DZIAŁ ZARZĄDZANIA
RYZYKIEM INFORMATYCZNYM

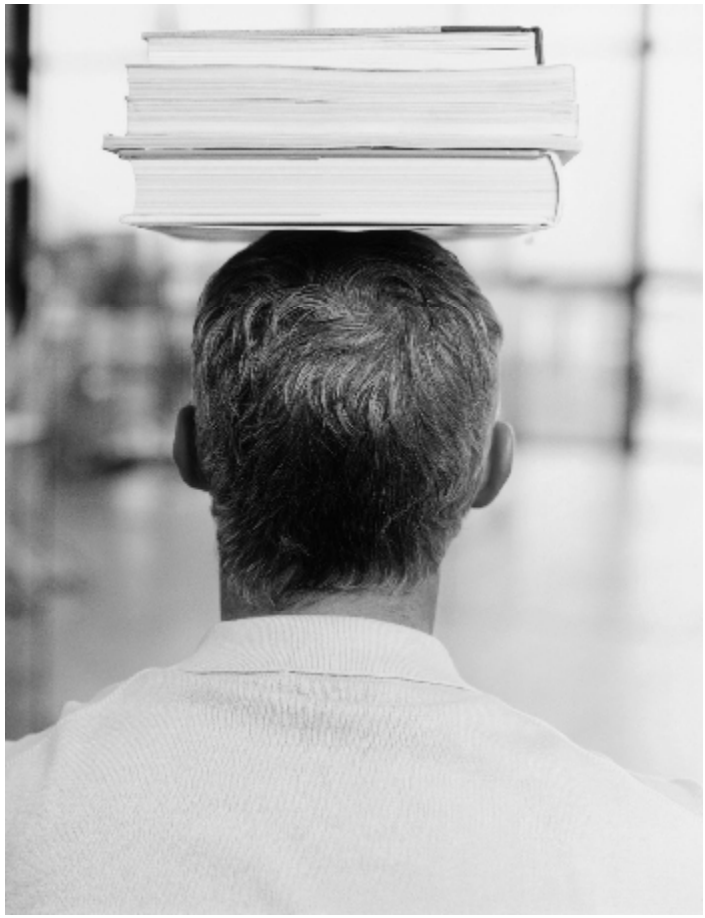
Analiza i zarządzanie ryzykiem systemów informatycznych

Wykład

Mirosław Ryba

Plan wykładu

- **Ryzyko vs. ryzyko systemów informatycznych**
- **Podejścia do analizy ryzyka systemów informatycznych**
- **Metody ilościowe – metoda Courtneya**
- **Metody ilościowe – metoda Fishera**
- **Metody jakościowe – MCSGRMF**
- **Metody jakościowe – NIST SP 800-30**
- **Standardy**
- **Metody oparte na rywalizacji**
- **Pytania i odpowiedzi**



Ryzyko vs. ryzyko systemów informatycznych

Pojęcia ryzyka

- **Ryzyko w ujęciu subiektywnym**

  Ryzyko jest pewną obiektywną prawidłowością cechującą świat realny, którą jednostka subiektywnie postrzega i interpretuje, i wyrażana jest poprzez niepewność wystąpienia określonych skutków stanu natury

- **Ryzyko w ujęciu psychologicznym**

  Ryzyko jest stanem umysłu człowieka, jeżeli stan umysłu się zmieni, to zmieni się również ryzyko. Ryzyko istnieje o tyle, o ile podmiot ma świadomość istnienia ryzyka

- **Ryzyko z perspektywy szacowania przyszłości**

  Ryzyko jest niepewnością przewidywania zdarzeń w przyszłości, wynikającą z niepełności i niedokładności danych statystycznych, na podstawie których dokonuje się szacowania przyszłości

Pojęcia ryzyka – cd.

- **Ryzyko w ujęciu projektowym**

  Ryzyko to skumulowany efekt prawdopodobieństwa niepewnych zdarzeń, które mogą korzystnie lub niekorzystnie wpływać na realizację projektu

- **Ryzyko w rozumieniu IIA (*ang. The Institute of Internal Auditors*)**

  Ryzyko jest niepewnością, co do możliwości wystąpienia zdarzenia mogącego mieć negatywny wpływ na osiągnięcie celów danej organizacji

- **Ryzyko w rozumieniu ISACA (*ang. Information Systems Audit and Control Association*)**

  Ryzyko jest możliwością wystąpienia zdarzenia, które będzie miało niepożądany wpływ na daną organizację i jej systemy informatyczne

Klasyfikacja ryzyka

- **Podział przedmiotowy:**
  - ryzyko subiektywne (przewidywania decydentów w organizacji)
  - ryzyko właściwe (na przykład wystąpienie jakiegoś zdarzenia losowego, czy też klęski żywiołowej)
  - ryzyko obiektywne (zdarzenia, których nie da się przewidzieć)
- **Podział rodzajowy:**
  - ryzyko stałe (występuje ciągle w całym systemie)
  - ryzyko zmienne (może ono występować okresowo)

Ryzyko systemów informatycznych

- **Ryzyko systemów informatycznych**

  Ryzyko systemów informatycznych to zagrożenie, iż technologia informatyczna stosowana w danej organizacji (niezależnie od jej rodzaju i skali działalności) :

  - nie spełnia wymogów biznesowych
  - nie zapewnia odpowiedniej integralności, bezpieczeństwa oraz dostępności danych
  - nie została odpowiednio wdrożona i nie działa zgodnie z założeniami

- **Ryzyko systemów informatycznych w ujęciu PN–I–13335–1:1999**

  Ryzyko systemów informatycznych jest zbiorczą miarą prawdopodobieństwa i wagi sytuacji, w której dane zagrożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie aktywów systemu, a zatem pośrednią lub bezpośrednią szkodę dla organizacji

Atrybuty bezpieczeństwa

- Atrybuty bezpieczeństwa informacji:
  - **poufność** (*ang. confidentiality*)
  - **integralność** (*ang. integrity*)
  - **dostępność** (*ang. availability*)

Atrybuty bezpieczeństwa – poufność

- **Poufność według standardu BS 7799 / ISO/IEC 17799**

  Poufność to zapewnienie, że informacja jest dostępna jedynie osobom upoważnionym

- **Podatność według ISO/IEC TR 13335–1 / PN-13335-1**

  Poufność to właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom

- **Poufność według ITSEC (*ang. Information Technology Security Evaluation Criteria*)**

