Zarządzanie bezpieczeństwem informacji – przepisy prawa a normy

UKSW, Warszawa, Listopad 2015

Dr inż. Grażyna Ożarek

Projekt Badawczo- Rozwojowy realizowany na rzecz bezpieczeństwa i obronności Państwa współfinansowany ze środków Narodowego Centrum Badań i Rozwoju
„MODEL REGULACJI JAWNOŚCI I JEJ OGRANICZEŃ W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM”

POLSKI KOMITET NORMALIZACYJNY

www.pkn.pl

Zarządzanie bezpieczeństwem informacji – przepisy prawa a normy

UKSW, Warszawa, Listopad 2015

Dr inż. Grażyna Ożarek

Prawo

nakazuje
nam zrobienie
czegoś

Normy

pokazują
jak należy to
zrobić

Obszary działalności w których prawnie wymagana jest ochrona danych i informacji

- Prawo dotyczące ochrony danych osobowych
- Prawo oświatowe
- Prawo bankowe
- Prawo finansowe
- Prawo przemysłowe
- Prawo archiwalne
- Prawo dotyczące informatyzacji państwa
- Prawo telekomunikacyjne
- Prawo dotyczące statystyki publicznej
- Prawo autorskie
- Prawo z zakresu ochrony zdrowia

Wybrane akty prawne wymagające bezpieczeństwa informacyjnego

USTAWA o ochronie danych osobowych

USTAWA o finansach publicznych KOMUNIKAT Ministra Finansów w sprawie standardów **kontroli zarządczej**

USTAWA o rachunkowości

USTAWA o dostępie do informacji publicznej

USTAWA o systemie informacji oświatowej

USTAWA o narodowym zasobie archiwalnym i archiwach

USTAWA o prawie autorskim i prawach pokrewnych

USTAWA - Kodeks karny - Rozdział XXXIII kodeksu dotyczy przestępstw przeciwko ochronie informacji

Wybrane akty wykonawcze	Normy
Rozporządzenie MSWiA z 10.09.2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych	PN-ISO/IEC 27001 PN-ISO/IEC 20000
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 Rady Ministrów 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
Rozporządzenia Ministra Zdrowia z zakresu informatyzacji służby zdrowia	PN-EN ISO 27799:2010 PN-ISO/IEC 27001

Rozporządzenie
Rady Ministrów
z dnia 12-04-2012 r.

§ 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

Rozporządzenie
Rady Ministrów
z dnia 12-04-2012 r.

§ 20.3. System zarządzania bezpieczeństwem informacji spełnia wymogi, o których mowa w ust. 1 i 2, jeżeli 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:

PN-ISO/IEC 17799, PN-ISO/IEC 27005,

PN-ISO/IEC 24762

Rozporządzenie
Rady Ministrów
z dnia 12-04-2012 r.

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, PN-ISO/IEC 20000-2

Obszar dobrych praktyk a normy

Dobre praktyki, to odwołanie się do uogólnionych pozytywnych doświadczeń lub ogólne zasady, które w wielu przypadkach zostały zastosowane z dobrym skutkiem

Obecnie, jedynie poprawną formą upowszechniania dobrych praktyk są **normy** (krajowe, regionalne, międzynarodowe)

Wyspecjalizowana treść norm jest na tyle ogólna, aby mogła być dopasowana do każdej organizacji, i jest wyposażona w mierniki, wskaźniki, które pozwalają upewnić się samodzielnie lub z wykorzystaniem III strony (audytorów zewnętrznych) o poziomie bezpieczeństwa

Dobre praktyki w normie PN-ISO/IEC 27001

1. Procesowe podejście

„Bezpieczeństwo nie jest produktem, lecz procesem” (K. Mitnick. Sztuka postępu)

„Bezpieczeństwo nie jest stanem tylko procesem. W sprawach bezpieczeństwa nie ma „spocznij”” **(St. Koziej)**

***„Nie jest problemem technicznym, lecz problemem związanym z ludźmi i zarządzaniem*.**

Ludzie wymyślają coraz skuteczniejsze zabezpieczenia techniczne, co znacznie utrudnia znalezienie luk w systemie (…) od strony technicznej.

(…) jeśli ktoś myśli, że aby chronić swoje zasoby informacyjne wystarczy tylko nadążać za postępem technicznym, ten jest w błędzie!” (K. Mitnick, Sztuka podstępu)

Dobre praktyki w normie PN-ISO/IEC 27001

2. Łączy i koordynuje różne działania w zakresie bezpieczeństwa informacyjnego

3. Wymaga:

- opracowania własnej polityki,
- określenia własnych celów w zakresie bezpieczeństwa informacyjnego
- zastosowania narzędzi do sprawdzenia w jakim stopniu cele te są osiągane

Czym jest SZBI wg rodziny PN-ISO/IEC 27000?

