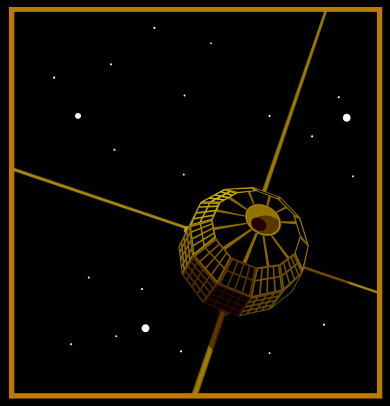
System zarządzania bezpieczeństwem informacji

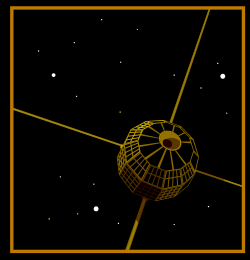
- zarys problematyki



- dr Marian Krupa

AGENDA

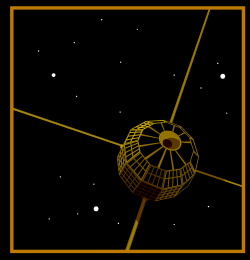
1. **Bezpieczeństwo informacji** – wprowadzenie do problematyki SZBI
2. **SYSTEM zarządzania bezpieczeństwem zasobów informacyjnych** – wymagania
3. **PROCES zarządzania bezpieczeństwem zasobów informacyjnych** – modelowanie i parametryzacja
4. **Zarządzanie projektem wdrożenia SZBI** – metodologia
5. **Audyt bezpieczeństwa systemów informacyjnych** – metodyka
6. **PDCA w procesach ISMS** – ciągłe doskonalenie
7. **Polityka bezpieczeństwa informacji** – studium przypadku



1. Bezpieczeństwo informacji

– wprowadzenie do problematyki SZBI

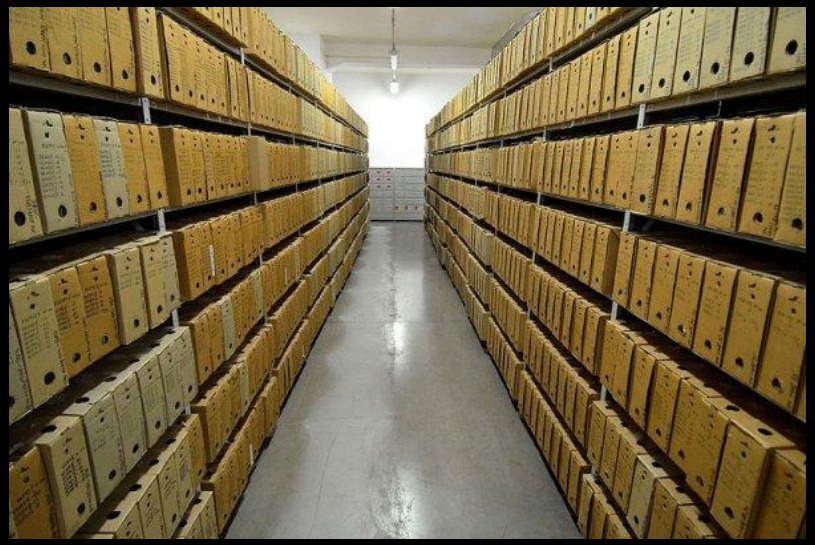
dr Marian Krupa



Megatrendy a cyberprestępczość

MEGATRENDY

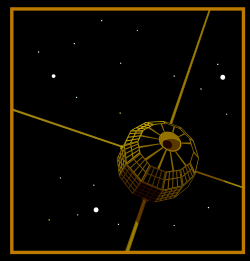
Zasoby informacyjne



Jak je chronić?

dr Marian Krupa

MEGATRENDY 2015

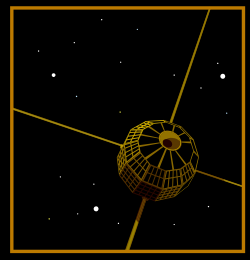


Wprowadzenie: RAPORT EY

- *Największym zagrożeniem obecnie są nasilające się **cyberataki**.*
- *5 z 10 największych **wycieków danych** w historii miało miejsce w 2013 i 2014 roku.*
- *Amerykańskie Centrum Studiów Strategicznych i Międzynarodowych szacuje, że **kradzież danych** oraz praw autorskich to koszt pomiędzy **375** a **575** miliardów USD rocznie.*

dr Marian Krupa

Cyberprzestępczość



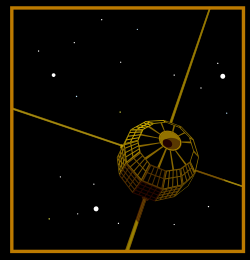
Wprowadzenie: RAPORT McAfee i CSIS

- *Podanie wiarygodnej wysokości strat finansowych, jaką powodują ataki cyberprzestępców, od dawna jest dla ekspertów dużym problemem.*

- *Cyberprzestępczość: **400 mld rocznie globalnych strat**!*
- *Według wyliczeń Uniwersytetu w Cambridge, na które powołuje się w swoim raporcie McAfee i CSIS, kradzież danych osobowych kosztuje jej ofiarę średnio **572** dolary.*

dr Marian Krupa

Cyberprzestępczość



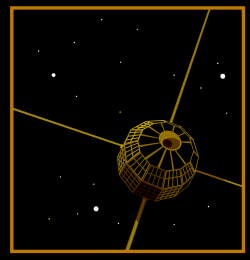
Wprowadzenie: RAPORT DELOITTE

- *Studium Deloitte sugeruje, że realny koszt cyberataku może być do 40% wyższy od ogólnych szacunków firm.*

- *Często koszty związane z cyberprzestępczością są ponoszone dopiero od 3 do 5 lat po ataku.*

dr Marian Krupa

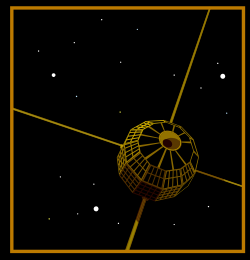
Cyberprzestępczość



WNIOSEK:

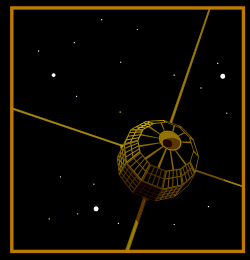
- *Wraz ze wzrostem znaczenia oraz KOSZTU pozyskania i zabezpieczenia informacji we współczesnym świecie oraz z rozwojem technik przetwarzania tych informacji (Internet, Hurtownie Danych) istotnym zagadnieniem w dzisiejszym świecie jest* ***zapewnienie ich bezpieczeństwa****.*

dr Marian Krupa



Rodzaje przestępstw

Przestępstwa w cyberprzestrzeni



Podział zagrożeń ze względu na źródło pochodzenie:

Ludzkie		Środowiskowe
Rozmyślne	Przypadkowe	
Podsłuch	Pomyłki	Trzęsienie ziemi
Modyfikacja informacji	Skasowanie pliku	Piorun
Włamania do systemu	Nieprawidłowe skierowanie	Powódź
Kradzież, wirus	Uszkodzenia fizyczne	Pożar

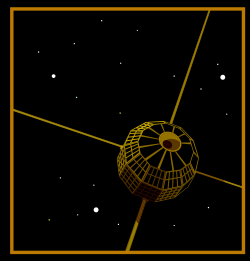
PN-I-13335-1

Ludzkie / rozmyślne / legalne
Oszustwo wynikające z niewiedzy użytkownika

dr Marian Krupa

J. Łańcucki (red.), Znormalizowane systemy zarządzania, UE w Poznaniu, Poznań 2010 .

Przestępstwa w cyberprzestrzeni

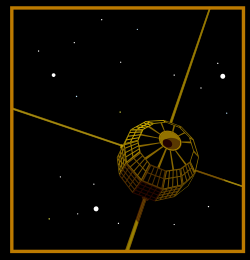


CHARAKTERYSTYKA zagrożeń:

- Źródło występowania,
- Motywacja,
- Częstotliwość pojawiania się,
- Dotkliwość szacowana przez zakres szkody,
- Rodzaj szkody (finansowa, prestiż, czas, zdrowie)

dr Marian Krupa

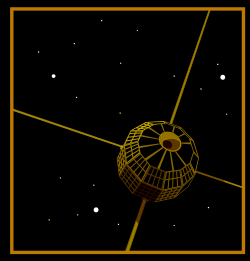
J. Łańcucki (red.), Znormalizowane systemy zarządzania, UE w Poznaniu, Poznań 2010 .



Rodzaje przestępstw

- przykłady

Przestępstwa w cyberprzestrzeni

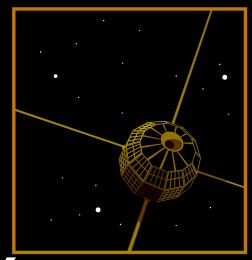


KRADZIEŻ TOŻSAMOŚCI:

- Kradzież tożsamości – jest to ogół przedsięwziętych czynności polegających na pozyskaniu prawdziwych danych realnie istniejących osób.
- Dane te są pozyskiwane w sposób niezgodny z obowiązującym prawem i w celu dalszego jego łamania, najczęściej w celu osiągnięcia korzyści majątkowej, ale również w celu naruszenia dóbr osobistych.

dr Marian Krupa

Przestępstwa w cyberprzestrzeni

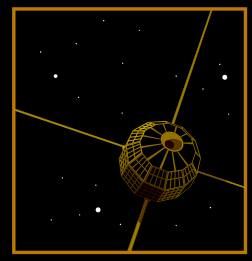


KRADZIEŻ TOŻSAMOŚCI: Atak zmasowany – „na ślepo”

- Uzyskiwanie danych poprzez wprowadzanie w błąd, co do autentyczności portali internetowych, przez wprowadzanie w błąd co do autentyczności źródła wiadomości elektronicznych przeki
fałszy
uzyski
autom
zmian

Art. 287. § 1. (oszustwo komputerowe gospodarcze) Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Przestępstwa w cyberprzestrzeni



KRADZIEŻ TOŻSAMOŚCI: Atak ukierunkowany

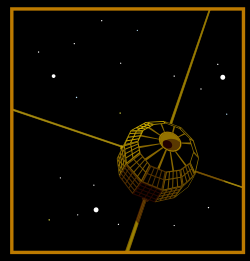
- Uzyskanie informacji poprzez włamanie ukierunkowane na konkretną osobę, która jest wcześniej obserwowana i podsłuchiwana, a także zbierane są o niej informacje ze

- *Art. 267. §1. (hacking i sniffing) Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

  § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

  § 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

Przestępstwa w cyberprzestrzeni

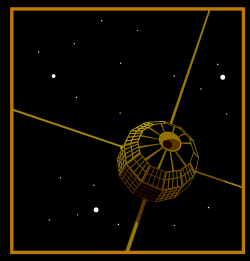


PHISHING (*spoofing*)**:**

- Jest skrzyżowaniem słów „fishing” – łowić ryby, z „personal data” – dane osobowe lub termin phishing jest niekiedy tłumaczony jako password harvesting fishing (łowienie haseł).

- Polega na **tworzeniu fałszywych wiadomości e-mail i witryn WWW**, które wyglądają identycznie jak serwisy internetowe znanych firm, aby skłonić klientów tych firm do podania swoich danych osobowych, numeru karty kredytowej lub informacji o elektronicznym rachunku bankowym – kodów i haseł potrzebnych do zalogowania i autoryzacji transakcji.

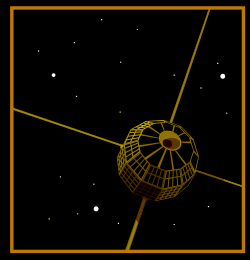
Przestępstwa w cyberprzestrzeni



PHISHING (*spoofing*)**: 1/2**

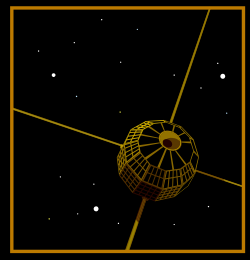
- Rozsyłanych sfałszowanych wiadomości e-mail, „udających” komunikaty wybranej instytucji (banku, urzędu itd.) z prośbą o przesłanie pinów, haseł lub kodów jednorazowych w celu weryfikacji poprawności działania serwisu.
- Rozsyłanych fałszywych wiadomości e-maili z odnośnikami (linkami) do spreparowanej strony WWW, np. e-banku, serwisu płatności elektronicznej, serwera poczty elektronicznej, serwisu społecznościowego lub serwisu aukcyjnego.
- Rozsyłanie złośliwego oprogramowania komputerowego (konie trojańskie).

Przestępstwa w cyberprzestrzeni



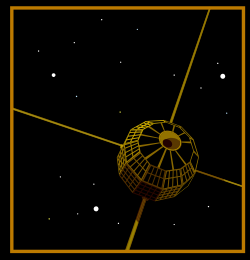
PHISHING (*spoofing*)**: 2/2**

- Zmiany adresu IP przedmiotowej strony na serwerze DNS i przekierowanie ruchu sieciowego na inny serwer, na którym „postawiono” wcześniej spreparowaną fałszywą stronę, np. banku,
- Zmiany pliku HOSTS znajdującego się na komputerze ofiary, który jest odpowiedzialny za interpretację adresów IP i przypisanych im nazw domenowych.



Wymogi prawne

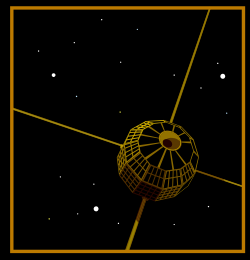
Uwarunkowania prawne



Ustawy i rozporządzenia:

- Ważną rolę w bezpieczeństwie informacji pełnią rozwiązania prawne, w których coraz częściej powoływane są normy z zakresu bezpieczeństwa informacji.
- *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.*
- *RODO – Rozporządzenie o Ochronie Danych Osobowych - 2018*

Uwarunkowania prawne



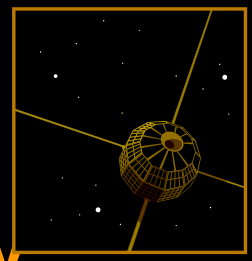
Informacja chroniona:

- Tajemnica postępowania administracyjnego i karnego,
- Tajemnica lekarska,
- Tajemnica skarbowa,
- Tajemnica handlowa,
- Tajemnica bankowa,
- Tajemnica ubezpieczeń społecznych,
- Tajemnica publicznego obrotu papierami wartościowymi,
- Tajemnica pomocy społecznej, itd.