  Poufność to ochrona przed nieautoryzowanym pozyskaniem informacji

Atrybuty bezpieczeństwa – integralność

- **Integralność według standardu BS 7799 / ISO/IEC 17799**

  Integralność jest zapewnieniem dokładności i kompletności informacji oraz metod jej przetwarzania

- **Integralność według ISO/IEC TR 13335–1 / PN-13335-1**

  Integralność danych to właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany

  Integralność systemu to właściwość zapewniająca, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej, celowej lub przypadkowej manipulacji

- **Integralność według ITSEC (*ang. Information Technology Security Evaluation Criteria*)**

  Integralność to ochrona przed nieautoryzowaną modyfikacją informacji

Atrybuty bezpieczeństwa – dostępność

- **Dostępność według BS 7799 oraz ISO/IEC 17799**

  Dostępność to zapewnienie, że osoby upoważnione mają możliwość wykorzystania informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne

- **Dostępność według ISO 7498–2**

  Dostępność to właściwość bycia możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot

- **Dostępność według wytycznych rządu kanadyjskiego**

  Dostępność to możliwość dostępu do systemów, programów, usług i informacji dla uprawnionych użytkowników, kiedy zachodzi taka konieczność i bez zbędnej zwłoki

- **Dostępność według ITSEC**

  Dostępność to ochrona przed nieautoryzowaną odmową udostępnienia informacji lub zasobu

Ryzyko systemów informatycznych z perspektywy audytu.

- **Ryzyko audytu R_A (*ang. Audit Risk*)**

$$R_A = R_W * R_K * R_D$$

- **Ryzyko wewnętrzne R_W (*ang. Inherent Risk*)**

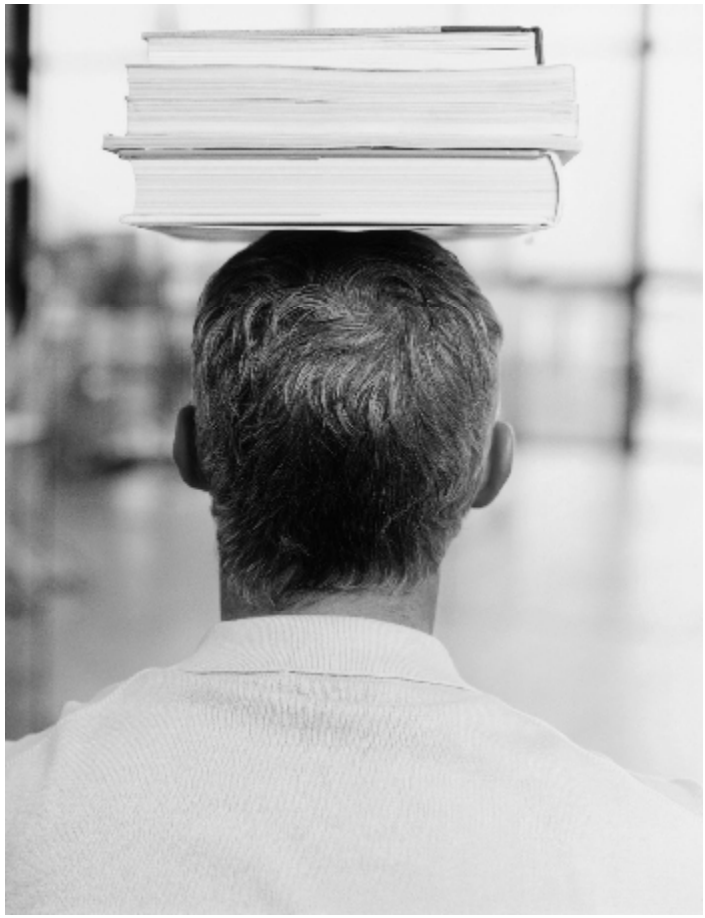
  Ryzyko wewnętrzne jest to podatność na wystąpienie istotnego błędu, który sam lub w połączeniu z innymi błędami, przy braku odpowiednich kontroli wewnętrznych, będzie miał istotny wpływ na analizowany obszar

- **Ryzyko kontroli R_K (*ang. Control Risk*)**

  Ryzyko kontroli jest to ryzyko polegające na braku możliwości uniknięcia lub wykrycia i skorygowania błędu we właściwym czasie przez system kontroli wewnętrznej

- **Ryzyko detekcji R_D (*ang. Detection Risk*)**

  Ryzyko detekcji jest ryzykiem polegającym na tym, iż analityczne procedury audytowe nie ujawnią błędu, który sam lub w połączeniu z innymi błędami będzie miał istotny wpływ na analizowany obszar



Podejścia do analizy ryzyka systemów informatycznych

Metody ilościowe

- **Metody ilościowe** (*ang.* ***quantitative***) – to metody, w ramach których próbuje się skwantyfikować i wyrazić liczbowo, na podstawie danych statystycznych, wielkość potencjalnych strat, prawdopodobieństwo ich wystąpienia, a w efekcie poziom występujących ryzyk

- Przykłady metod ilościowych:
  - metoda Courtneya
  - metoda Fishera
  - metoda Parkera

Metody jakościowe

- **Metody jakościowe** (*ang.* ***qualitative***) – to metody bazujące na ocenie zagrożeń, poziomu ryzyka i płynących z tego ewentualnych strat, na podstawie znajomości analizowanych zagadnień, doświadczenia i intuicji osoby oceniającej

- Przykłady metod jakościowych:
  - The Microsoft Corporate Security Group Risk Management Framework
  - NIST SP 800-30
  - Simple Technique for Illustrating Risk – STIR
  - Facilitated Risk Analysis Process – FRAP

