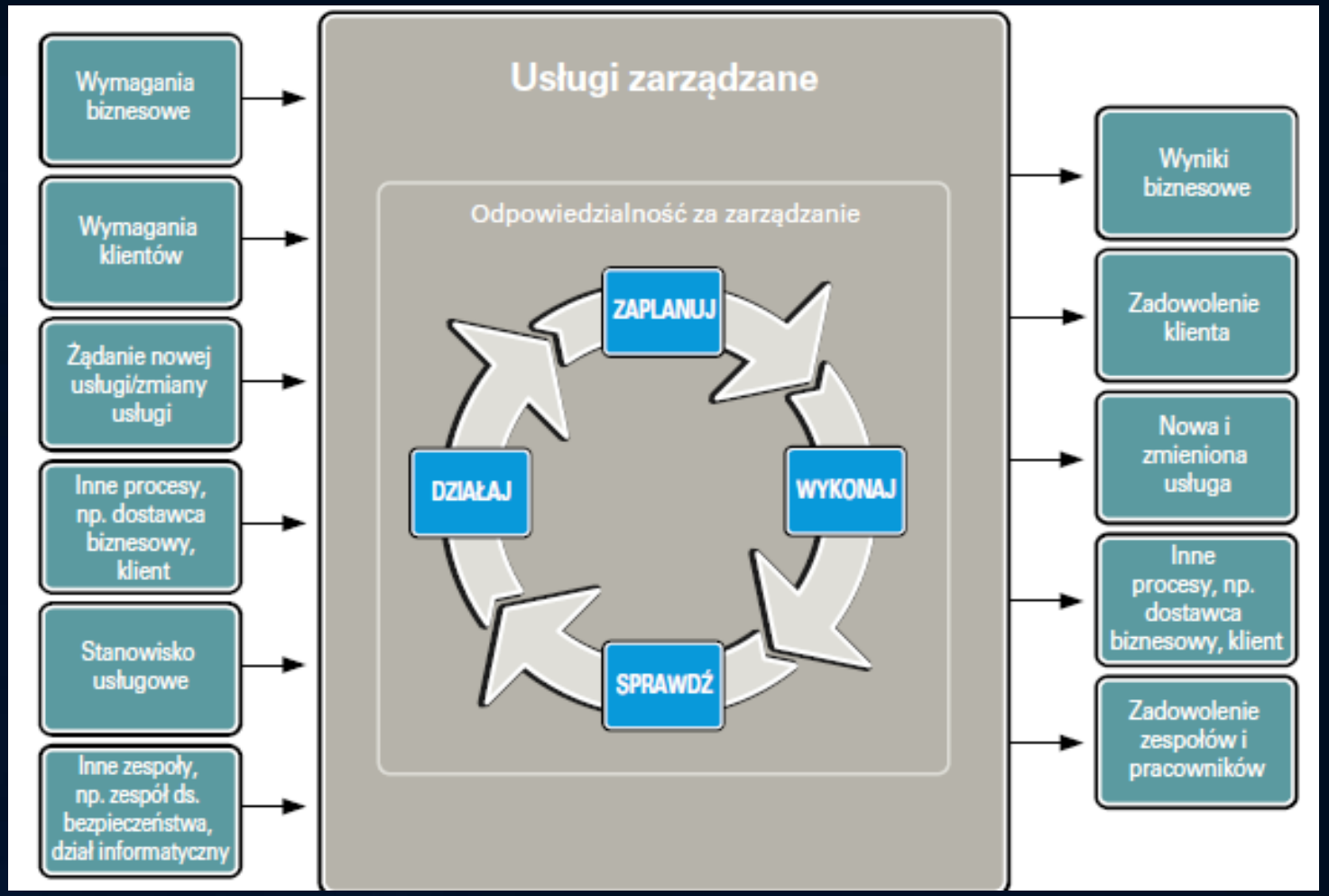
- **ISO/IEC 20000-1:2005 SPECYFIKACJA WYMAGAŃ** zawiera zestaw minimalnych wymagań i promuje podejście oparte na zintegrowanych procesach w celu efektywnego świadczenia usług zarządzanych, które pozwolą sprostać wymaganiom biznesowym i wymaganiom klientów. (ewentualnie certyfikat)

- **ISO/IEC 20000-2:2005 REGUŁY POSTĘPOWANIA** – obejmuje kodeks postępowania dotyczący zarządzania usługami (Code of Practice for Service Management), który w skondensowanej formie zawiera kluczowe elementy najlepszych procedur ITIL. Celem tego dokumentu jest ułatwienie firmom stworzenia procesów niezbędnych do osiągnięcia celów części 1.

Procesy zarządzania usługami IT



Doskonalenie jakości usług IT



Procesy zarzadzania usługami IT wg normy