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

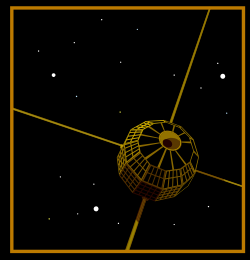
Uwarunkowania prawne



RODO (unijne rozporządzenie dotyczące ochrony danych osobowych):

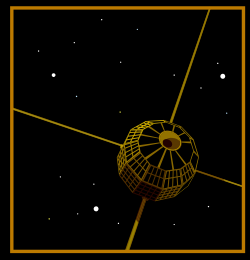
- Od maja 2018 roku przepisy dotyczące ochrony danych osobowych dla wszystkich 28 państw członkowskich mają być ujednolicone.
- Rozporządzenie zawiera zestaw wytycznych, które MUSI spełnić KAŻDY przedsiębiorca działający na terenie UE.

https://businessinsider.com.pl



Systemy / Normy zarządzania bezpieczeństwem informacji

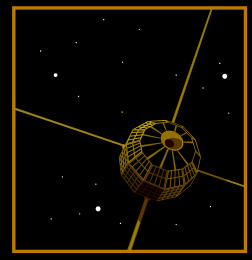
Systemy ZBI



Krok 1 - autorefleksja

dr Marian Krupa

Systemy ZBI - autorefleksja

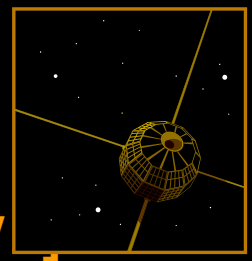


Co wiem o własnym systemie bezpieczeństwa danych?

- Przed podjęciem decyzji o wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) należy sprawdzić poziom wiedzy w powyższym zakresie !!!

dr Marian Krupa

Systemy ZBI - autorefleksja



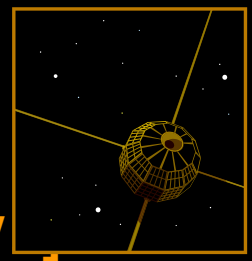
Co wiem o własnym systemie bezpieczeństwa danych? [1/

- Czy mogę powiedzieć, że **mam wdrożony system** zarządzania bezpieczeństwem informacji?

- **Wiem jak on działa** i mam wszystkie niezbędne procedury chroniące informację oraz aktywa mające wartość dla mojej firmy? (umowy, dokumenty niepubliczne, dane pracowników, sprzęt informatyczny)

dr Marian Krupa

Systemy ZBI - autorefleksja



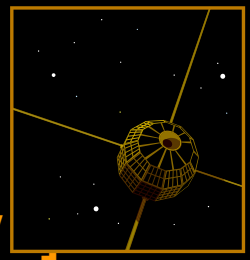
Co wiem o własnym systemie bezpieczeństwa danych? [1/]

- **Czy dobrze chronię dane** przetwarzanie w swojej jednostce? Czy mogę powiedzieć, że kontroluję wypływ danych z firmy? Wdrożyłem procesy, które regulują relacje z partnerami biznesowymi i dostosowałem model IT do modelu biznesowego w firmie?

- **Czy użytkownicy są szkoleni** wewnętrznie? Czy są świadomi zagrożeń, które mogą pojawić się w poczcie elektronicznej? Czy są świadomi metod ataków socjotechnicznych?

dr Marian Krupa

Systemy ZBI - autorefleksja



Co wiem o własnym systemie bezpieczeństwa danych? [2/]

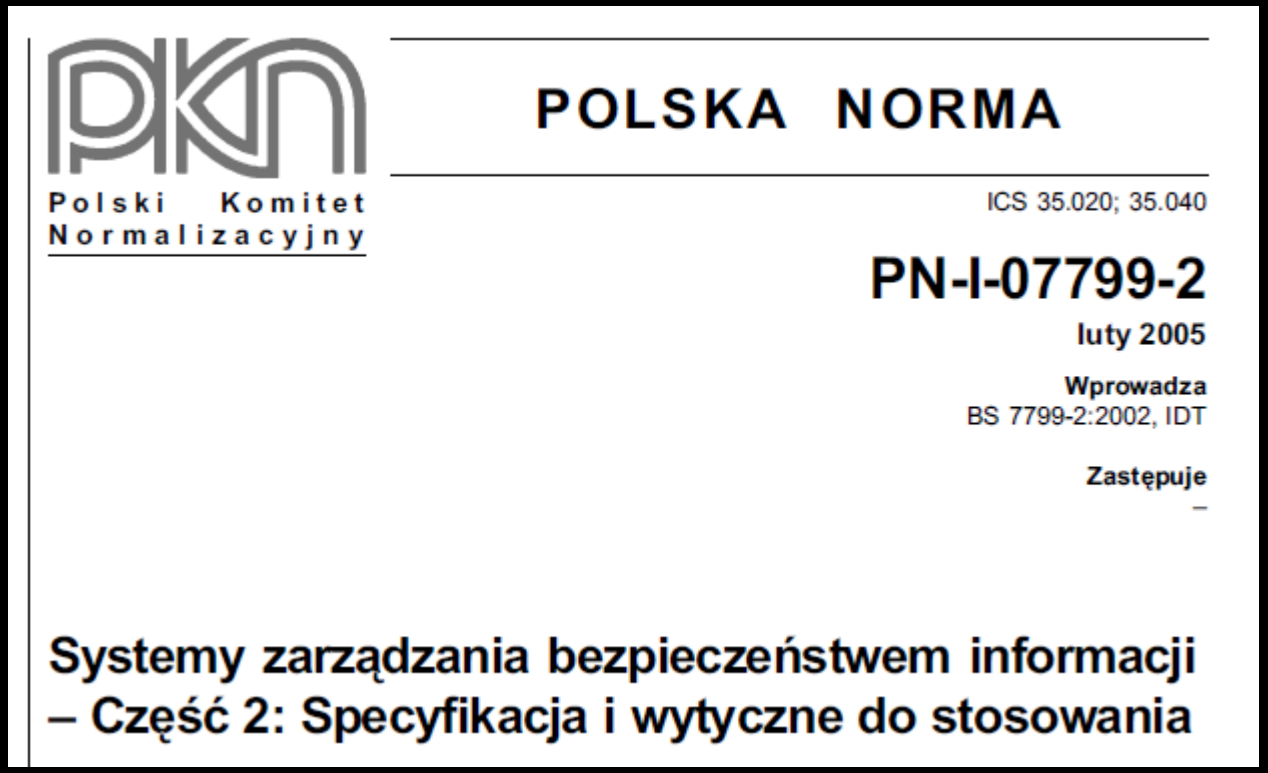
Jeżeli na większość z tych pytań pada odpowiedź negatywna

– jest to znak, że system zarządzania danymi wymaga wdrożenia lub zmian!

dr Marian Krupa

Systemy ZBI

POLSKIE Normy w zakresie zarządzania bezpieczeństwem informacji (British Standards Institution):



Polski Komitet Normalizacyjny

POLSKA NORMA

ICS 35.020; 35.040

PN-I-07799-2

luty 2005

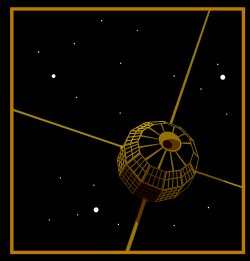
Wprowadza
BS 7799-2:2002, IDT

Zastępuje
–

Systemy zarządzania bezpieczeństwem informacji – Część 2: Specyfikacja i wytyczne do stosowania

dr Marian Krupa

Systemy ZBI

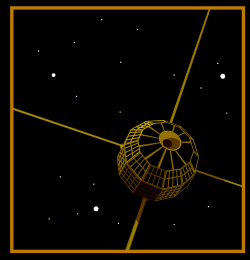


Normy w zakresie zarządzania bezpieczeństwem informacji i budowy systemów zarządzania bezpieczeństwem informacji:

- Polska Norma PN-ISO/IEC **27000**:2014-11 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – **Przegląd i terminologia**;
- jest wprowadzeniem normy ISO/IEC 27000:2014

dr Marian Krupa

Systemy ZBI

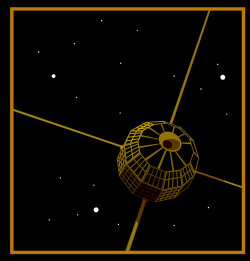


Normy w zakresie zarządzania bezpieczeństwem informacji i budowy systemów zarządzania bezpieczeństwem informacji:

- Polska Norma PN-ISO/IEC **27001**:2014-12 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – **Wymagania**;
- jest wprowadzeniem normy ISO/IEC 27001:2013

dr Marian Krupa

Systemy ZBI

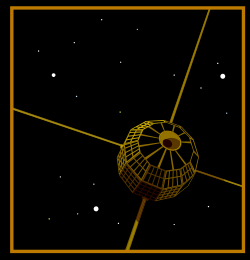


Normy w zakresie zarządzania bezpieczeństwem informacji i budowy systemów zarządzania bezpieczeństwem informacji:

- Polska norma PN-ISO/IEC **27002**:2014-12 Technika informatyczna – Techniki bezpieczeństwa – **Praktyczne zasady zabezpieczania informacji**;
- jest wprowadzeniem normy ISO/IEC 27002:2013.

dr Marian Krupa

Systemy ZBI

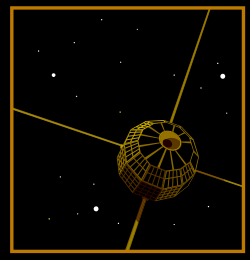


Normy w zakresie zarządzania bezpieczeństwem informacji i budowy systemów zarządzania bezpieczeństwem informacji:

- Norma PN-ISO/IEC **24762**:2010 Technika informatyczna – Techniki bezpieczeństwa – **Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.**
- Jest to wprowadzenie normy ISO/IEC 24762:2008.

dr Marian Krupa

Systemy ZBI



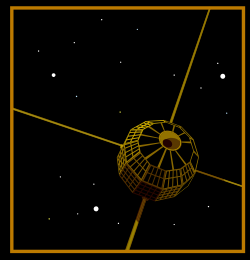
KRYPTOGRAFIA:

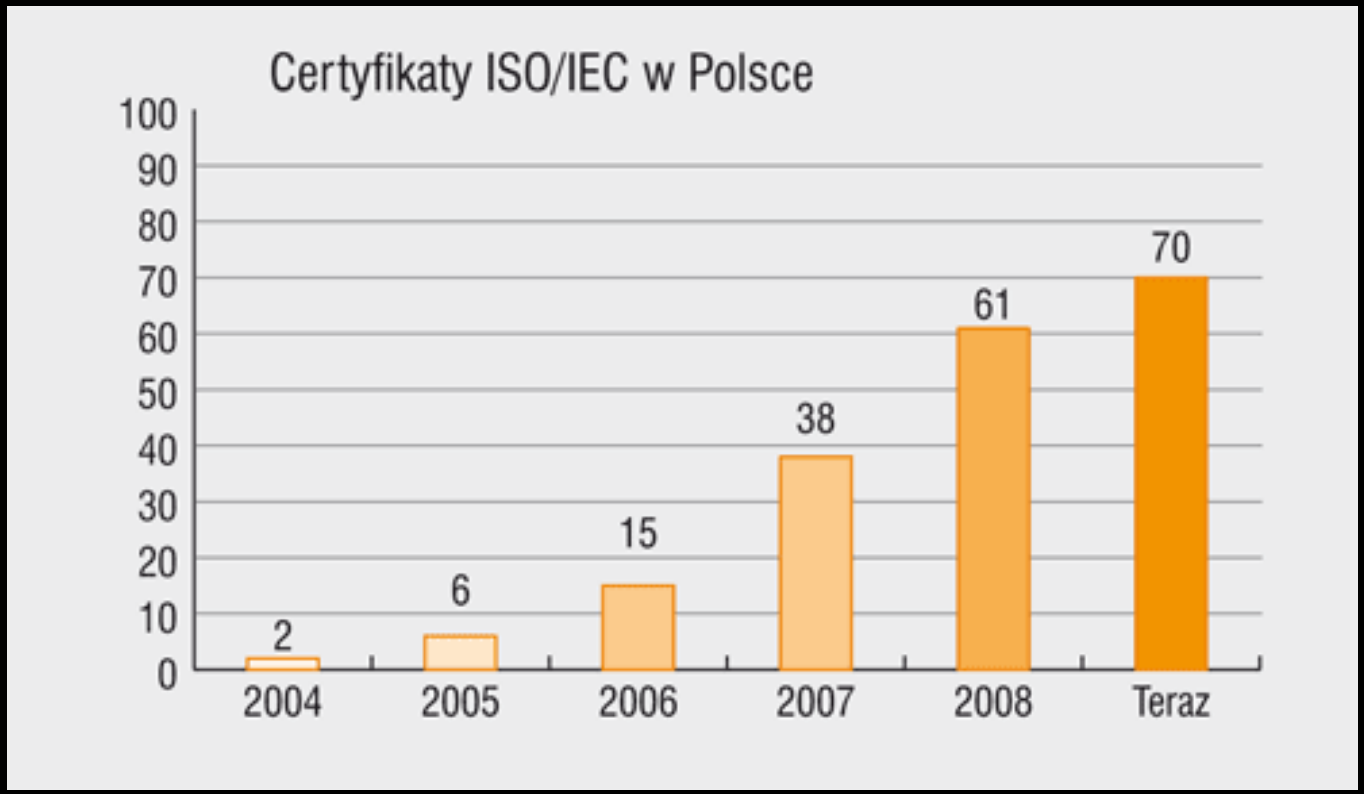
- **Algorytmy kryptograficzne** - podkomitet JTC 1/SC 27
- **Klucze kryptograficzne** - ISO/IEC/JTC 1/SC 27 WG 2