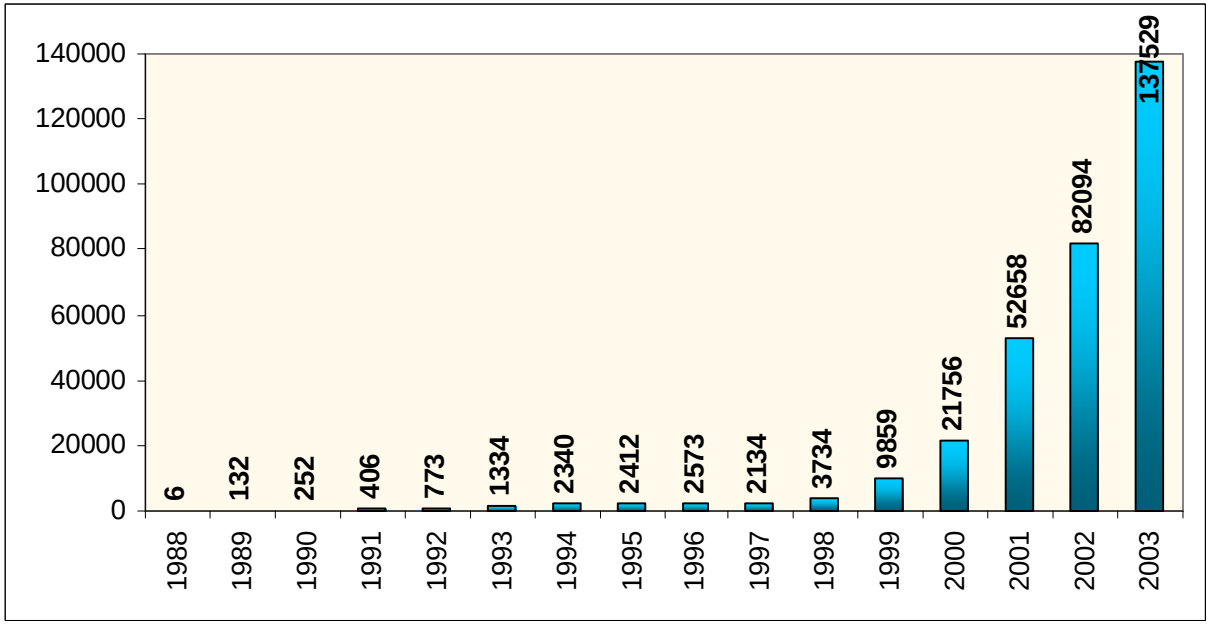
Standardy

- Wprowadzenie standardów bezpieczeństwa ma na celu określenie i upowszechnienie wskazówek i rekomendacji dotyczących zarządzania ryzykiem oraz mechanizmów kontrolnych stanowiących najlepsze praktyki.

- Przykłady standardów bezpieczeństwa:
  - norma BS 7799 / ISO 17799
  - norma ISO/IEC TR 13335 / PN–I–13335–1
  - Standard Australijski – AS/NZS 4360:1999
  - Wytyczne Rządu Kanadyjskiego – metoda Threat and Risk Assessment – TRA

Metody oparte na rywalizacji

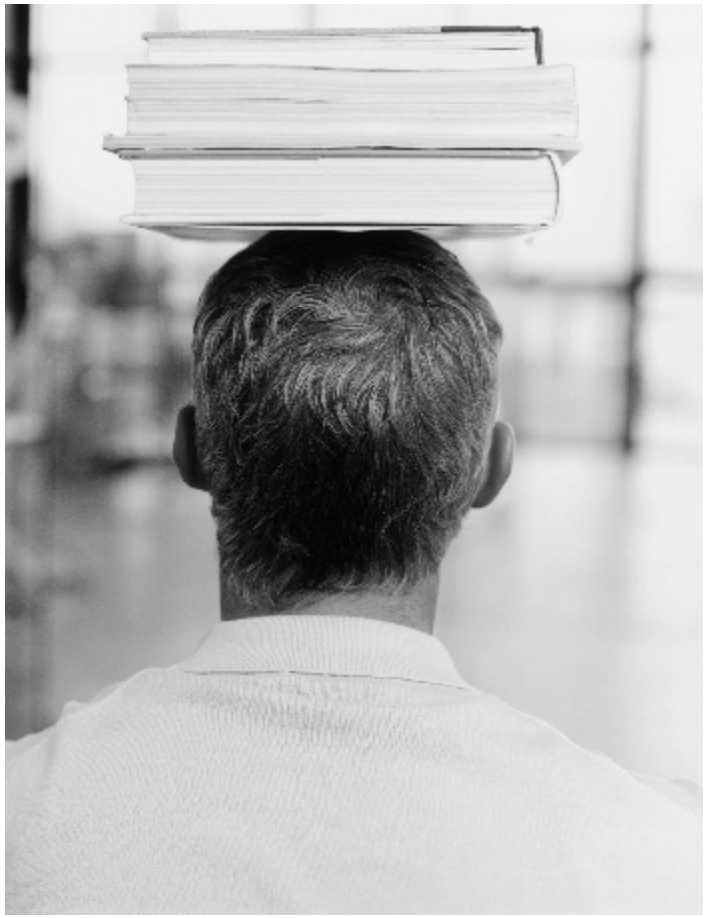
- Koncepcja metod opartych na rywalizacji (*ang. competitive methods*) jest próbą uzależnienia wynikowej wielkości ryzyka systemów informatycznych od zachowań i predyspozycji ludzkich



Ilość incydentów zgłoszonych do CERT/CC* w latach 1988 – 2003

Incydent to grupa niepożądanych zdarzeń posiadających wspólną przyczynę

**Computer Emergency Response Team Coordination Center*



Metody ilościowe – metoda Courtney

Sposób wyznaczania ryzyka wg. Courtney'a

- **Koncepcja ryzyka wg. Courtney'a**

$$R = P \cdot C$$

  - P – prawdopodobieństwo wystąpienia określoną ilość razy z ciągu roku, zdarzenia powodującego stratę dla organizacji
  - C – strata dla danej organizacji będąca wynikiem pojedynczego wystąpienia zdarzenia powodującego stratę

- **ALE (*ang. Annual Loss Exposure*)** – oczekiwana roczna strata – wartość przewidywanych średnich rocznych strat wynikłych z wykorzystania podatności danego systemu informatycznego