Jest systemowym, kompleksowym podejściem do ustanowienia, wdrożenia i utrzymania bezpieczeństwa informacyjnego; jego elementami są:

- **Polityka** (zawiera **własną** definicję bezpieczeństwa informacyjnego, jego ogólne cele, zakres, znaczenie dla organizacji, oświadczenie o intencjach organizacji w zakresie SZBI, krótkie wyjaśnienie zasad i wymagań, które mają szczególne znaczenie dla organizacji oraz odwołanie do szczegółowych dokumentów)
- **procedury**,
- **wytyczne**,
- **aktywa podstawowe i wspierające**

Kompleksowe zapewnienie bezpieczeństwa informacyjnego wg PN-ISO/IEC 27001

1. Polityka bezpieczeństwa informacyjnego
2. Organizacja bezpieczeństwa informacji
3. Bezpieczeństwo zasobów ludzkich
4. Zarządzanie aktywami
5. Kontrola dostępu
6. Kryptografia
7. Bezpieczeństwo fizyczne i środowiskowe
8. Bezpieczna eksploatacja
9. Bezpieczeństwo łączności
10. Pozyskiwanie, rozwój i utrzymywanie systemów
11. Relacje z dostawcami
12. Zarządzanie incydentami
13. Ciągłość działania
14. Zgodność z wymaganiami prawnymi i umownymi

Aktywa podstawowe

- Procesy i działania podstawowe
  (określenie procesów krytycznych)
- Dane i informacje
  (należą do nich nie tylko te wykorzystywane w działaniach operacyjnych ale także dane i informacje archiwizowane i przeznaczone do utylizacji)

Aktywa wspierające

- Siedziba
- Sprzęt
- Oprogramowanie
- Sieć
- Personel
- Struktura organizacyjna

Bezpieczeństwo informacji wg serii PN-ISO/IEC 27000, czego dotyczy?

Dotyczy informacji, która pojmowana jest jako zasób majątkowy o ustalonej wartości (aktywa), a w związku z tym wymaga ochrony m.in. przed utratą jej istotnych atrybutów

Warto pamiętać!

- Dostępność dokładnych, kompletnych danych w wymaganym czasie jest katalizatorem efektywności działań
- Ochrona aktywów informacyjnych umożliwia każdej organizacji zachowanie i doskonalenie własnego wizerunku, działanie zgodnie z prawem i osiąganie celów

Własne wymagania bezpieczeństwa wg serii PN-ISO/IEC 27000

Trzy główne źródła

1. **Przepisy prawne, statutowe, regulacje wewnętrzne, zobowiązania kontraktowe, środowisko kulturowe**

2. **Zbiór zasad, celów i wymagań przetwarzania danych i informacji wypracowanych przez organizację**

3. **Szacowanie ryzyka dotyczące działań w placówce z uwzględnieniem celów organizacji**

(szacownie ryzyka pozwala zidentyfikować zagrożenie dla aktywów, ocenić podatność na zagrożenia i prawdopodobieństwo ich wystąpienia oraz estymować potencjalne skutki)

Założenia systemu zarządzania bezpieczeństwem informacyjnym wg rodziny norm PN-ISO/IEC 27000

Założenia - prezentowane w ujęciu kodeksu wymagań - nakładają powinność:

1. Świadomej i celowej analizy potencjalnych zagrożeń planowanych działań
2. Oceny ryzyka ich wystąpienia i materializacji
3. Predykcji kosztów utrzymania bezpieczeństwa własnego zasobu informacyjnego

Polskie Normy serii PN-ISO/IEC 27000 z zakresu zarządzania bezpieczeństwem informacji

PN-ISO/IEC 27001 – wymagania stawiane systemom zarządzania bezpieczeństwem informacji

PN-ISO/IEC (19977) 27002 praktyczne zasady zarządzania bezpieczeństwem informacji

Zawiera wzorcowy wykaz celów stosowania zabezpieczeń oraz wykaz 166 zabezpieczeń w 14 obszarach kontrolnych (bezpieczeństwa)

PN-ISO/IEC 27005 – Zarządzanie ryzykiem w bezpieczeństwie informacji

Zawiera przykłady 43 typowych zagrożeń i 85 podatności w różnych obszarach bezpieczeństwa (sprzęt, oprogramowanie, sieć, personel, siedziba, organizacja)