- *Powszechnie uważa się, że nie ma bezpiecznych rozwiązań kryptograficznych, których algorytm nie jest znany i starannie przetestowany, tajne natomiast pozostają klucze kryptograficzne.*

dr Marian Krupa

Systemy ZBI / certyfikacja

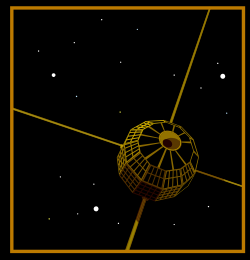


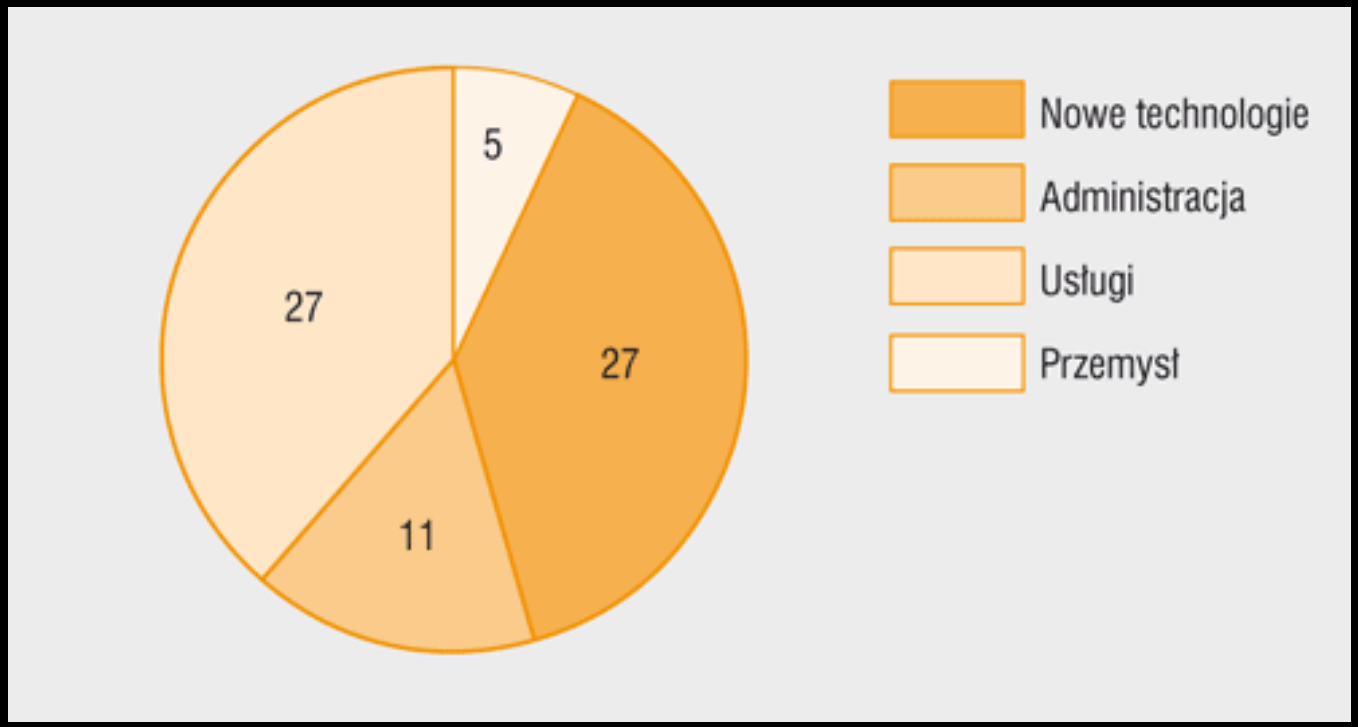


Wykres. Zrealizowane certyfikaty ISO/IEC w Polsce (stan na październik 2008 r.)

dr Marian Krupa

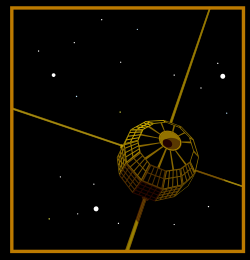
Systemy ZBI / certyfikacja





Wykres. Rozkład uzyskanych certyfikatów wg branż

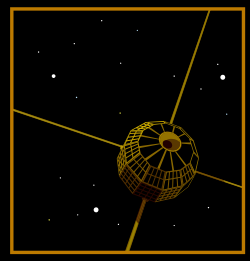
dr Marian Krupa



Certyfikacja

zgodnie z wymaganiami normy PN-ISO/IEC 27001:2007/13

Certyfikat - oferta



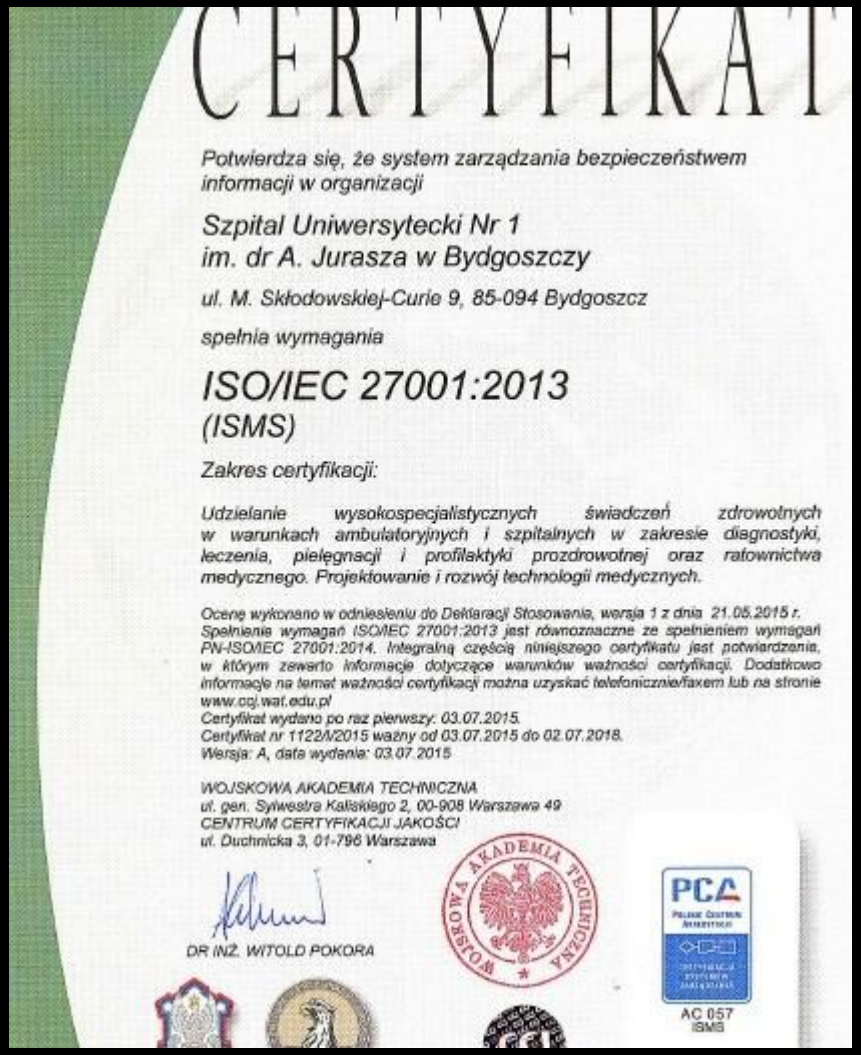
Certyfikat SZBI

- Polski Komitet Normalizacyjny oferuje **certyfikat SZBI** podmiotom zainteresowanym potwierdzeniem zgodności wdrożonego przez nie Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej SZBI, z wymaganiami normy PN-ISO/IEC 27001:2014-12.

- Oferowane przez PKN certyfikaty funkcjonującego w organizacji SZBI/SZJ na zgodność z normą PN-ISO/IEC 27001 mogą okazać się niezbędne np. jako element konieczny do uzyskania certyfikatu PN dla usług (wyrobów), gdzie bezpieczeństwo informacji ma wpływ na zapewnienie ciągłości zgodności usługi (wyrobu) z określonymi wymaganiami lub jako warunek współpracy…

dr Marian Krupa

Certyfikat SZBI (ISMS)



CERTYFIKAT

Potwierdza się, że system zarządzania bezpieczeństwem informacji w organizacji

Szpital Uniwersytecki Nr 1
im. dr A. Jurasza w Bydgoszczy

ul. M. Skłodowskiej-Curie 9, 85-094 Bydgoszcz

spełnia wymagania

ISO/IEC 27001:2013
(ISMS)

Zakres certyfikacji:

Udzielanie wysokospecjalistycznych świadczeń zdrowotnych w warunkach ambulatoryjnych i szpitalnych w zakresie diagnostyki, leczenia, pielęgnacji i profilaktyki prozdrowotnej oraz ratownictwa medycznego. Projektowanie i rozwój technologii medycznych.

Ocenę wykonano w odniesieniu do Deklaracji Stosowania, wersja 1 z dnia 21.05.2015 r.
Spełnienie wymagań ISO/IEC 27001:2013 jest równoznaczne ze spełnieniem wymagań PN-ISO/IEC 27001:2014. Integralną częścią niniejszego certyfikatu jest potwierdzenia, w którym zawarto informacje dotyczące warunków ważności certyfikacji. Dodatkowo informacje na temat ważności certyfikacji można uzyskać telefonicznie/faxem lub na stronie www.ccj.wat.edu.pl
Certyfikat wydano po raz pierwszy: 03.07.2015.
Certyfikat nr 1122/I/2015 ważny od 03.07.2015 do 02.07.2018.
Wersja: A, data wydania: 03.07.2015

WOJSKOWA AKADEMIA TECHNICZNA
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa 49
CENTRUM CERTYFIKACJI JAKOŚCI
ul. Duchnicka 3, 01-796 Warszawa

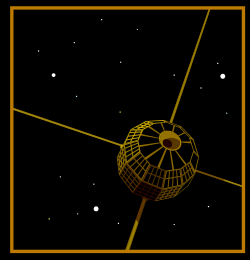
DR INŻ. WITOLD POKORA

WOJSKOWA AKADEMIA TECHNICZNA

PCA
AC 057
ISMS

ISMS - Information Security Management System

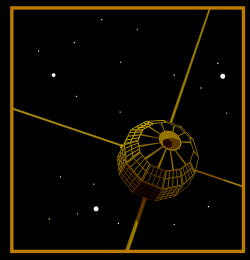
dr Marian Krupa



Kluczowe czynniki bezpieczeństwa informacji

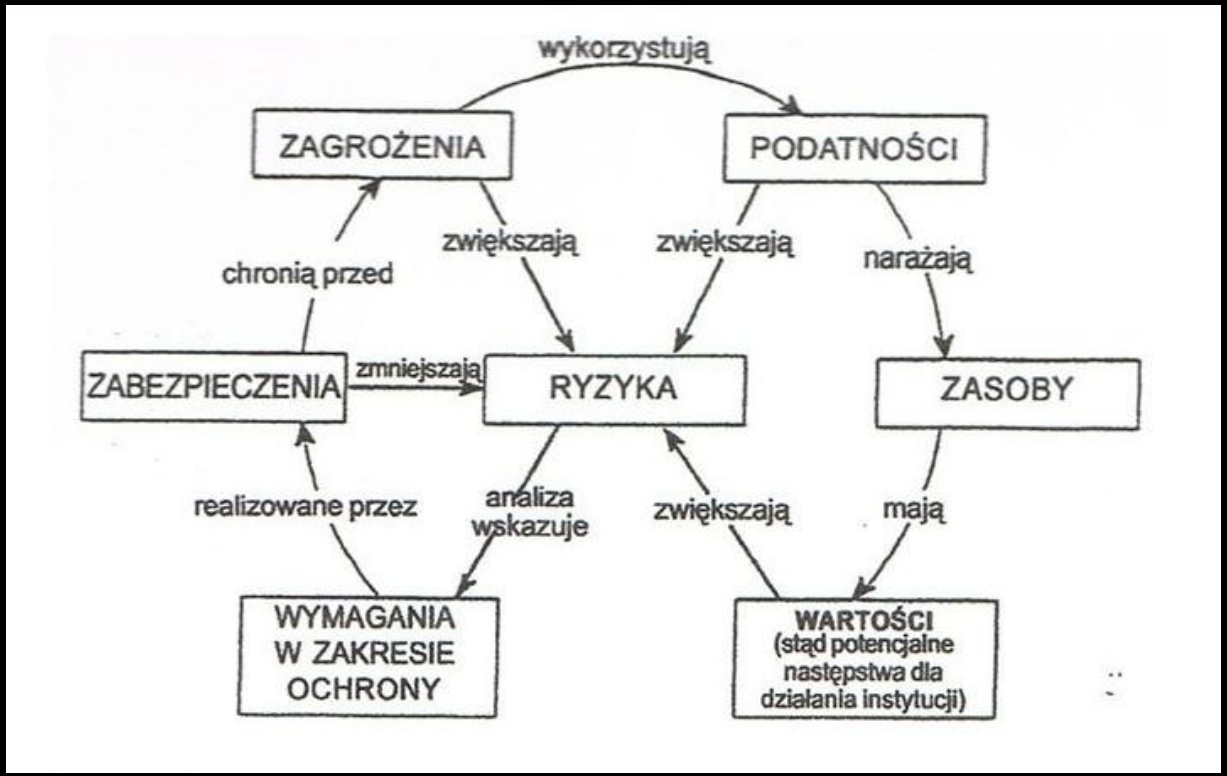
Model / System ZBI

KCB informacji



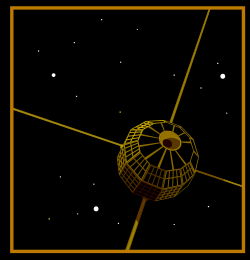
Zgodnie z PN-I-13335-1 wyróżniamy:

- ✓ Zagrożenie - Zasoby - Zabezpieczenie - Podatność



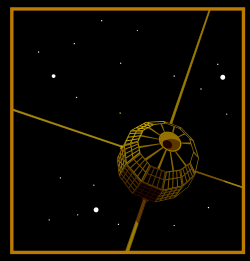
dr Marian Krupa

J. Łańcucki (red.), Znormalizowane systemy zarządzania, UE w Poznaniu, Poznań 2010 .



Definicje

DEFINICJE



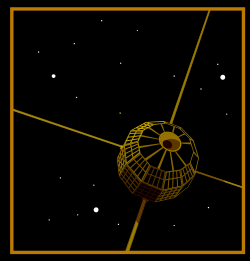
INFORMACJA:

- Aktyw, który ma dla instytucji wartość i dlatego należy go odpowiednio chronić [ISO/IEC/ 27002].
- Zbiór danych (faktów biznesowych, ekonomicznych, prawnych itd.) ustrukturyzowanych z punktu widzenia potrzeb decyzyjnych [MK].
- Wiedza biznesowa.

dr Marian Krupa

J. Łańcucki (red.), Znormalizowane systemy zarządzania, UE w Poznaniu, Poznań 2010 .

DEFINICJE



BEPIECZEŃSTWO:

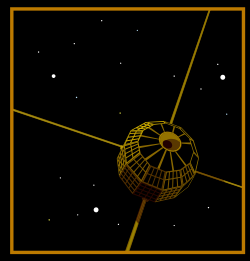
- Bezpieczeństwo teleinformatyczne – poziom uzasadnionego zaufania, że potencjalne straty nie zostaną poniesione.