$$ALE = \frac{10^{f+i-3}}{3}$$

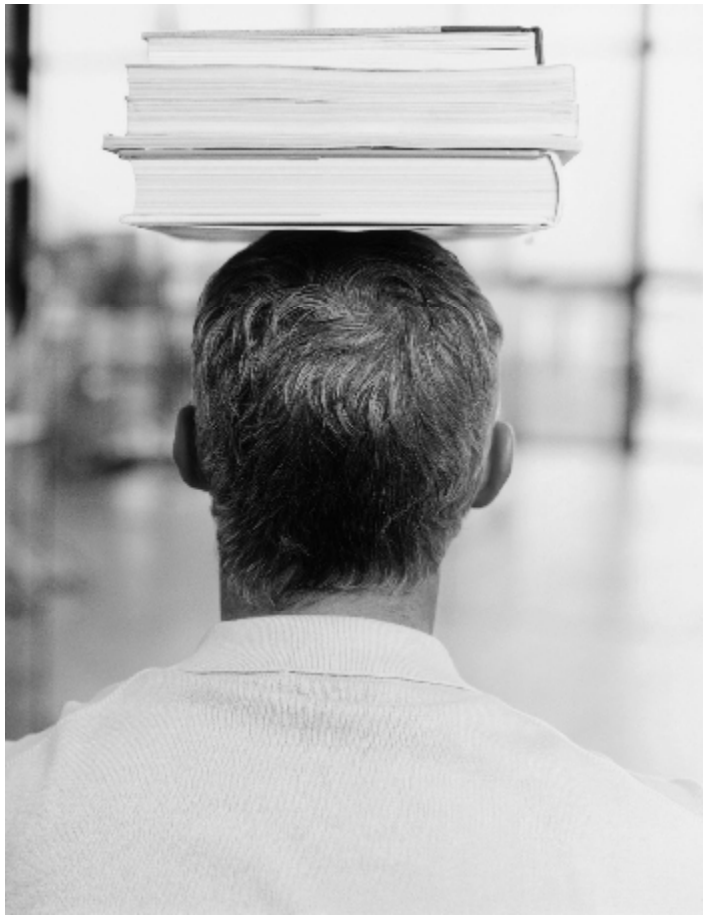
  - f – indeks określający szacowaną częstotliwość wystąpienia zdarzenia powodującego stratę
  - i – indeks określający szacowaną wysokość straty spowodowanej wystąpieniem zdarzenia powodującego tą stratę

Sposób wyznaczania ryzyka wg. Courtney'a – cd.

Prawdopodobieństwo wystąpienia zdarzenia	Wartość parametru *f*	Rząd wielkości szacowanej straty	Wartość parametru *i*
raz na 300 lat	1	10 PLN	1
raz na 30 lat	2	100 PLN	2
raz na 3 lata	3	1 000 PLN	3
raz na 100 dni	4	10 000 PLN	4
raz na 10 dni	5	100 000 PLN	5
raz na dzień	6	1 000 000 PLN	6
10 razy dziennie	7	10 000 000 PLN	7
100 razy dziennie	8	100 000 000 PLN	8
1000 razy dziennie	9	1 000 000 000 PLN	9

Grupy zagrożeń wg. Courtneya

- Przypadkowe ujawnienie danych
- Przypadkowa modyfikacja danych
- Przypadkowe usunięcie danych
- Celowe ujawnienie danych
- Celowa modyfikacja danych
- Celowe usunięcie danych



Metody ilościowe – metoda Fishera

Metoda Fishera

- Metoda Fishera [1984] jest rozwinięciem metody Courtney'a w kompletną metodykę projektowania rozwiązań bezpieczeństwa systemów informatycznych
- W celu prawidłowego zastosowania metody Fishera wymagane jest, aby w danej organizacji była wprowadzona polityki bezpieczeństwa
- Proces zarządzania ryzykiem systemów informatycznych według Fishera:
  - Faza 1 – Zebranie informacji
  - Faza 2 – Identyfikacja zagrożeń
  - Faza 3 – Ocena ryzyka
  - Faza 4 – Projektowanie mechanizmów kontrolnych
  - Faza 5 – Ocena ekonomicznej opłacalności mechanizmów

Faza 1 – Zebranie informacji

- Zadania
  - identyfikacja i klasyfikacji zasobów systemów informatycznych
  - zebranie informacji o zasobach systemów informatycznych podlegających dalszej analizie

Faza 2 – Identyfikacja zagrożeń

- Proces mapowania zagrożeń (6 grup zagrożeń Courtneya) na 11 punktów kontrolnych Fishera
- Punkty kontrolne Fishera (*ang. data exposure control points*):
  - *Pozyskiwanie danych* – manualne tworzenie i transport danych
  - *Przekazywanie danych* – manualne wprowadzanie danych źródłowych do systemu informatycznego
  - *Zmiana formy danych* – konwersja danych źródłowych na maszynowe
  - *Transport danych (wejściowych)* – przesyłanie danych maszynowych
  - *Odbiór danych* – odbiór lub przechowywanie danych w systemie informatycznym
  - *Przetwarzanie danych* – wykonywanie programu (obliczenia lub operacje na danych)
  - *Przygotowywanie danych (wyjściowych)* – przeniesienie danych na taśmy, dyski, wydruki
  - *Migracja danych* – migracja danych poza systemem informatycznym
  - *Transport danych (wyjściowych)* – transmisja danych (elektroniczna lub manualna) do użytkowników końcowych
  - *Użytkowanie danych* – wykorzystywanie i przetwarzanie danych przez użytkownika
  - *Usuwanie danych* – usunięcie danych z systemu informatycznego po ich wykorzystaniu

Faza 3 – Ocena Ryzyka

- Wyznaczenie poziomu ryzyka z wykorzystaniem aparatu Courtneya

$$R = P \cdot C$$

  - P – prawdopodobieństwo wystąpienia określoną ilość razy z ciągu roku, zdarzenia powodującego stratę dla organizacji
  - C – strata dla danej organizacji będąca wynikiem pojedynczego wystąpienia zdarzenia powodującego stratę

Faza 4 – Projektowanie mechanizmów kontrolnych

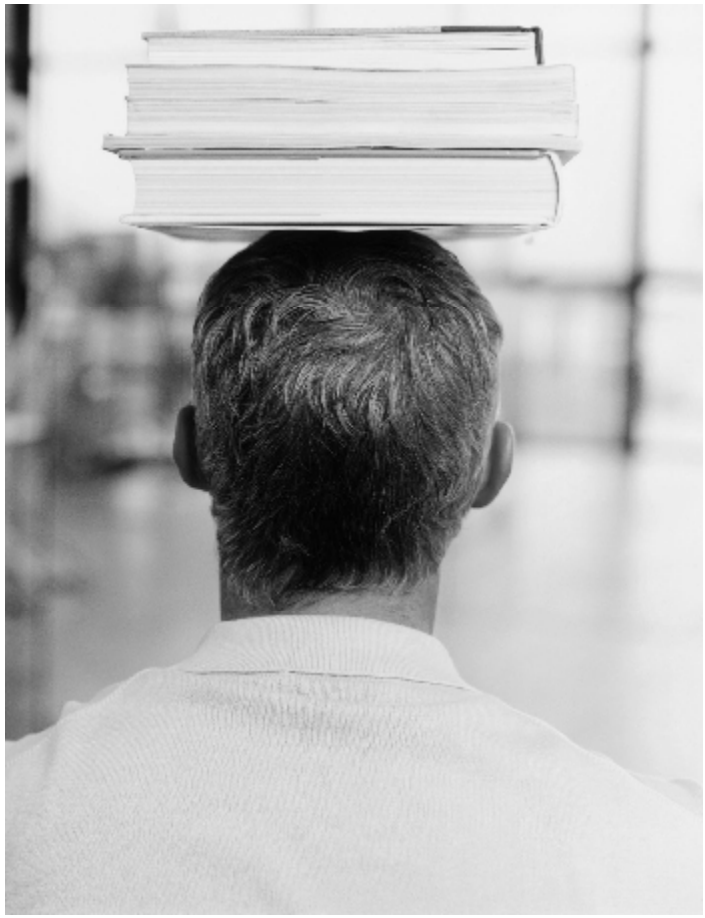
- Grupy mechanizmów kontrolnych:
  - **prewencyjne** (*ang. preventive*)
  - **detencyjne** (*ang. detective*)
  - **korekcyjne** (*ang. corrective*)
- W wyniku Fazy 4, do każdego zidentyfikowanego ryzyka powinien zostać dobrany odpowiedni mechanizm kontrolny
- Poziom dobieranych zabezpieczeń powinien być adekwatnych do potrzeb – do poziomu ryzyka oraz wartości zasobów