Przykładowe etapy wdrażania SZBI

Określanie zasobów systemu informacyjnego

inwentaryzacja, lokalizacja zasobów, klasyfikacja i wycena
określenie grup i kategorii użytkowników poszczególnych informacji

Analiza zagrożeń i ocena ryzyka

zagrożenia, słabe punkty, zależności
ocena skuteczności już istniejących zabezpieczeń
szacowanie kosztów/strat
określenie ryzyka akceptowalnego

Projektowanie dokumentacji

polityka bezpieczeństwa (SZBI), zdefiniowanie zakresu SZBI
procedury, instrukcje, zasady, ustawy, rozporządzenia,
wewnętrzne akty prawne, umowy

Projektowanie systemu zabezpieczeń

PN-ISO/IEC 27002

Wdrażanie zabezpieczeń

szkolenia/testy

Eksploatacja sytemu zabezpieczeń

analiza stanu - monitorowanie, skanowanie, analiza, raportowanie –
wykrywanie słabości, nowych zagrożeń

Uniwersalne zasady bezpieczeństwa

Zasada przywilejów koniecznych – użytkownik systemu informacyjnego posiada prawo dostępu tylko do tych zasobów, które są konieczne do wykonywania zadań

Zasada usług koniecznych – tylko te które są konieczne do prawidłowego funkcjonowania szkoły

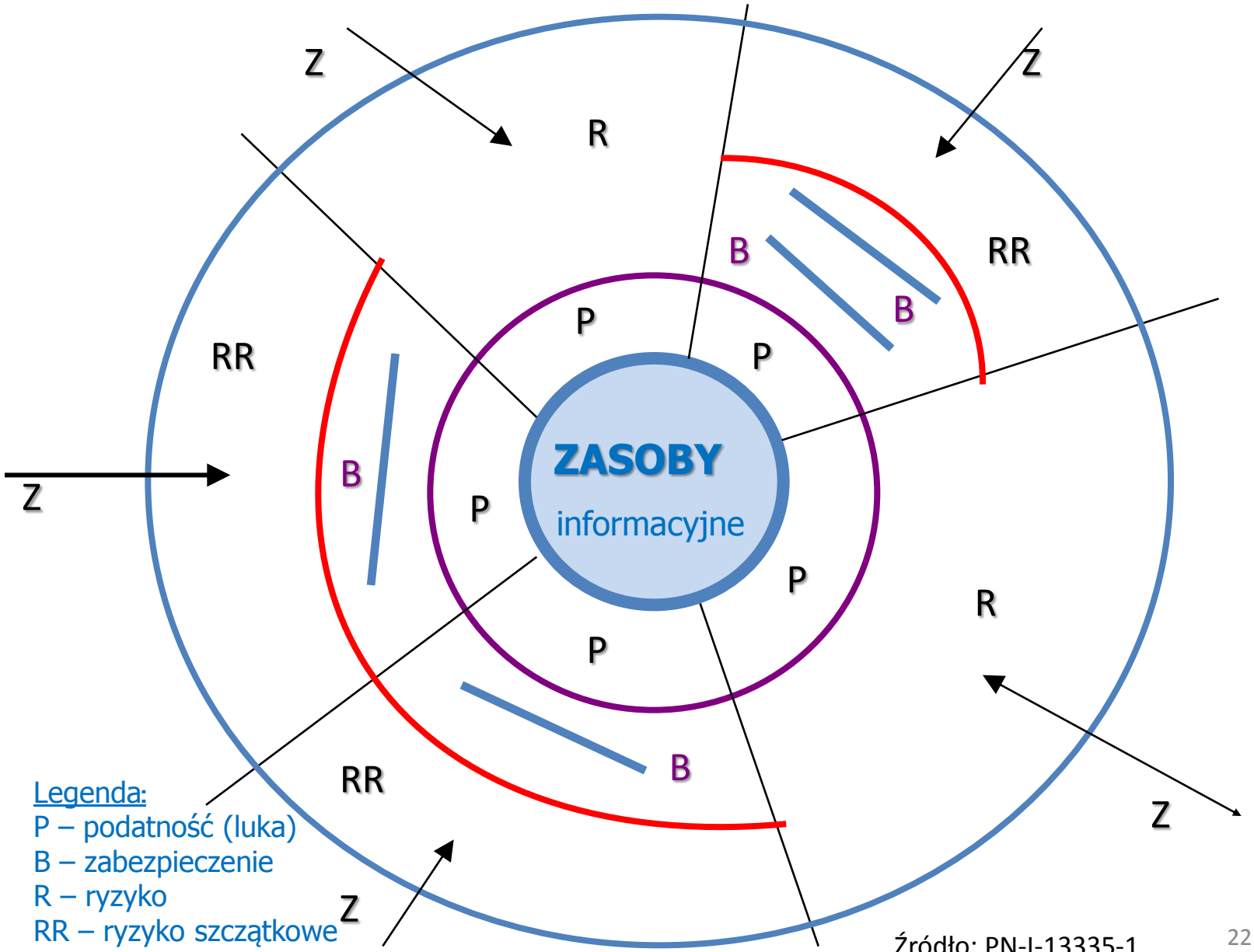
Zasada ubezpieczania zabezpieczeń – stosowanie wielowarstwowych zabezpieczeń, które ubezpieczają się wzajemnie