- Celem wszystkich działań z zakresu bezpieczeństwa informacyjnego **jest ochrona danych (informacji)** a nie tyle infrastruktury teleinformatycznej (komputerów).

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE



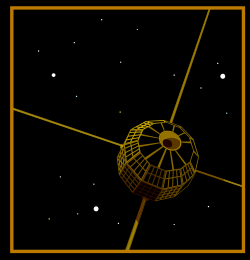
ZASOBY (1/2):

- Wszystko to co ma wartość dla instytucji [PN-I-3335-1:1999].
- **Aktywa** (zasoby) informatyczne: wszelkie oprogramowanie, dane, sprzęt, zasoby administracyjne, fizyczne, komunikacyjne lub ludzkie w systemie informatycznym lub w działalności informatycznej [PN-I-02000:2002].
- **Atrybuty** (aktywa): wartość, podatność, zabezpieczenia.

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE



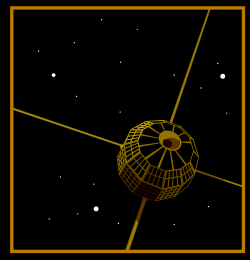
ZASOBY - przykłady:

- Informacyjne (dokumenty, bazy danych);
- Zasoby fizyczne (sprzęt komputerowy, budynki, infrastruktura teleinformatyczna;
- Oprogramowanie;
- Pracownicy;
- *Know-how* – zdolność świadczenia usług lub produkowania;
- Dobra niematerialne (wizerunek firmy – PR).

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE



ZAGROŻENIE:

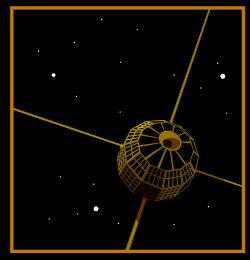
- Potencjalna możliwość naruszenia bezpieczeństwa systemu informatycznego [PN-I-02000:2002].

- Zagrożenie jest potencjalną przyczyną wystąpienia niekorzystnego zjawiska, które może spowodować szkody dla systemu lub organizacji.

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE



PODATNOŚĆ (1/2):

- Wady lub luki w:
  - W strukturze fizycznej organizacji,
  - procedurach,
  - zarządzaniu / administrowaniu,
  - sprzęcie / oprogramowaniu,
  - zamierzone lub niezamierzone działania personelu,

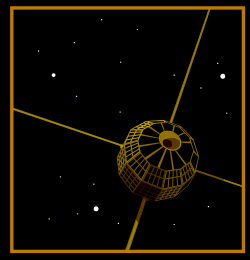
które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika.

[PN-I-02000:2002].

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE

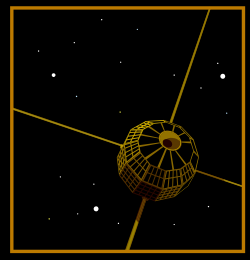


PODATNOŚĆ (2/2):

- Łatwość, z jaką można naruszyć bezpieczeństwo danego zasobu (np. danych) lub systemu (np. infrastruktury informatycznej).
- Analiza podatności polega na badaniu słabości, które mogą być wykorzystane przez zidentyfikowane zagrożenia.

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE



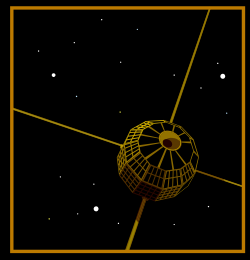
Ryzyko:

- Możliwość, że konkretne zagrożenie wykorzysta konkretną podatność systemu przetwarzania danych [PN-I-02000:2002].
- Ryzyko to prawdopodobieństwo wystąpienia przypadku, w którym podatność zasobu lub grup zasobów może zostać wykorzystana, by stworzyć zagrożenie ich zniszczenia lub utraty.

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE



- **Ryzyko** jest iloczynem trzech parametrów:
  1. Podatność zasobów;
  2. Prawdopodobieństwo wystąpienia zagrożenia;
  3. Wartość straty (potencjalna) powstałej w wyniku następstwa.

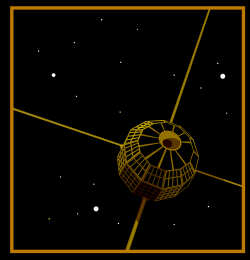
Następstwo:

- Rezultat niepożądanego incydentu [PN-I-13335-1:1999].

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE



Zabezpieczenia:

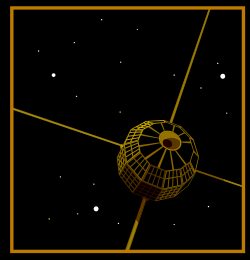
- Praktyka, procedura lub mechanizm redukujący ryzyko [PN-I-13335-1:1999].

- Celem zabezpieczeń jest:
  1. ochrona przed zagrożeniami;
  2. ograniczanie podatności;
  3. minimalizowanie następstw;
  4. wykrywanie błędów i nieprawidłowości
  5. wsparcie w trakcie ewentualnego odtwarzania systemu.

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE



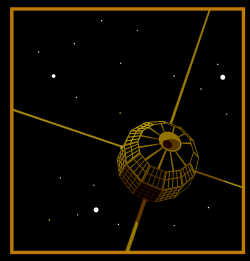
Zabezpieczenia: przykłady

1. Oprogramowanie antywirusowe,
2. Podpisy cyfrowe
3. Szyfrowanie
4. Sieciowe zapory (*firewall*)
5. Kopie zapasowe
6. Zasilanie rezerwowe
7. Narzędzia monitoringu i analizy sieci
8. Mechanizmy kontroli dostępu
9. ?

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE



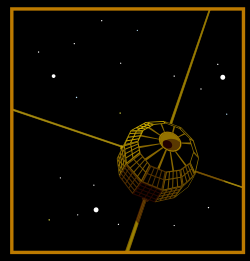
Polityka bezpieczeństwa instytucji: obejmuje wszystkie istotne zagrożenia dla prawidłowego funkcjonowania danej organizacji.

Polityka bezpieczeństwa informacji: dotyczy zagrożeń dotyczących ochrony informacji

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

DEFINICJE



Polityka bezpieczeństwa informacji

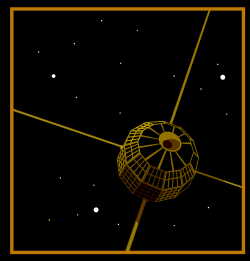
[TISM / Total Information Security Management]**:**

- Co podlega ochronie informacyjnej – wymagania prawne / wewnętrzne;
- Jakie systemy / platformy są nośnikiem informacji;
- Kto i w jakim zakresie ma dostęp do informacji;
- Kto odpowiada za bezpieczeństwo informacji;
- Kto odpowiada za infrastrukturę / systemy informacyjne.
- Kto odpowiada za kompleksowe zarządzanie bezpieczeństwem informacji;

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

CELE



Polityka bezpieczeństwa informacji (1/2)

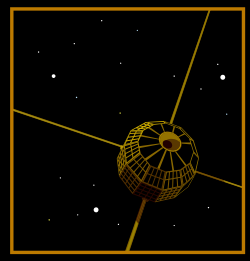
- **Poufność informacji** - oznacza, że jest ona dostępna wyłącznie dla osób, które zostały upoważnione do korzystania z danej informacji.

- **Dostępność informacji** - oznacza możliwość wykorzystania zasobu przez upoważnioną osobę, na każde uzasadnione żądanie, w ustalonym czasie.

- **Integralność informacji** - oznacza, że informacja nie uległa zmianie od czasu ostatniej autoryzowanej modyfikacji lub nie została usunięta w niekontrolowany sposób.

dr Marian Krupa

CELE



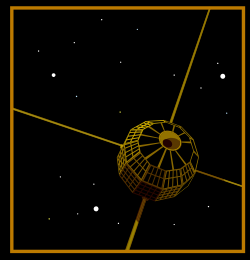
Polityka bezpieczeństwa informacji (2/2)

- **Autentyczność** - właściwość polegającą na tym, że pochodzenie lub zawartość danych jest taka jak deklarowana.

- **Niezaprzeczalność** - brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.

- **Rozliczalność** - właściwość pozwalającą przypisać określone działanie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.

dr Marian Krupa

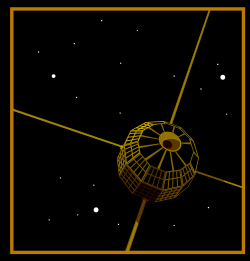


2. SYSTEM zarządzania bezpieczeństwem zasobów informacyjnych

– wymagania

dr Marian Krupa

Wymagania



ZAKRES NORMY ISO/IEC 27001:

- System zarządzania bezpieczeństwem informacji (SZBI),
- Odpowiedzialność kierownictwa,
- Wewnętrzne audyty jakości,
- Przeglądy SZBI realizowane przez kierownictwo,
- Doskonalenie SZBI.

Norma stanowi uniwersalny (ogólny) model ZSBI, który może być stosowany przez każdą organizację działającą w różnych sektorach.

dr Marian Krupa

J. Łańcucki (red.), Znormalizowane systemy zarządzania, UE w Poznaniu, Poznań 2010 .

WYMAGANIA

Bezpieczeństwo informacji (ISO 27001)

Poziom organizacji

Polityka bezpieczeństwa

Organizacja bezpieczeństwa informacji

Zarządzanie zasobami

Kontrola dostępu

Zgodność

Bezpieczeństwo personelu

Bezpieczeństwo fizyczne i środowiskowe

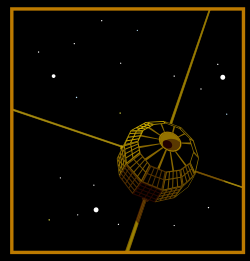
Utrzymanie i rozwój systemów informatycznych

Zarządzanie systemami i siecią

Zarządzanie ciągłością działania

Poziom operacyjny

Wymagania



Charakterystyka NORMY ISO/IEC 27001:

- **Polityka bezpieczeństwa** – tworzy ramy dla zaplanowania i wdrożenia SZBI w danej organizacji.

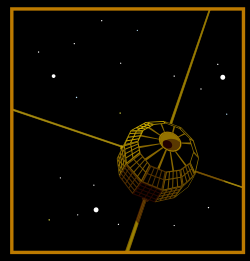
- Zawiera wskazówki w jaki sposób zarząd firmy / organizacji powinien zaplanować i potem wdrożyć sprawny SZBI.

- Definiuje również zakres odpowiedzialności kierownictwa.

dr Marian Krupa

J. Łańcucki (red.), Znormalizowane systemy zarządzania, UE w Poznaniu, Poznań 2010 .

Wymagania



Charakterystyka NORMY ISO/IEC 27001:

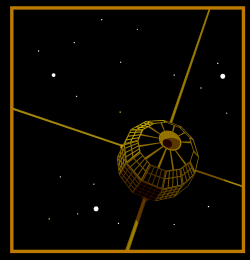
- **Organizacja bezpieczeństwa** – sposób wdrożenia polityki bezpieczeństwa

- Powołanie odpowiednich struktur / zespołów,
- Opracowanie metodyki,
- Zabezpieczenie finansowe,
- Zatrudnienie firm zewnętrznych w zakresie przygotowania danej organizacji do procesu certyfikacji.

dr Marian Krupa

J. Łańcucki (red.), Znormalizowane systemy zarządzania, UE w Poznaniu, Poznań 2010 .

Wymagania



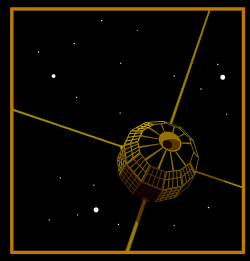
Charakterystyka NORMY ISO/IEC 27001:

- **Zarządzanie aktywami** – inwentaryzacja zasobów informacyjnych.
- **Bezpieczeństwo zasobów ludzkich** – system nadzoru i monitorowania poszczególnych grup pracowników w zakresie dostępu do zasobów informacyjnych.
- **Bezpieczeństwo fizyczne i środowiskowe** – fizyczne zabezpieczenie budynków, pomieszczeń – serwerowni, zasady konserwacji i procedur bezpieczeństwa pracy.

dr Marian Krupa

J. Łańcucki (red.), Znormalizowane systemy zarządzania, UE w Poznaniu, Poznań 2010 .

Wymagania



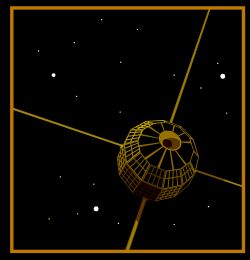
Charakterystyka NORMY ISO/IEC 27001:

- **Zarządzanie systemami i sieciami** – ochrona oprogramowania i danych.
- **Kontrola dostępu do systemów** – system ról i uprawnień oraz procedury administracyjne.
- **Nabycie systemu informacyjnego, rozwój i utrzymanie** – polityka bezpieczeństwa, system testów.
- **Zarządzanie incydentami** – monitorowanie zjawisk wpływających negatywnie na stan bezpieczeństwa informacyjnego oraz działania korygujące.