Faza 5 – Ocena ekonomicznej opłacalności mechanizmów

- Urealnienie biznesowe zidentyfikowanych mechanizmów z wykorzystaniem wskaźnika ROI (*ang. Return on Investment*)

$$ROI = \frac{\text{zysk operacyjny w danym okresie}}{\text{wartość zainwestowanego kapitału}}$$

- Wyznaczona wielkość ryzyka dla poszczególnych mechanizmów kontrolnych interpretowana jest jako zysk operacyjny
- Szacowany koszt mechanizmu kontrolnego traktowany jest jako wartość inwestowanego kapitału
- Kadra zarządzająca podejmuje decyzję, które mechanizmy kontrolne wdrożyć uwzględniając:
  - maksymalny akceptowalny poziom ryzyka
  - minimalny akceptowalny poziom ROI

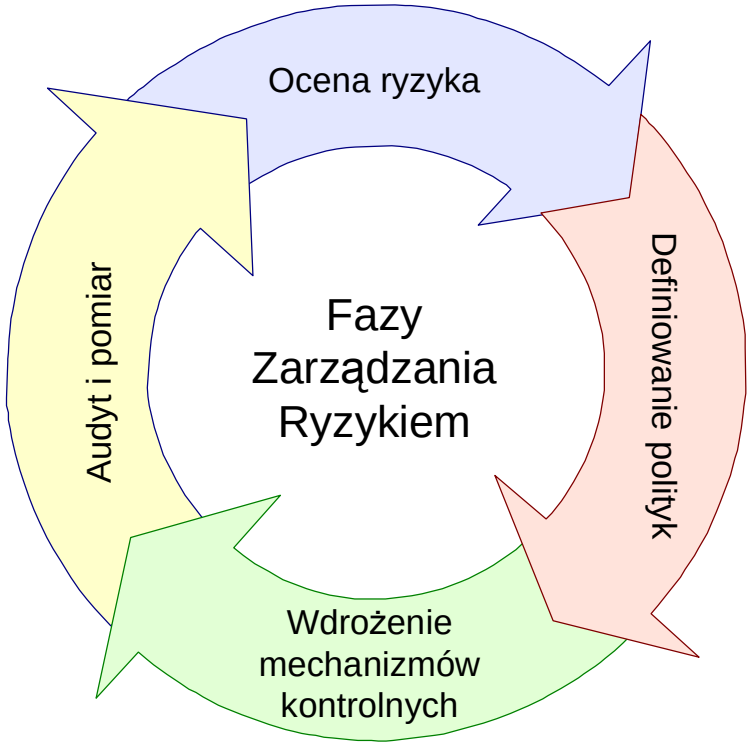


Metody jakościowe – metodyka Microsoftu

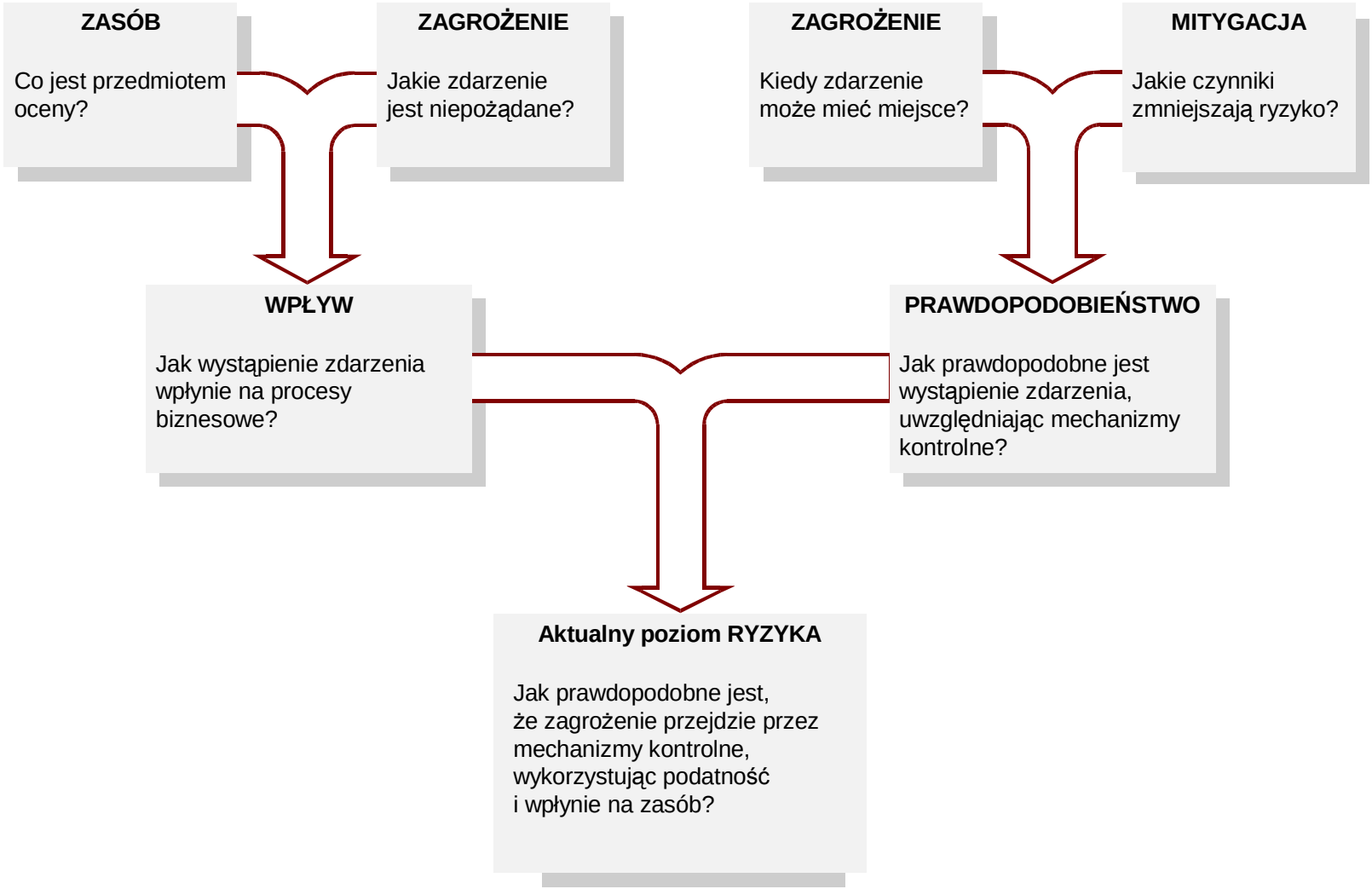
The Microsoft Corporate Security Group Risk Management Framework

