

"Audyt IT, a zarządzanie ryzykiem w tym obszarze "

**WYKŁADOWCA:
ANNA SŁODCZYK**

***Konferencja „BIN 2009”
WARSZAWA, 08-09-2009***

Agenda

- Po co audyt IT w obszarze zarządzania ryzykiem?
- Co sprawdzamy i wg jakich kryteriów?
- Modele zarządzania ryzykiem i szacowania ryzyka
- Podstawowe, a często mylone pojęcia i ich udział w prawidłowym przeprowadzeniu ww. audytu
- Plan postępowania z ryzykiem
- Przykłady „z życia wzięte”

Zarządzanie ryzykiem

Skoordynowane działania kierowania
i kontrolowania organizacji
z uwzględnieniem ryzyka

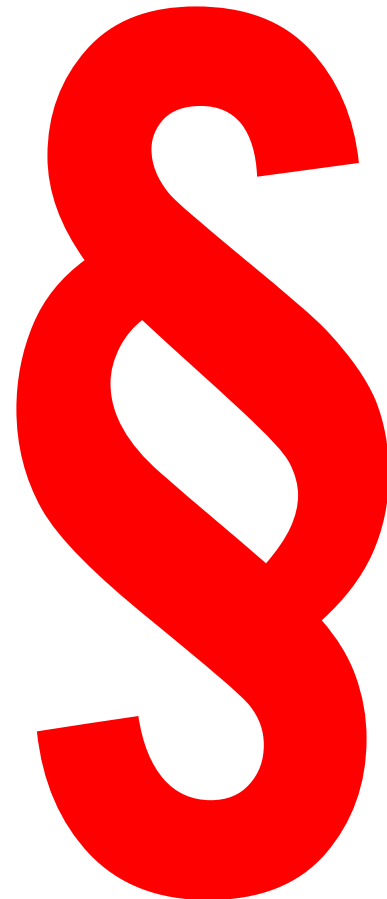
(ISO/IEC Guide 73)

Po co zarządzamy ryzykiem w obszarze IT?

- Aby na stałe i na bieżąco panować nad zmieniającą się sytuacją – monitoring obszaru IT i jego wpływu na całą organizację
- Aby stosować się do ustalonych kryteriów – wg ustaleń najwyższego kierownictwa lub wg wymagań normatywnych czy prawnych
- Aby monitorować wprowadzane świadomie zmiany w obszarze IT, pozostając w ramach ustalonych kryteriów – testowanie
- Aby nie zapominać o stosowaniu działań prewencyjnych, ekonomicznie uzasadnionych w organizacji
- Aby w miarę możliwości unikać ryzyk lub je właściwie transferować
- Aby wykorzystywać istniejące szanse dla firmy

Wybrane Ustawy dotyczące ochrony informacji:

- **O ochronie informacji niejawnych**
- **O ochronie danych osobowych**
- **O ochronie osób i mienia**
- **O rachunkowości**
- **Kodeks Spółek Handlowych**
- **Prawo bankowe**
- **Ustawa ubezpieczeniowa**



Normy dotyczące bezpieczeństwa informacji:

PN ISO/IEC 17799

„Praktyczne zasady zarządzania bezpieczeństwem informacji”

PN-ISO/IEC 27001

„System zarządzania bezpieczeństwem informacji - wymagania”

PN-I-13335-1

Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych

System zarządzania bezpieczeństwem informacji

Ta część całościowego systemu zarządzania, oparta na podejściu wynikającym z **ryzyka biznesowego**, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji

ISMS - information security management system

PN-I-07799-2

SZBI – system zarządzania bezpieczeństwem informacji

PN-ISO/IEC 27001

A co, jeśli nie spełnimy kryteriów, np. prawnych?