dr Marian Krupa

J. Łańcucki (red.), Znormalizowane systemy zarządzania, UE w Poznaniu, Poznań 2010 .

Wymagania



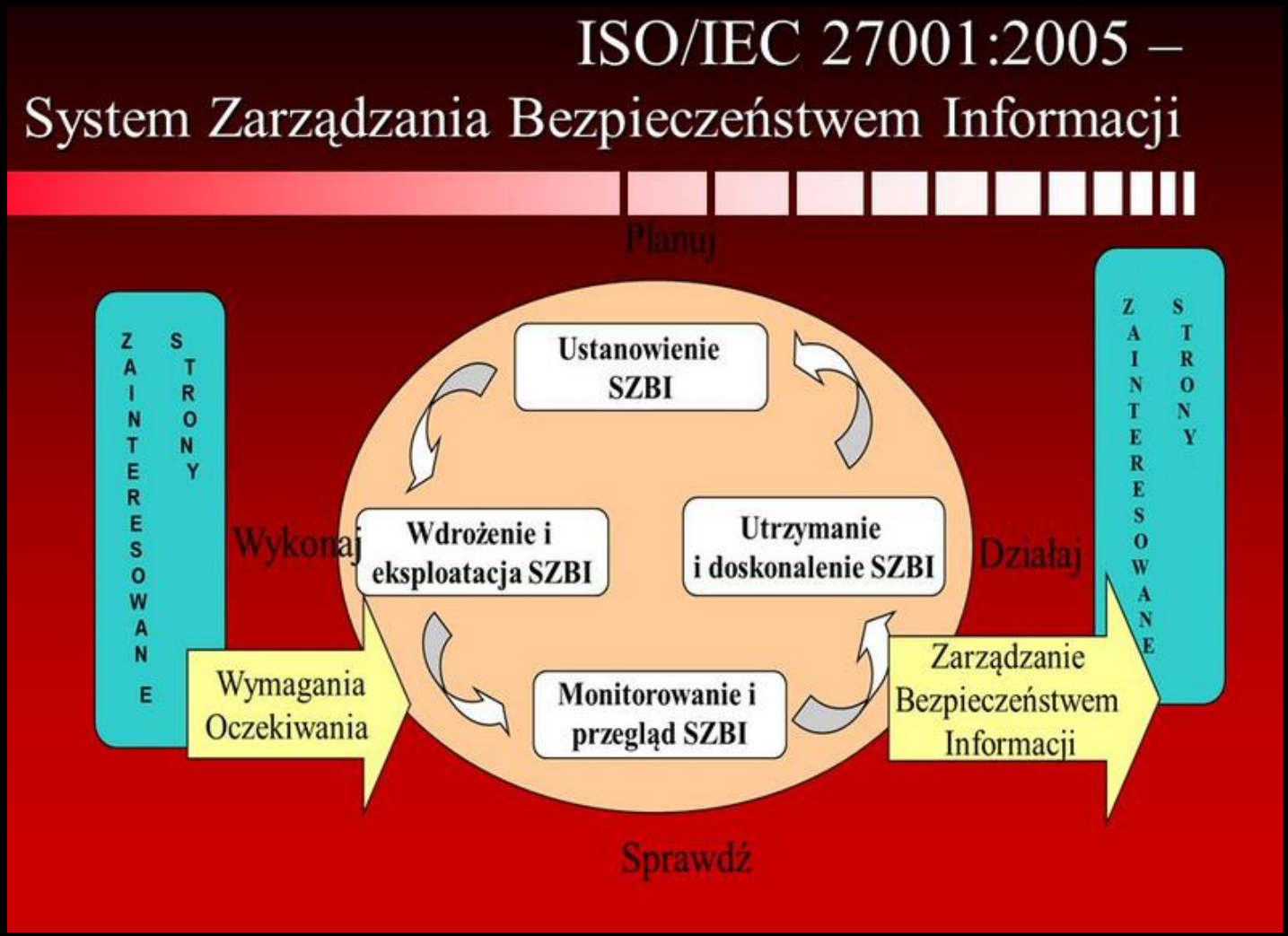
Charakterystyka NORMY ISO/IEC 27001:

- **Zarządzanie ciągłością działania** – reakcja na zjawiska kryzysowe – awarie, sytuacje losowe itd.
- **Zgodność z obowiązującym prawem oraz wewnętrznymi wymaganiami** – zakres zgodności przewidziany w procesie certyfikacji.

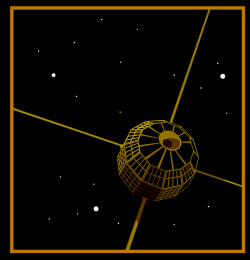
dr Marian Krupa

J. Łańcucki (red.), Znormalizowane systemy zarządzania, UE w Poznaniu, Poznań 2010 .

WYMAGANIA



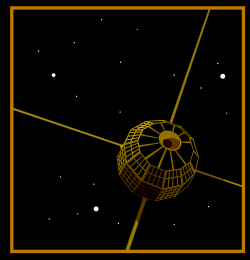
dr Marian Krupa



3. PROCES zarządzania bezpieczeństwem zasobów informacyjnych

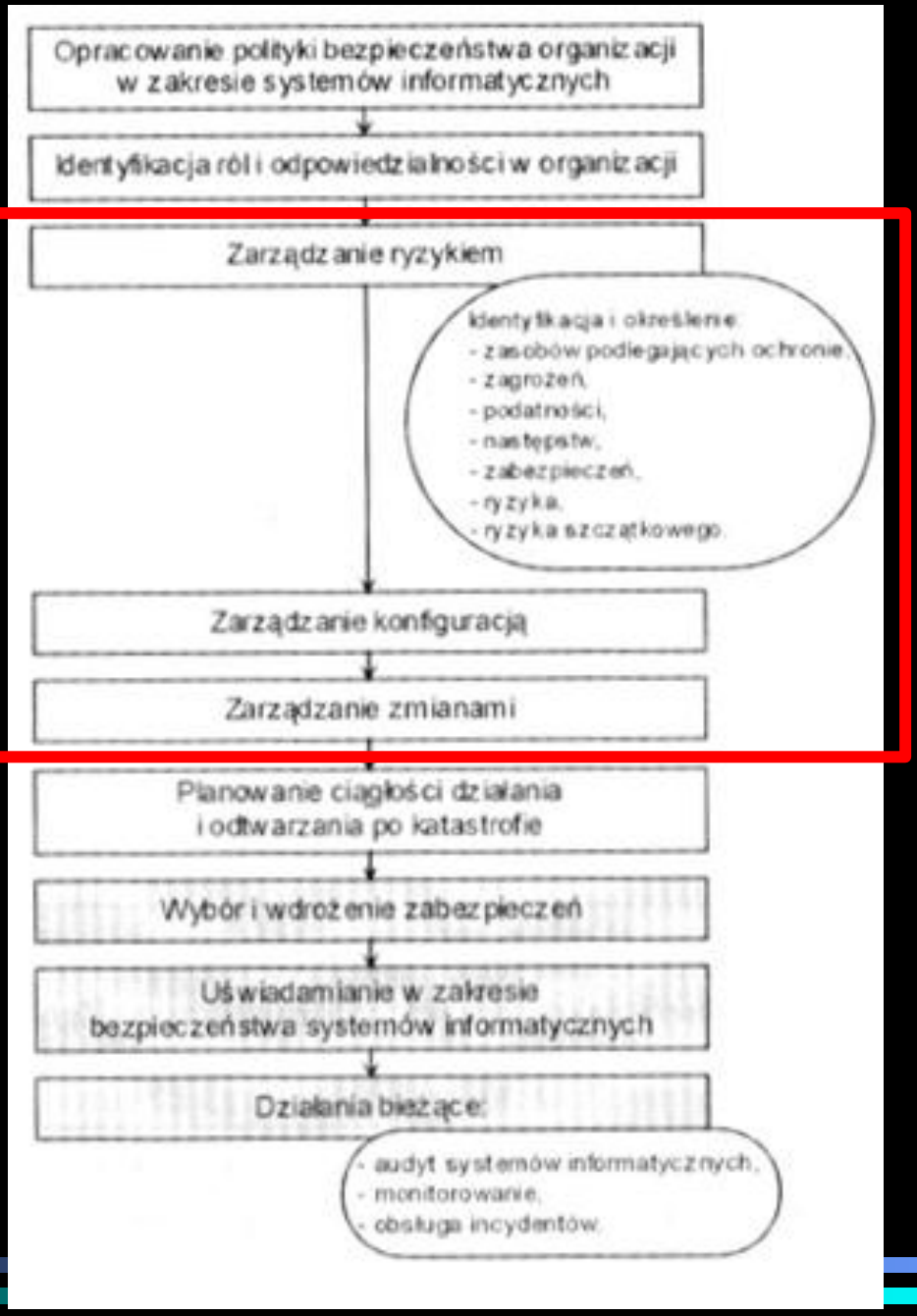
– modelowanie i parametryzacja

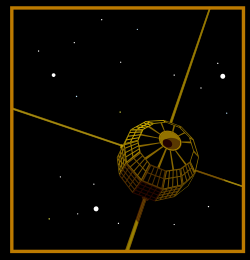
dr Marian Krupa



PROCES zarządzania bezpieczeństwem informacji

Proces ZBI

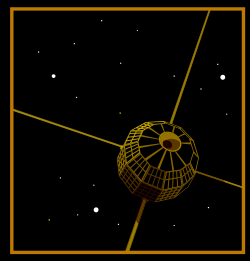




M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

dr Marian Krupa

Proces zarządzania bezpieczeństwem informacji



Definicje:

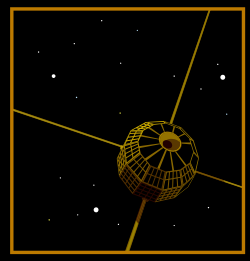
- **Proces ZBI** – logicznie uporządkowana z perspektywy zapewnienia bezpieczeństwa informacji sekwencja działań.

- Do kluczowych zadań / faz w ramach ZBI możemy zaliczyć:
  - Zarządzanie **ryzykiem** (zagrożeniami i podatnością)
  - Zarządzanie **konfiguracją** (implementacją)
  - Zarządzanie **zmianami** (doskonaleniem)

dr Marian Krupa

M. Molski, M. Łacheta, Przewodnik audytora systemów informatycznych, Helion, Gliwice 2007.

Proces zarządzania bezpieczeństwem informacji



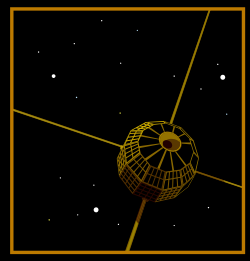
Zarządzanie ryzykiem [PN-I-133335-1:1999]:

- Całkowity proces **identyfikacji**, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na zasoby systemu informatycznego.
- Identyfikacja ryzyka obejmuje:
  1. Analizę środowiskową
  2. Scenariusze zagrożeń
  3. Analizę potencjalnych strat
  4. Identyfikację systemową / kompleksową

dr Marian Krupa

M. Molski, M. Łacheta, Przewodnik audytora systemów informatycznych, Helion, Gliwice 2007.

Proces zarządzania bezpieczeństwem informacji



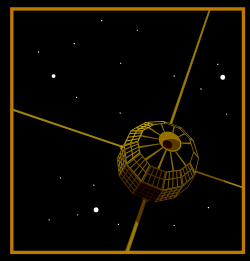
Zarządzanie konfiguracją:

- Proces weryfikacji zmian w systemie.
- Zarządzanie konfiguracją ma gwarantować, że wprowadzanie planów, zmian, koncepcji:
  1. nie obniża jakość funkcjonowania systemu w zakresie bezpieczeństwa organizacji;
  2. zapewnia ciągłość działania, w tym odtworzenie zasobów informacyjnych oraz infrastruktury IT;
  3. Spełnia standardy prawne w zakresie legalności oprogramowania

dr Marian Krupa

M. Molski, M. Łacheta, Przewodnik audytora systemów informatycznych, Helion, Gliwice 2007.

Proces zarządzania bezpieczeństwem informacji



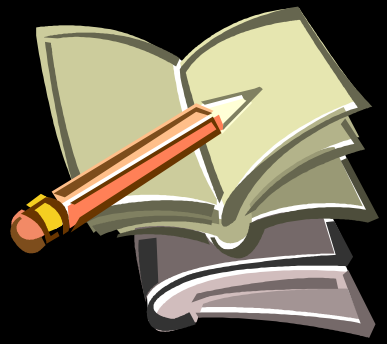
Zarządzanie zmianą:

- Identyfikacja nowych wymagań w zakresie bezpieczeństwa.
- Zmiany mogą dotyczyć:
  1. Nowych procedur i funkcji systemu
  2. Aktualizacji oprogramowania
  3. Zmian infrastruktury IT
  4. Pojawienie się nowych użytkowników / zakresów uprawnień
  5. Wprowadzenie dodatkowych funkcji w zakresie rozszerzenia potrzeb i zmian prawnych.

Zmiany mogą być realizowane tylko w ramach zatwierdzonych procedur!

dr Marian Krupa

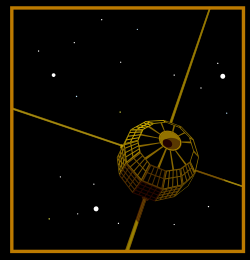
M. Molski, M. Łacheta, Przewodnik audytora systemów informatycznych, Helion, Gliwice 2007.



Projekt 1:

Model procesu ZBI w firmie XYZ

dr Marian Krupa



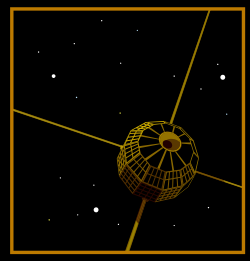
4. Zarządzanie projektem wdrożenia SZBI

– metodologia

dr Marian Krupa

Proces wdrożenia ISMS

Information Security Management System

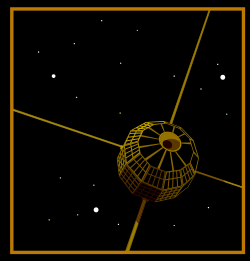


Zarządzanie projektem wdrożenia obejmuje:

1. **Definiowanie strategii / celów / źródeł finansowania**
2. **Etapy projektu** - harmonogram
3. **Strukturę projektu** – ludzie + zakres odpowiedzialności
4. **Dobór instrumentów i narzędzi zarządzania projektem**
5. **Ocenę ekonomiczną projektu**
6. **Ocenę jakościową projektu**

dr Marian Krupa

Proces wdrożenia ISMS/SZBI



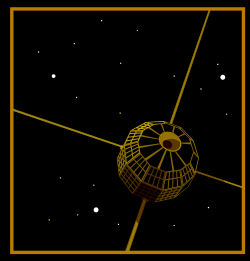
Etapy projektu SZBI:

1. **Ustanowienie ISMS** (Polityka bezpieczeństwa)
2. **Wdrożenie i eksploatacja systemu**
3. **Monitorowanie i przegląd**
4. **Utrzymanie i doskonalenie**
5. **Opracowanie dokumentacji**
6. **Przegląd wewnętrzny**
7. **Audyty wewnętrzne / zewnętrzne**

+ szkolenia, ?

dr Marian Krupa

Proces wdrożenia ISMS

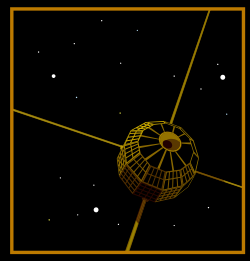


Ustanowienie ISMS:

- **Dokument / strategia ISMS** – uwzględnia charakter prowadzonej działalności, zasoby informacyjne będące w posiadaniu jednostki, lokalizację zasobów oraz stosowane technologie.
- Cele i zasady ISMS, wymagania prawne i biznesowe, ocena ryzyka i poziomu bezpieczeństwa, ocena skutków materializacji ryzyka, procedury dotyczące dokumentacji ora stosowanych norm.