Zasada odpowiedzialności – za utrzymanie właściwego poziomu bezpieczeństwa odpowiada konkretna osoba (która wie jakie konsekwencje poniesie, jeśli zaniedba obowiązki)

Zasada świadomości – bezpieczeństwo zależy od świadomego zaangażowania każdego pracownika

Zasada najsłabszego ogniwa - poziom zabezpieczeń wyznacza najmniej zabezpieczony element systemu

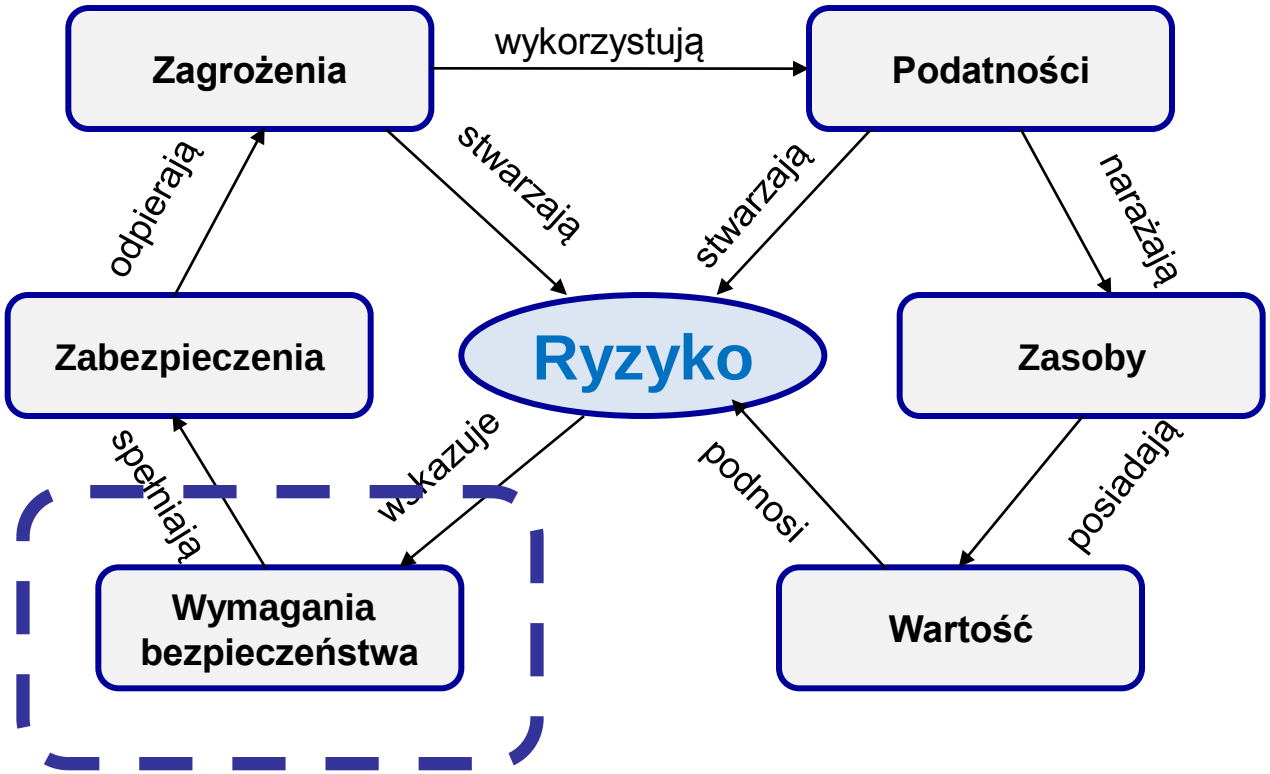
Ogólny model bezpieczeństwa



Legenda:
P – podatność (luka)
B – zabezpieczenie
R – ryzyko
RR – ryzyko szczątkowe
Z - zagrożenia