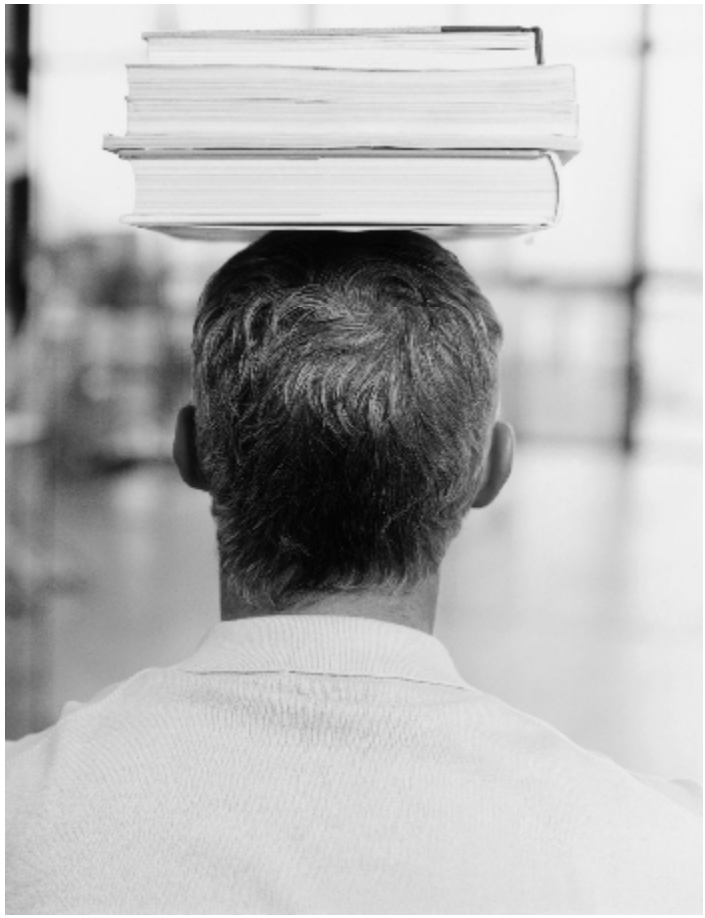
MCSGRMF – Etapy procesu

- Ocena ryzyka
- Definiowanie polityk
- Wdrożenie mechanizmów kontrolnych
  - ludzie, proces i technologia
  - analiza nakładów i wyników (*ang. cost/benefit analysis*)
- Audyt i pomiar
  - monitorowanie, audyt, pomiar i kontrola środowiska z perspektywy efektywności rozwiązań



MCSGRMF – Ocena ryzyka





Metody jakościowe – NIST SP 800-30

NIST SP 800–30 – Koncepcja metodyki

- Metodyka opracowana przez **National Institute of Standards and Technology**
- Special Publication 800–30 – **Risk Management Guide for Information Technology Systems**
- Metodyka definiuje proces zarządzania ryzykiem systemów informatycznych w odniesieniu do całego cyklu życia systemu SDLC (*ang. System Development Life Cycle*)
- Etapy procesu zarządzania ryzykiem systemów informatycznych wg NIST SP 800–30:
  - ocena ryzyka (9 kroków)
  - ograniczanie ryzyka
  - monitorowanie i reagowanie na zmiany

Faza I – Ocena ryzyka

- (1) Wybór systemów objętych oceną, określenie zakresu oceny oraz zgromadzenie informacji dotyczących wybranych systemów
- (2) Identyfikacja i stworzenie kompletnej listy zagrożeń odnoszących się do systemów informatycznych objętych przeprowadzaną oceną ryzyka
- (3) Identyfikacja i stworzenie kompletnej listy podatności w objętych oceną systemach informatycznych, które mogą zostać wykorzystane przez zidentyfikowane uprzednio zagrożenia
- (4) Analiza zaimplementowanych bądź planowanych mechanizmów kontrolnych i zabezpieczających mających na celu minimalizację istotności potencjalnych zidentyfikowanych zagrożeń bądź ich całkowitą eliminację
- (5) Określenie prawdopodobieństw wykorzystania podatności przez zidentyfikowane źródła zagrożeń. Prawdopodobieństwa te powinny być określone w trzystopniowej skali jako:
  - wysokie (1,0)
  - średnie (0,5)
  - niskie (0,1)

Faza I – Ocena ryzyka – cd.

- (6) Analiza i określenie wpływu na system, dane i organizację, faktu wykorzystania podatności systemu informatycznego (obniżenia integralności, dostępności i poufności) – wielkość wpływu określona jest w trzystopniowej skali jako:
  - wysoki (100)
  - średni (50)
  - niski (10)
- (7) Wyznaczenie za pomocą macierzy „poziomu ryzyka” (*ang. Risk – Level Matrix*), całkowitego ryzyka dla zidentyfikowanych zagrożeń. Na podstawie macierzy określany jest poziom całkowitego ryzyka dla każdego ze zidentyfikowanych zagrożeń jako:
  - wysoki – dla iloczynu z przedziału (50 , 100]
  - średni – dla iloczynu z przedziału (10 , 50]
  - niski – dla iloczynu z przedziału [1 , 10]

	niski (10)	średni (50)	wysoki (100)
wysoki (1,0)	**Niski** 10 x 1,0 = 10	**Średni** 50 x 1,0 = 50	**Wysoki** 100 x 1,0 = 100
średni (0,5)	**Niski** 10 x 0,5 = 5	**Średni** 50 x 0,5 = 25	**Średni** 100 x 0,5 = 50
niski (0,1)	**Niski** 10 x 0,1 = 1	**Niski** 50 x 0,1 = 5	**Niski** 100 x 0,1 = 10

Faza I – Ocena ryzyka – cd.