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

Proces wdrożenia ISMS



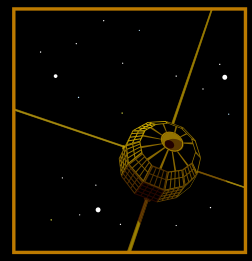
Wdrożenie strategii i eksploatacja systemu:

- **zawiera:**
  - Opracowanie planu postępowania z ryzykiem
  - Wdrożenie planu zarządzania ryzykiem
  - Wdrożenie zabezpieczeń
  - Przeprowadzenie szkoleń – uświadamianie i motywowanie
  - Eksploatacja infrastruktury / zabezpieczeń
  - Zarządzanie zasobami informacyjnymi
  - Opracowanie i wdrożenie procedur na wypadek sytuacji kryzysowych

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

Proces wdrożenia ISMS



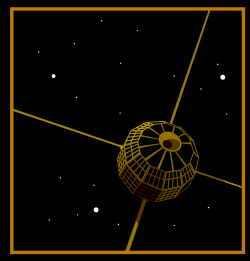
Monitorowanie i przegląd:

- **Organizacja powinna:**
  - Realizować procedury szybkiego reagowania na sytuacje kryzysowe!
  - Realizować regularne przeglądy skuteczności ISMS
  - Regularnie oceniać poziom ryzyka i zabezpieczeń
  - Cyklicznie przeprowadzać audyty wewnętrzne
  - Wykonywać przeglądy ISMS przez kierownictwo (raz do roku)
  - Zlecać realizację audytów zewnętrznych (raz na 2-3 lata)

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

dr Marian Krupa

Proces wdrożenia ISMS



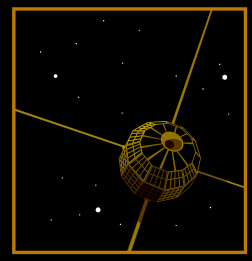
Utrzymanie i doskonalenie:

- **Organizacja powinna realizować następujące zadania:**
  - Projektować rozwiązania usprawniające ISMS
  - Wdrażać usprawnienia w ramach ISMS
  - Stale podejmować działania korygujące i zapobiegawcze
  - Informować różne grupy interesariuszy o wynikach działań
  - Deklarowanie o osiąganiu celów zabezpieczeń

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

dr Marian Krupa

Proces wdrożenia ISMS



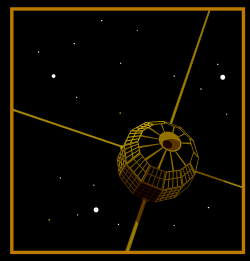
Wymagania dotyczące dokumentacji:

- **Prawidłowo opracowana dokumentacja ISMS zawiera:**
  - Deklaracje polityki bezpieczeństwa i celów stosowania zabezpieczeń
  - Zakres ISMS oraz zabezpieczenia potrzebne do realizacji ISMS
  - Raport z procesu szacowania ryzyka
  - Plan postępowania z ryzykiem
  - Opis procedur niezbędnych do zapewnienia efektywnego zarządzania bezpieczeństwem informacji
  - Deklarację stosowania (osoby odpowiedzialne)

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

Proces wdrożenia ISMS



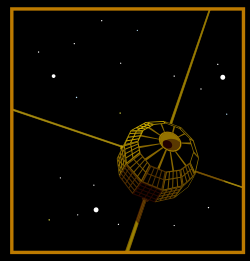
Przegląd wewnętrzny:

- **Norma PN-I-07799-2:2005 zobowiązuje kierownictwo do przeprowadzania regularnych przeglądów ISMS w oparciu o:**
  - Wyniki audytów wewnętrznych i zewnętrznych
  - Informacje zebrane od różnych grup interesariuszy
  - Raporty dotyczące skuteczności i efektywności ISMS
  - Informacje na temat działań korygujących i naprawczych
  - Ocena podatności i ryzyka na nowe zjawiska
  - Przegląd działań w zakresie zmian systemu
  - Zalecenia dotyczące doskonalenia ISMS

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

Proces wdrożenia ISMS



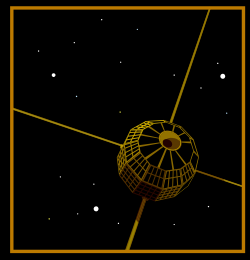
Audyty wewnętrzne / zewnętrzne:

- **Zalety:**
  - Optymalizacja, redukcja kosztów IT
  - Możliwość uzyskania usługi o lepszej jakości (obiektywność)
  - Dostęp
  - Gwaran
  - Koncen
  - Wyższa
  - Wyższa

Wady / RYZYKA:
- Wyższe koszty niż planowano
- Osłabienie pozycji rynkowej dostawcy usług
- Niedotrzymanie warunków umowy
- Niskie kompetencje w zakresie wiedzy branżowej
- Korzystanie z niewłaściwych standardów / wzorców branżowych

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

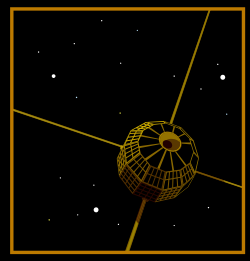


5. Audyt bezpieczeństwa systemów informacyjnych

– metodyka

dr Marian Krupa

AUDYT BSI



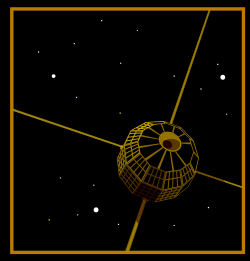
Definicje [PN-EN ISO 19011:2003]**:**

- **AUDYT** – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu (?).
- **Dowód z audytu** – zapisy, stwierdzenia faktu lub inne informacje, które są istotne ze względu na kryteria (zestaw polityk, procedur lub wymagań) audytu i możliwe do zweryfikowania.
- **Audytor** – osoba mające kompetencje (?) do przeprowadzenia audytu.

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

AUDYT BSI



Definicje [PN-EN ISO 9001:2009]**:**

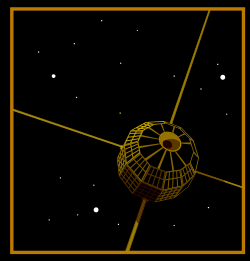
- Dążenie organizacji do doskonalenia powinno być jej celem.
- **Ciągłe doskonalenie** jest traktowane i identyfikowane jako jedna z zasad zarządzania jakością umożliwiająca poprawę efektywności organizacji, w tym zakresie ZBI.
- Jednym z narzędzi (instrumentem) służącym doskonaleniu systemu zarządzania jakością jest audyt.

J. Wawrzyniak, H. Małolepszy, *Audit narzędziem doskonalenia*, Instytut Technologii Bezpieczeństwa "MORATEX", 2010.

- **Audyt bezpieczeństwa informacyjnego** – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu ciągłego doskonalenia systemu ZBI.

dr Marian Krupa

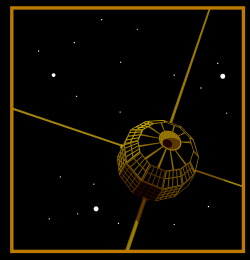
AUDYT BSI



Definicje

- Pojęcie audytu bywa mylone z kontrolą. W odróżnieniu od kontroli audyt działa na podstawie planu / problemu / dylematu (kontrola często przeprowadzana jest na zlecenie), skupia się na ocenie ex-ante (kontrola na ex-post) [Gołębiowski].
- Współcześnie audyt przeprowadzany jest w sposób ukierunkowany raczej na usprawnienie organizacji, niż na wskazanie nieprawidłowości [Knedler, Stasiak].
- Nie ma charakteru represyjnego, w raporcie z audyt nie powinno wymieniać się nazwisk i wskazywać winnych [Gołębiowski].

AUDYT BSI



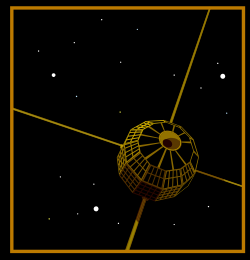
Wyróżniamy następujące kategorie audytu:

- Informatyczny; systemów informatycznych / teleinformatycznych
- Oprogramowania i legalności
- Bezpieczeństwa
- Telekomunikacyjny
- Infrastruktury; sprzętu informatycznego
- Inne ? (np. jakościowe dotyczące systemu zarządzania)

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

AUDYT BSI



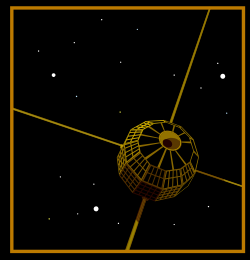
Audyt INFORMATYCZNY:

- Poświadczenie zgodności funkcjonowania systemów informatycznych z regulacjami prawnymi (bezpieczeństwo formalne / prawne);
- Weryfikacja poziomu bezpieczeństwa systemów informatycznych;
- Wykonanie inwentaryzacji zasobów informatycznych, w tym zasobów informacyjnych;
- Analizy ryzyka związanego z prowadzeniem projektu informatycznego;
- Ocena ekonomiczna dotycząca racjonalnego wykorzystania zasobów informatycznych w procesach biznesowych.

dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

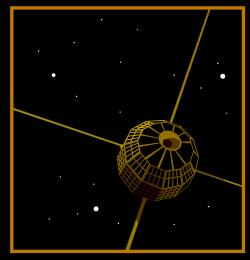
AUDYT BSI



Audyt BEZPIECZEŃSTWA (1/2) - korzyści:

- AB jest działaniem określającym faktyczne bezpieczeństwo funkcjonowania systemu informatycznego.
- Obejmuje wszystkie aspekty techniczne i administracyjne, służące wykrywaniu potencjalnych niebezpieczeństw, na jakie narażony jest konkretny system.
- Dzięki audytom bezpieczeństwa wykrywane są słabe punkty systemu, co pozwala na ich wzmocnienie i dzięki temu zmniejszenie ryzyka utraty danych lub dostępu do nich przez osoby nieuprawnione.

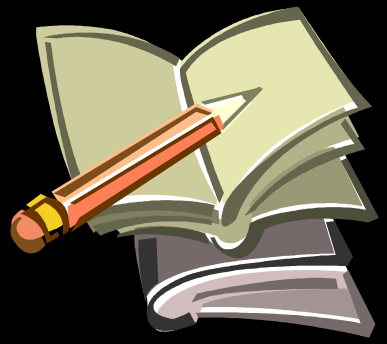
AUDYT BSI



Audyt BEZPIECZEŃSTWA (2/2) - korzyści:

- Fachowa ocena poziomu bezpieczeństwa teleinformatycznego,
- Wykrycie słabych punktów w systemie zabezpieczeń wraz z oceną potencjalnych zagrożeń,
- Wiarygodność dla kontrahentów,
- Opracowanie polityki bezpieczeństwa i wdrożenie jej do systemu,
- Usprawnienie działania sieci teleinformatycznej i zarządzania nią,
- Dostarczenie narzędzi oraz środków do przeciwdziałania zagrożeniom,
- Zmniejszenie ryzyka związanego z ujawnieniem danych przechowywanych w systemie,
- Personel zna zasady bezpieczeństwa teleinformatycznego.

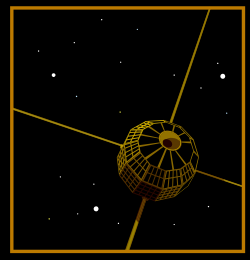
dr Marian Krupa



Projekt 2:

Audyt SZBI w firmie XYZ

dr Marian Krupa

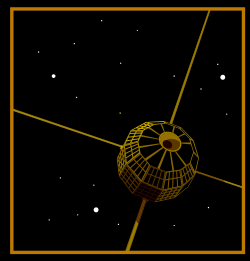


6. PDCA w procesach

ISMS – ciągłe doskonalenie

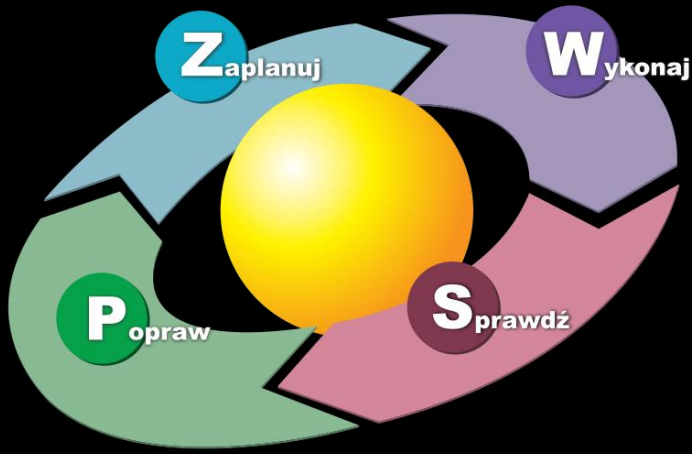
dr Marian Krupa

PDCA w ISMS



Ciągłe doskonalenie:

- **Ustanowienie i zarządzanie ISMS wymaga cyklicznego podejścia, którego celem jest zapewnienie, że procedury przyjęte w danej organizacji są dokumentowane i w razie potrzeby doskonalone.**