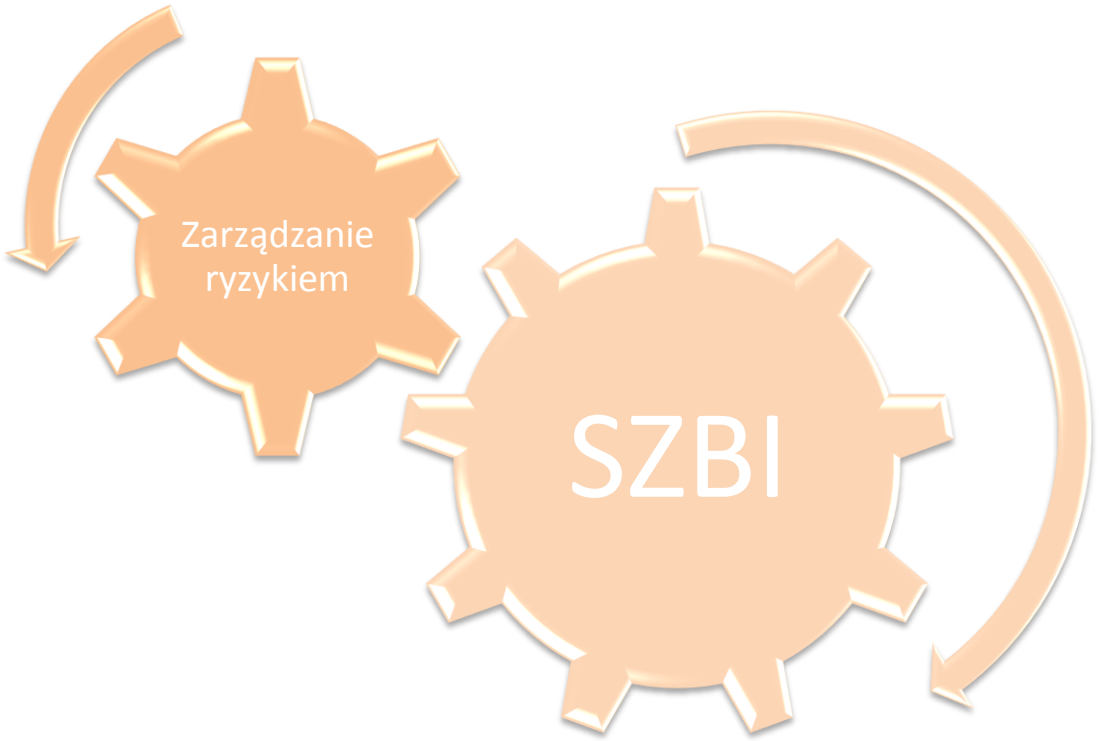
Źródło: PN-I-13335-1

Związki w zarządzaniu ryzykiem



Źródło: opr. wł. na podst. PN-I-13335-1

SZBI wg PN-ISO/IEC 27001 a zarządzanie ryzykiem



Bezpieczeństwo informacyjne wg serii PN-ISO/IEC 27000 a bezpieczeństwo ogólne

Konsekwencją wszelkich działań polegających na świadomym nadzorowaniu **bezpieczeństwa informacyjnego** (danych i informacji, które gromadzimy, korzystamy z nich i udostępniamy otoczeniu) jest wzrost bezpieczeństwa ogólnego

Bezpieczeństwo informacyjne → **Bezpieczeństwo ogólne**

Dziękuję za uwagę

grazyna.ozarek@pkn.pl

Bibliografia

- PN-ISO/IEC 27001:2014-12 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji – Wymagania
- PN-ISO/IEC 27002:2014-12 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji
- PN-ISO/IEC 27005:2014-01 Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji
- http://zabezpieczenia.com.pl/ochrona-informacji/teoria-ochrony-informacji-cz-1
- Krawiec J. Ożarek G.: Ochrona danych osobowych w praktyce. Wyd. PKN, Warszawa 2013
- Krawiec J. Ożarek G.: SZBI w praktyce. Zabezpieczenia. Wyd. PKN, Warszawa 2014
- http://www.wprost.pl/ar/475972/Koziej-Bezpieczenstwo-to-nie-stan-To-proces/