Karalność za brak przestrzegania

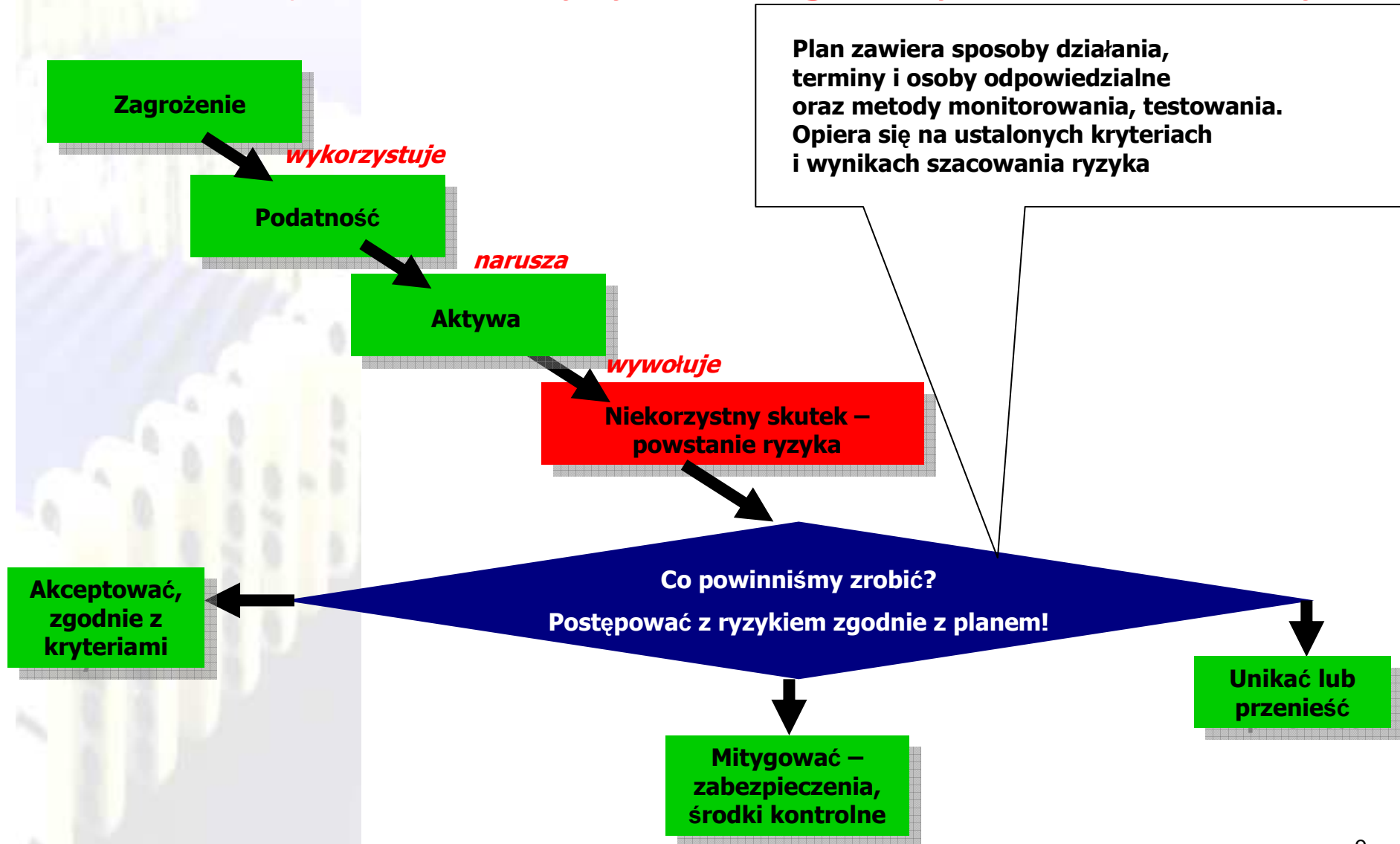
przepisów dotyczących danych osobowych:

grzywna

kara ograniczenia wolności

kara pozbawienia wolności od roku do lat trzech

Plan postępowania z ryzykiem – główny przedmiot audytu



Trzeba dobrze rozumieć podstawowe pojęcia, takie jak:

- podatność
- zagrożenie
- skutek
- prawdopodobieństwo
- kryteria
- ryzyko
- zarządzanie ryzykiem
- ciągłość działania
- akceptacja ryzyka

Atrybuty bezpieczeństwa informacji

- **poufność – jakie zagrożenia???**
- **Integralność - jakie zagrożenia???**
- **dostępność - jakie zagrożenia???**

Ale również.....

- **rozliczalność – jakie zagrożenia???**
- **autentyczność**
- **niezaprzeczalność**
- **niezawodność**

System informatyczny wspomagający zarządzanie ryzykiem powinien:

- wiązać ze sobą wszystkie elementy ryzyka
- badać oddziaływania konkretnego ryzyka na całą organizację
- monitorować proces zarządzania ryzykiem w układzie ciągłym
- alarmować w sytuacjach przekroczenia kryteriów
- testować wdrożenie środków kontrolnych i monitorować efekty tego wdrożenia
- umożliwiać szybkie znalezienie wpływu określonego zagrożenia na wszystkie elementy obszaru IT i całej firmy, czyli identyfikować wszystkie ryzyka
- uporządkować wymagania i dokumentację
- dać możliwość pracownikom uzupełniania opisu zauważonych ryzyk i zagrożeń w trybie ON-LINE
- ułatwić przeprowadzenie audytu w obszarze zarządzania ryzykiem

QUIZ DO PYTANIA:

„Kiedy, z jaką częstotliwością przeprowadza się szacowanie ryzyka?”

Dziękuję za uwagę

Anna Słodczyk,

Tel + 48 604 122 278

www.annaslodczyk.com

[Powołane w wykładzie normy można zakupić w www.pkn.pl](http://www.pkn.pl)