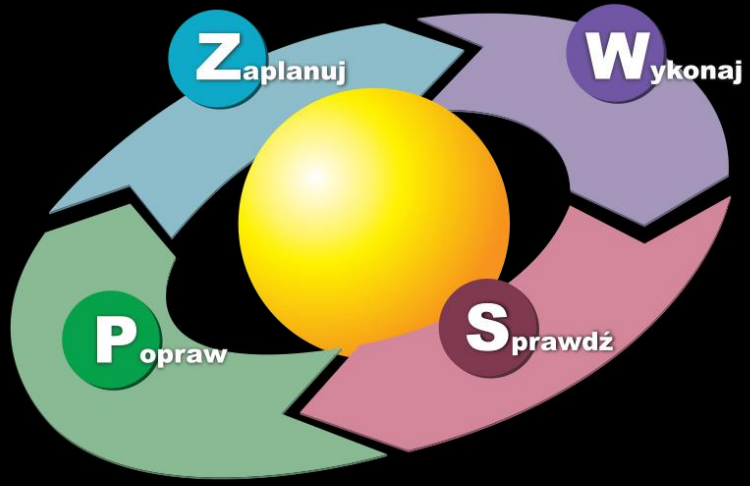


dr Marian Krupa

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

PDCA w ISMS

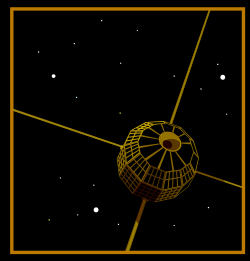
Ciągłe doskonalenie:



Planuj – *Plan* (ustanowienie ISMS)	Ustanowienie polityki ISMS, celów, procesów i procedur istotnych dla zarządzania ryzykiem oraz doskonalenia bezpieczeństwa informacji tak, aby uzyskać wyniki zgodne z ogólnymi politykami i celami organizacji.
Wykonuj – *Do* (wdrożenie i eksploatacja ISMS)	Wdrożenie i eksploatacja polityki ISMS, zabezpieczeń, procesów i procedur.
Sprawdzaj – *Check* (monitorowanie i przegląd ISMS)	Szacowanie i – tam, gdzie ma zastosowanie – pomiar wydajności procesów w odniesieniu do polityki ISMS, celów i doświadczenia praktycznego oraz dostarczanie raportów kierownictwu do przeglądu.
Działaj – *Act* (utrzymanie i doskonalenie ISMS)	Podejmowanie działań korygujących i zapobiegawczych, bazujących na wynikach wewnętrznego audytu ISMS i przeglądzie realizowanym przez kierownictwo lub na innych istotnych informacjach w celu zapewnienia ciągłego doskonalenia ISMS.

dr Marian Krupa

PDCA w ISMS

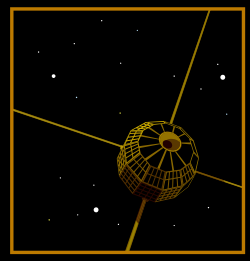


PDCA – Faza planowania:

- Celem fazy planowania jest ustanowienie polityki bezpieczeństwa oraz procedur dla zarządzania ryzykiem i doskonalenia ISMS.
- Etap ten ma zapewnić, że system zarządzania bezpieczeństwem informacji został ustanowiony prawidłowo, zidentyfikowano wszystkie rodzaje ryzyka i opracowano odpowiedni plan ich ograniczenia.
- Wytyczne określające zawartość wspomnianej polityki podaje ISO/IEC 17799.

dr Marian Krupa

PDCA w ISMS

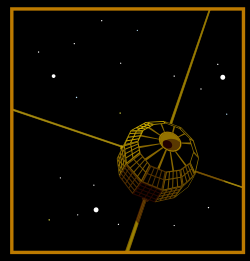


PDCA – Faza wykonania:

- Na etapie wykonania ma miejsce wdrożenie i eksploatacja przyjętej polityki bezpieczeństwa oraz ustalonych zabezpieczeń i procedur.
- W celu zapewnienia skutecznego funkcjonowania ISMS należy przypisać odpowiednie zasoby (materialne i niematerialne) do implementacji zabezpieczeń oraz…
- wdrożyć program uświadamiania i szkolenia pracowników w zakresie zarządzania ryzykiem i bezpieczeństwem.

dr Marian Krupa

PDCA w ISMS

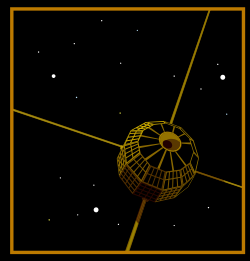


PDCA – Faza sprawdzania (1/2):

- W fazie sprawdzania realizowany jest pomiar lub szacowanie wykonania procedur i wymogów polityki bezpieczeństwa.
- Działania sprawdzające mają poświadczyć, że wdrożone zabezpieczenia funkcjonują efektywnie i zgodnie z zamierzeniami, a ISMS pozostaje skuteczny.
- Jeśli mechanizmy zabezpieczające okażą się nieodpowiednie, należy podjąć działania naprawcze.
- Celem czynności korygujących jest utrzymanie spójności dokumentacji ISMS i niedopuszczenie do narażania instytucji na nieakceptowane ryzyko.

dr Marian Krupa

PDCA w ISMS

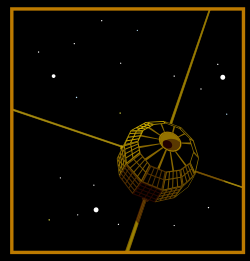


PDCA – Faza sprawdzania (2/2):

- **Rutynowe sprawdzanie** – procedury wykonywane regularnie w ramach procesu biznesowego, które pozwalają wykryć nieprawidłowości będące wynikiem przetwarzania.
- **Samokontrolujące procedury** – narzędzie umożliwiające natychmiastowe wykrycie każdego błędu pojawiającego się w trakcie wykonywania jakiegoś procesu (np. narzędzie monitorujące sieć, które powoduje uruchomienie alarmu w momencie wystąpienia defektu).
- **Uczenie się od innych** – zbadanie, jak inne instytucje radzą sobie z określonymi problemami dotyczącymi ISMS.
- **Wewnętrzne audyty ISMS** – działania wykonywane regularnie (przynajmniej raz w roku) w celu określenia poprawności funkcjonowania ISMS.

dr Marian Krupa

PDCA w ISMS

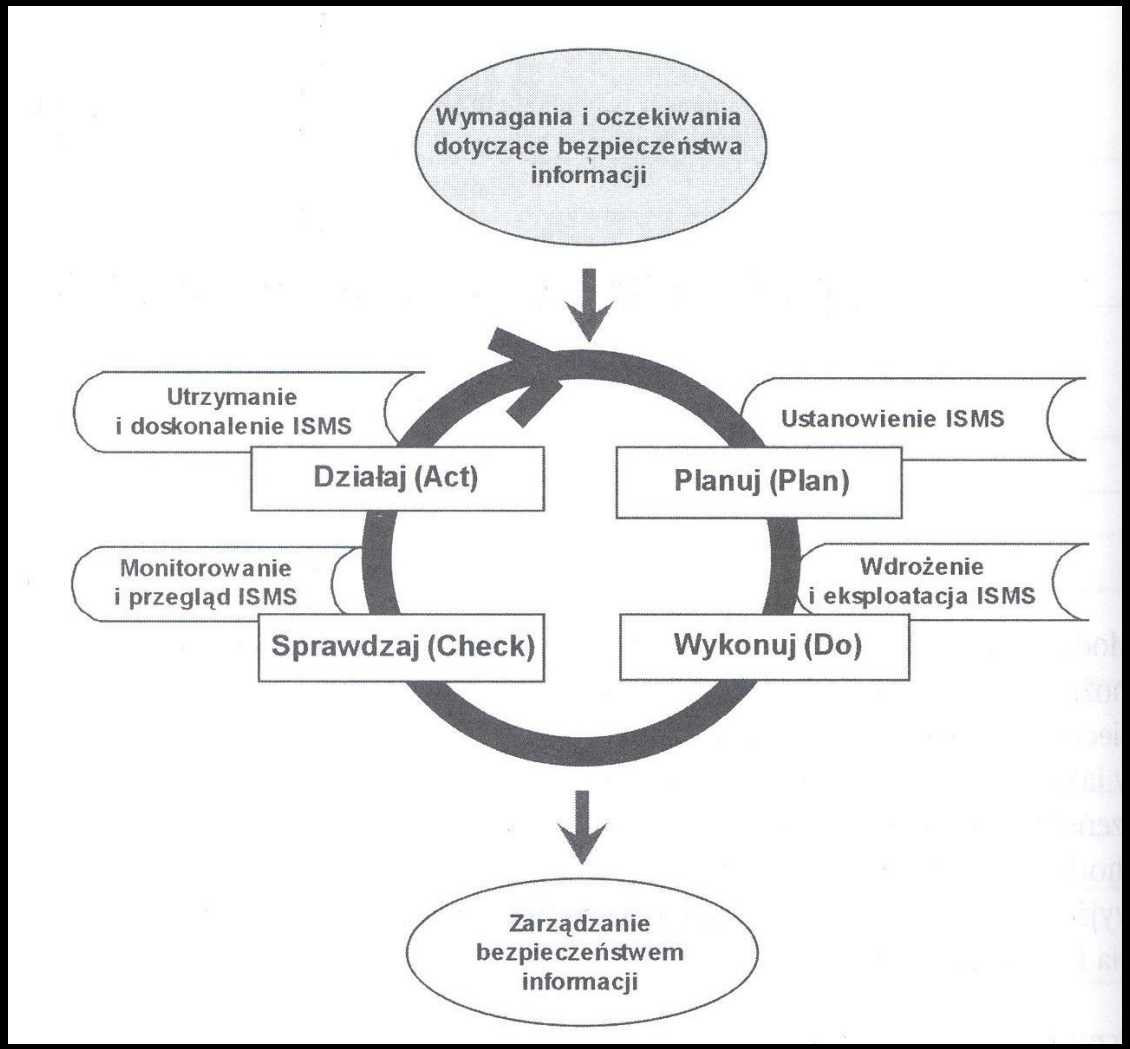


PDCA – Faza działania:

- Celem fazy działania jest podjęcie (wdrożenie) odpowiednich czynności naprawczych oraz zapobiegawczych na podstawie wniosków kierownictwa wyciągniętych z przeprowadzonych w poprzedniej fazie testów.
- Wszystkie te działania mają prowadzić do **ciągłego doskonalenia** ISMS.
- Według PN-I-07799-2:2005 zaleca się podejmowanie działań korygujących (lub reaktywnych) w celu eliminowania przyczyny niezgodności lub innych niepożądanych sytuacji i zapobiegania ich powtórzeniu.

dr Marian Krupa

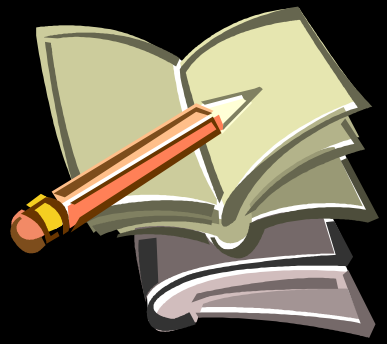
PDCA w ISMS



Model PDCA wykorzystywany w procesach ISMS:

M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

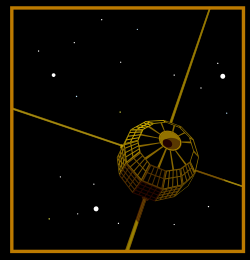
dr Marian Krupa



Projekt 3:

PDCA w SZBI

dr Marian Krupa

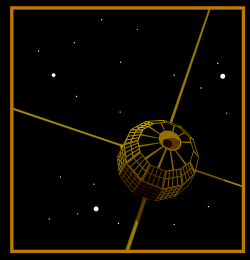


7. Polityka bezpieczeństwa informacji (PBI)

– studium przypadku

dr Marian Krupa

PBI w Urzędzie Marszałkowskim w Poznaniu

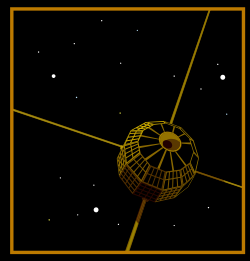


POLITYKA BEZPIECZEŃ INFORMACJI

Spis treści:

dr Marian Krupa

PBI w Urzędzie Marszałkowskim w Poznaniu



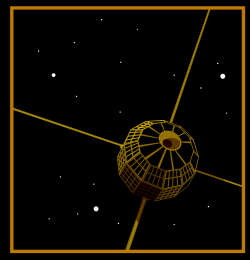
Polityka Bezpieczeństwa Informacji (PBI)

DEKLARACJA: zgodnie z wymaganiami normy PN-ISO/IEC 27001:2007 system ZBI podlega następującym regułom:

- **Reguła poufności informacji** - zapewnienie, że informacja jest udostępniana jedynie osobom upoważnionym
- **Reguła integralności informacji** - zapewnienie zupełnej dokładności i kompletności informacji oraz metod jej przetwarzania
- **Reguła dostępności informacji** - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba

dr Marian Krupa

PBI w Urzędzie Marszałkowskim w Poznaniu

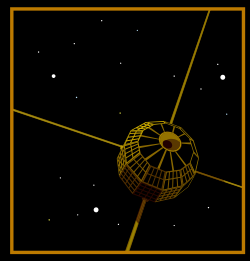


CELE – Polityka Bezpieczeństwa ZI

Celem wdrożonego systemu zarządzania bezpieczeństwem informacji jest osiągnięcie poziomu organizacyjnego i technicznego, który:

- będzie gwarantem pełnej ochrony danych Klientów oraz ciągłość procesu ich przetwarzania,
- zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych oraz jawnych,
- zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania,
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualne wykorzystanie na szkodę Spółki,
- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa Spółki, jej interesów oraz posiadanych i powierzonych jej informacji.