- (8) Opracowanie z uwzględnieniem istniejących ograniczeń technologicznych, organizacyjnych i finansowych, rekomendacji dla mechanizmów kontrolnych i zabezpieczających oraz innych rozwiązań mających na celu minimalizację ryzyka systemów informatycznych do poziomu akceptowalnego przez organizację bądź jego całkowitą eliminację

- (9) Przygotowanie dokumentacji wyników przeprowadzonej oceny ryzyka systemów informatycznych w postaci oficjalnego raportu, którego odbiorcami jest kadra zarządzająca

Faza II – Ograniczenie ryzyka

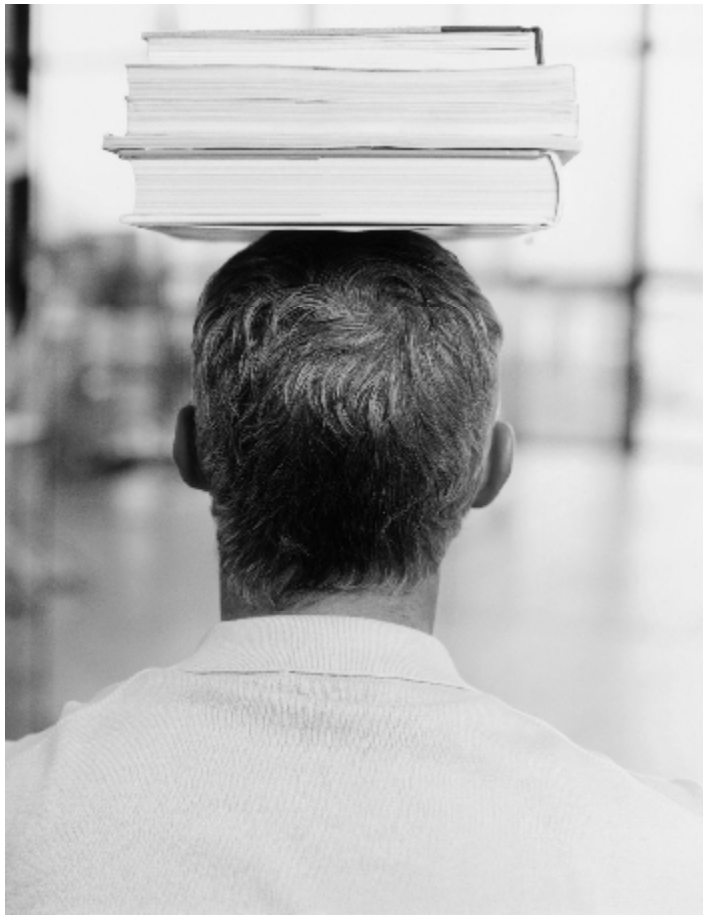
- Priorytetyzacja, ocena i implementacja mechanizmów kontrolnych i zabezpieczających zarekomendowanych w ramach procesu oceny ryzyka (Faza I)
- Mechanizmy kontrolne i zabezpieczające definiowane są w podziale na mechanizmy:
  - **wspomagające** (*ang. support controls*) – mechanizmy podstawowe, wykorzystywane przez inne mechanizmy (np. jednoznaczna identyfikacja użytkowników, zarządzanie kluczami publicznymi)
  - **prewencyjne** (*ang. prevent controls*) – mające za zadanie zapobieganie występowaniu incydentów naruszających bezpieczeństwo
  - **detekcyjno–naprawcze** (*ang. detect and recover controls*) – wykrywające zaistniałe incydenty i minimalizujące ich skutki
- **Ryzyko szczątkowe** (*ang. residual risk*) – ryzyko pozostałe po implementacji nowych lub rozszerzeniu istniejących mechanizmów kontrolnych i zabezpieczających

Faza II – Ograniczenie ryzyka – postępowanie z ryzykiem

- **Przejęcie ryzyka** (*ang. Risk Assumption*) – akceptacja potencjalnego ryzyka i kontynuacja operacyjnego wykorzystania systemu IT lub implementacja mechanizmów kontrolnych obniżających poziom ryzyka do akceptowalnego poziomu
- **Unikanie ryzyka** (*ang. Risk Avoidance*) – unikanie ryzyka poprzez eliminację jego przyczyn i/lub konsekwencji (np. ograniczenie funkcjonalności lub wyłączenie systemu w przypadku rozpoznania symptomów – niedopuszczenie do wystąpienia straty)
- **Ograniczanie ryzyka** (*ang. Risk Limitation*) – ograniczenie ryzyka poprzez implementację mechanizmów kontrolnych ograniczających wpływ zagrożeń wykorzystujących podatności
- **Planowanie ryzyka** (*ang. Risk Planning*) zarządzanie ryzykiem poprzez stworzenie planu ograniczanie ryzyka uwzględniającego priorytetyzację, implementację i utrzymanie zabezpieczeń i mechanizmów kontrolnych
- **Poznanie i akceptacja ryzyka** (*ang. Research and Acknowledgment*) – obniżenie ryzyka straty poprzez poznanie występujących podatności oraz opracowanie mechanizmów kontrolnych ograniczających dane podatności
- **Przeniesienie ryzyka** (*ang. Risk Transference*) – przeniesienie ryzyka poprzez wykorzystanie źródeł kompensacji ewentualnych strat (np. wykupienie ubezpieczenia)