PBI w Urzędzie Marszałkowskim w Poznaniu



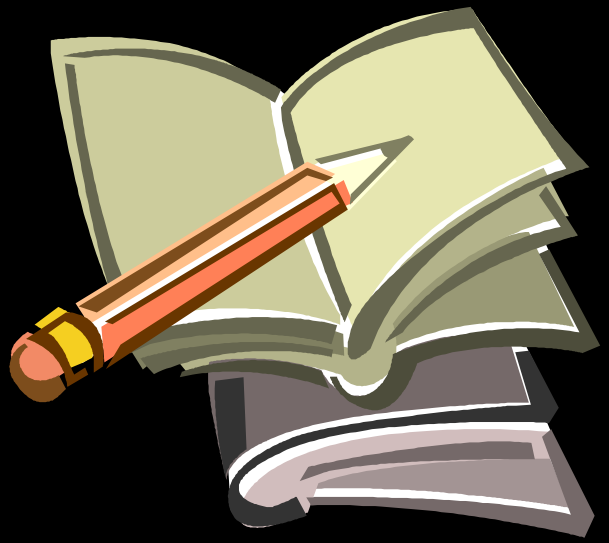
ZADANIA – Polityka Bezpieczeństwa ZI

Powyższe cele realizowane są poprzez:

- wyznaczenie osób odpowiedzialnych zapewniających optymalny podział i koordynację zadań związanych z zapewnieniem bezpieczeństwa informacji,
- wyznaczenie właścicieli dla kluczowych aktywów przetwarzających informację, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu bezpieczeństwa,
- przyjęcie za obowiązujące przez wszystkich pracowników polityk i procedur bezpieczeństwa obowiązujących w Spółce,
- określeniu zasad przetwarzania informacji, w tym stref w których może się ono odbywać,
- przegląd i aktualizację polityk i procedur postępowania dokonywaną przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty,
- ciągłe doskonalenie systemu zapewnia bezpieczeństwa informacji funkcjonującego w Spółce zgodnie z wymaganiami normy PN-ISO/IEC 27001:2007 i zaleceniami wszystkich zainteresowanych stron.

Prezes Zarządu

dr Marian Krupa

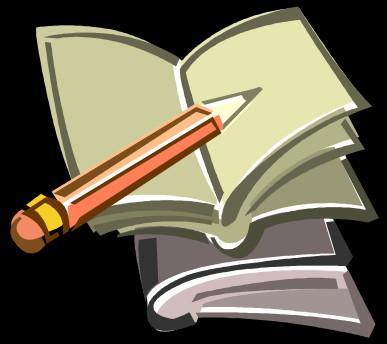


dr Marian Krupa

Metody doskonalenia SZBI

- Model procesu ZBI
- Audyt SZBI w firmie XYZ
- PDCA a SZBI (MIND MAPPING)

dr Marian Krupa



Projekt 1:

Model procesu ZBI w firmie XYZ

dr Marian Krupa

Opis zadania:

Na podstawie wymagań norm ISO z zakresu zapewnienia bezpieczeństwa informacji opracuj:

1. Model procesu ZBI (notacja BPMN)
2. Wykonaj jego parametryzacji (Cele / mierniki / zadania)

Metodyka:

1. Zdefiniuj cel i zakres projektu
2. Dobierz właściwe instrumenty (notacja) i narzędzia (oprogramowanie)
3. Zdefiniuj zadania – czynności obejmujące SZBI
4. Zdefiniuj osoby odpowiedzialne (uczestnicy)
5. **Opracuj schemat procesu zgodnie z przyjętą notacją (model procesu)**
6. Wykonaj parametryzację procesu

Modelowanie procesu ZBI:

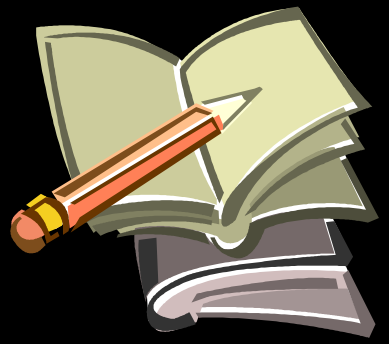
1. Model procesu ZBI (notacja BPMN)

Uczestnicy	PROCES ZBI w firmie XYZ

Modelowanie procesu ZBI:

2. Parametryzacja procesu ZBI (KCS)

KCS (czynniki oceny)	OCENA		Zadania
	AS-IS (obecna)	TO-BE (oczekiwana)	
			1. 2. 3.
			1. 2. 3.
			1. 2. 3.



Notacja BPMN:

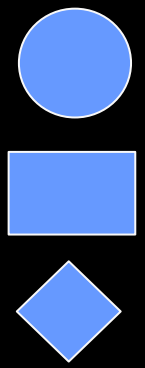
Wprowadzenie metodologiczne

dr Marian Krupa

Notacja BPMN

DEFINICJA

- Notacja **BPMN** powstała w ramach ***Business Process Management Initiative***, obecnie jest utrzymywana przez konsorcjum ***Object Management Group*** (http://www.omg.org)**.**
- W**ersja** standardu BPMN to **2.0** obejmuje 3 typy obiektów:
  - ✓ **zdarzenia**
  - ✓ **czynności**
  - ✓ **bramki**



+ przepływ sterowania

http://www.omg.org

Żeliński J., Modelowanie procesów biznesowych, dlaczego mają sens tylko metody formalne i uznane notacje., www.gigacon.org

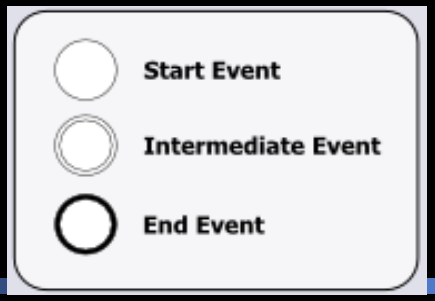
Notacja BPMN

Obiekty BPMN:

1. Zdarzenie *Event* – symbolizowane przez okrąg.

Zdarzenia mogą być początkowe (**START event**), pośrednie (**INTERMEDIATE event**) i końcowe (**END event**).

Występują następujące **typy zdarzeń**: nieokreślone, komunikat, sygnał, zasada, czas, anulowanie, zerwanie (terminacja), usterka, eskalacja, kompensacja, łącze wielokrotne.



Notacja BPMN

Obiekty BPMN:

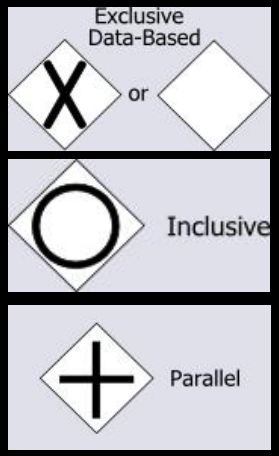
2. Czynność *Activity* – symbolizowane przez prostokąt z zaokrąglonymi rogami.

Czynność to „praca” wykonywana w procesie lub w przypadku diagramów choreografii (mapowania procesów) „współpraca” (powiązania wejścia-wyjścia) wykonywana pomiędzy procesami.

Notacja BPMN

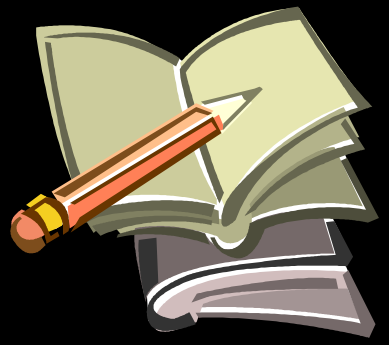
Obiekty BPMN:

3. Bramka logiczna *Gateway* – symbolizowaną przez romb. Bramki mogą rozdzielać lub łączyć **przepływy**.



- wykluczająca, oparta na danych (XOR)
  - *tylko jeden wybór*
- obejmująca (różne kombinacje wyników) / (OR)
  - *jeden wybór lub dowolnie więcej*
- równoległa (AND)
  - *wszystkie muszą być spełnione / realizowane*

http://www.omg.org



Model procesu ZBI:

Prace projektowe

dr Marian Krupa

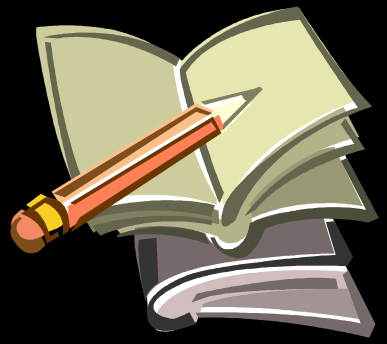
MODEL procesu ZBI (BPMN):

Zadania	Uczestnicy

KCS dla procesu ZBI:

Wskaźniki (KCS - Kluczowe Czynniki Sukcesu) i propozycje udoskonalenia procesu:

Nazwa + formula WSKAŹNIKA	WARTOŚĆ		Propozycja USPRAWNIEŃ
	obecna AS-IS	**oczekiwana** TO-BE	
Terminowość wykonania zlecenia - termin dostawy / termin zamówienia = różnica [dni]	średni czas opóźnień = 3 dni	średni czas opóźnień = 2 dni	1. Wdrożyć koncepcje "Time Management". 2. Workflow akceptacyjny WF (dok. elektroniczne). 3. Umowy ramowe.



Projekt 2:

Audyt SZBI w firmie XYZ

dr Marian Krupa

Kontrola vs Audyt:

KONTROLA	AUDYT
Wykrywa błędy formalne – głównie przepisy zewnętrzne	Wykrywa niezgodności dotyczących głównie norm wewnętrznych
Wymierza kary	Rekomenduje lepsze rozwiązania
Pełni funkcje nadzorcze / kontrolne	Pełni funkcje doradcze / usprawniające
CEL: Eliminacja błędów	CEL: Zapobieganie niezgodnościom
Ocena przeszłości	Refleksja dotycząca przyszłości
Nie uwzględnia doświadczeń innych. Każda kontrola jest oceniana indywidualnie	Odwołuje się do „najlepszych praktyk” / doświadczeń innych jednostek / firm / projektów
Kontroler posiada z mocy prawa uprawnienia operacyjne / decyzyjne	Audytor nie ma uprawnień decyzyjnych – przedstawia rekomendacje
OCENA	**OCENA + REKOMENDACJE**

Opis zadania:

1. Na podstawie dostarczonego raportu przeprowadź audyt SZBI w firmie XYZ.
2. CELEM audytu jest ocena i poprawa (doskonalenie) poziomu SZBI (Tabela 2).
3. Przedstaw 3 REKOMENDACJE (Tabela 3) udoskonalenia SZBI w firmie XYZ w oparciu o a) zdefiniowane priorytety oraz b) uzyskane oceny (Tabela 1).

Treść raportu do zadania 1:

Firma XYZ prowadzi działalność wydawniczą na terenie Polski.

W wyniku przeprowadzonej wizji lokalnej oraz wywiadu z kierownictwem oraz z pracownikami zebrano podstawowe informacje w zakresie funkcjonowania SZBI w badanej firmie.

Obejmuje ona następujące zapisy…

Lista pytań audytora w zakresie SBI – PRIORYTETY:

Lp.	Pytania	Priorytet [1-10]
1	Istnieje dokumentacja dotycząca systemu zabezpieczenia jednostki organizacyjnej i systemu informatycznego ze wskazaniem osób odpowiedzialnych	
2	Została opracowana analiza ryzyka oraz zostały wdrożone procedury zarządzania ryzykiem	
3	Istnieją zabezpieczenia fizyczne obejmujące budynki i serwerownie	
4	Powstał kompleksowy system zarządzania uprawnieniami	
5	Zakupiono profesjonalne zabezpieczania danych w systemach informatycznych	
6	Istnieje stały nadzór administratora nad funkcjonowaniem sieci lokalnej	

10 – 1
9 – 2
8 – 3
7 – 4
6 – 5

Lista pytań audytora w zakresie SBI – ocena + rekomendacje:

Lp.	Pytania	Ocena [0;1;3]	Wstępne rekomendacje
1	Istnieje dokumentacja dotycząca systemu zabezpieczenia jednostki organizacyjnej i systemu informatycznego ze wskazaniem osób odpowiedzialnych		
2	Została opracowana analiza ryzyka oraz zostały wdrożone procedury zarządzania ryzykiem		
3	Istnieją zabezpieczenia fizyczne obejmujące budynki i serwerownie		
4	Powstał kompleksowy system zarządzanie uprawnieniami		

Pełna zgodność = 3 pkt. *(utrzymać działania na obecnym poziomie)*

Częściowa zgodność =1 pkt. *(wymagane są działa usprawniające)*

Brak zgodności = 0 pkt. *(konieczność natychmiastowej eliminacji niezgodności)*

OCENA i rekomendacje SZBI:

Wartości [pkt]	Ocena	Wartość procentowa
0 - 10	*stan wysokiego zagrożenia*	**do 36%**
11-15	*stan średniego zagrożenia*	**37% - 52%**
16-20	*stan zagrożenia*	**53% - 69%**
21-29	*stan umiarkowanego zagrożenia*	**70% - 99%**
30	*brak uzasadnionego zagrożenia*	**100 %**

REKOMENDACJE udoskonalenia SZBI w firmie XYZ

1	
2	
3	

Projekt 3:

Zasoby informacyjne

(mind mapping)

dr Marian Krupa

Zasoby informacyjne

Na podstawie lektury artykułu pt. „ROZWÓJ KONCEPCJI INFORMACJI I WIEDZY JAKO ZASOBU ORGANIZACJI” zdefiniuj przy pomocy diagramu mapy (*mind mapping*) pojecie „zasoby informacyjne” w kontekście systemu Zarządzania Bezpieczeństwem Informacji.

Zasoby informacyjne

- **Mind mapping** (mapa myśli) – technika wizualizacji złożonych problemów uwzględniająca relacje przyczynowo-skutkowe.

- **MP** - innowacyjny sposób poszukiwania, porządkowania, i komunikowania dowolnych zagadnień, problemów, definicji.

- Ma na celu przyspieszyć pracę i dać lepszy efekt m.in. w zakresie zapamiętania i zrozumienia złożonych problemów.

Zasoby informacyjne

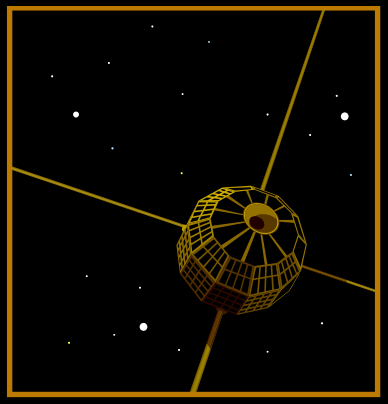
Mind mapping – zasady tworzenia mapy myśli:

- używamy obrazów i symboli – skróty i uproszczenia
- najważniejsze słowa / kategorie oznaczamy najsilniej (kolor)
- agregujemy zagadnienia w liczbie 5-7 kategorii / perspektyw
- jedna "odnoga" prowadzi tylko do jednego słowa albo rysunku
- używamy liter różnych wielkości i kroju
- używamy kolorów według swojej intuicji i uznania
- zamieszczamy na mapie nie tylko same informacje, ale i skojarzenia, pytania, problemy !!!
- dajemy się ponieść wyobraźni…

Doskonalenie SZBI

Zasoby informacyjne SZBI

PYTANIA?



- dr Marian Krupa