Faza III – Monitorowanie i reagowanie na zmiany

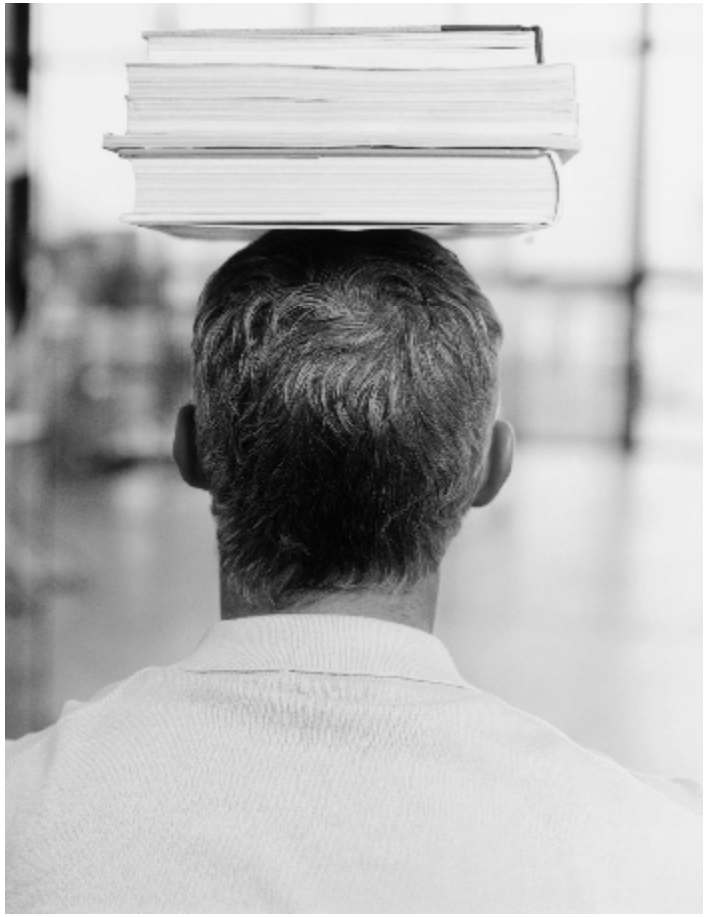
- Faza wynika ze zmienności środowiska teleinformatycznego mogącej prowadzić do:
  - powstawania nowych ryzyk
  - ponownego wystąpienia ryzyka, które zostało uprzednio ograniczone
- Pożądane cechy procesu:
  - zaangażowanie wyższej kadry zarządzającej
  - pełne wsparcie działu IT
  - wiedza i doświadczenie członków zespołu dokonującego analizy pojawiających się zagrożeń i ryzyk
  - świadomość pracowników
  - ciągła ocena poziomu ryzyka



Standardy

Wybrane standardy związane z ryzykiem systemów informatycznych

- **W myśl normy PN–I–13335–1 warunkiem uznania systemu informatycznego za bezpieczny jest spełnienie następujących atrybutów bezpieczeństwa:**
  - **poufności**, co oznacza ochronę przed ujawnieniem informacji nieuprawnionemu odbiorcy
  - **integralności**, co oznacza ochronę przed modyfikacją lub zniekształceniem aktywów informacyjnych przez osobę nieuprawnioną
  - **dostępności**, co oznacza gwarancję uprawnionego dostępu do informacji przy zachowaniu określonych rygorów czasowych
  - **rozliczalności**, co oznacza określenie i weryfikowanie odpowiedzialności za działania, usługi i funkcje realizowane za pośrednictwem systemu informacyjnego
  - **autentyczności**, co oznacza weryfikację tożsamości podmiotów lub prawdziwość aktywów systemu informacyjnego
  - **niezawodności**, co oznacza gwarancję odpowiedniego zachowania się systemu informacyjnego i otrzymanych wyników



Metody oparte na rywalizacji

Koncepcja Marcello

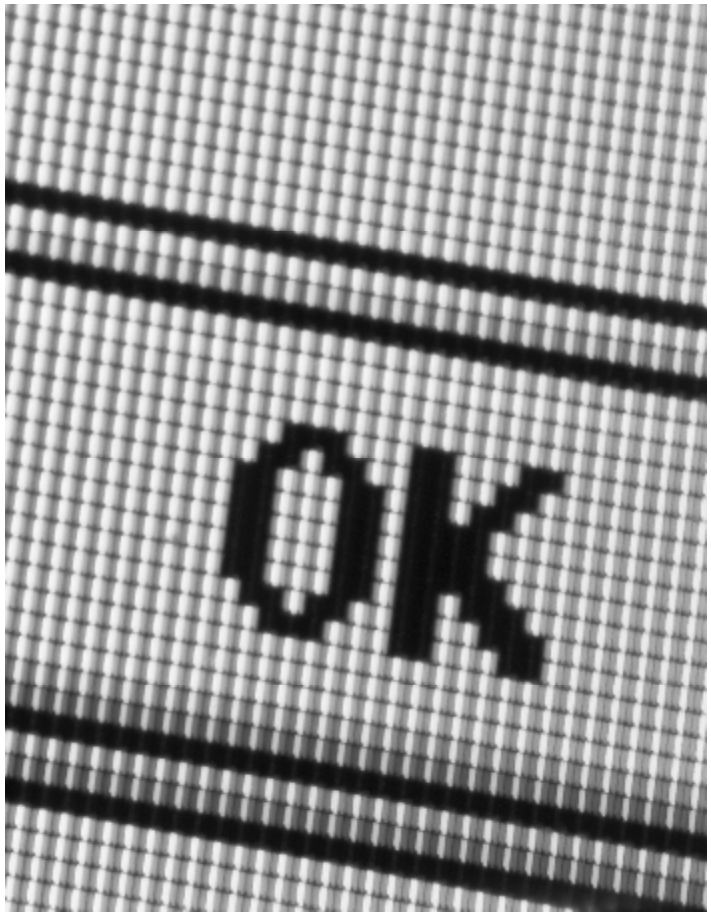
- **Formuła Marcello:**

$$R = q^2 \cdot \Psi \cdot \frac{1}{t^2} \cdot F$$

  - q – poziom wiedzy atakującego o atakowanym systemie
  - Ψ – stosunek skłonności do ryzyka strony broniącej do strony atakującej
  - $\frac{1}{t}$ – poziom nieznajomości systemu przez atakującego
  - F – poziom przekonania o sukcesie strony atakującej

Metodyka OPSEC

- **Metodyka Operations Security – OPSEC**, opublikowana została w USA w postaci dyrektywy National Security Decision Directive NSDD 298 z dnia 22 stycznia 1988
- **Proces OPSEC**, prowadzący do oszacowania poziomu ryzyka, powinien przebiegać według następującego schematu:
  - identyfikacja zasobów mogących być potencjalnym celem stron atakujących
  - analiza zagrożeń – identyfikacja stron atakujących, celów ich działań, intencji, wiedzy i możliwości
  - analiza podatności – badanie czynników, jakie mogą doprowadzić do przełamania zabezpieczeń systemu informatycznego poprzez wykorzystanie jego słabości
  - oszacowanie ryzyka – wycena efektów potencjalnego wykorzystania podatności systemu oraz przeprowadzenie analizy nakładów i wyników (*ang. cost–benefit analysis*) możliwych działań naprawczych
  - identyfikacja i wdrożenie stosownych zabezpieczeń



Pytania i odpowiedzi