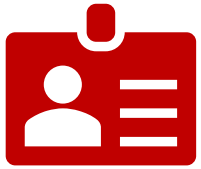
IT Security Trends

Warszawa | 18 września 2019

SZACOWANIE RYZYKA dla cyberbezpieczeństwa

dr Łukasz Kister

o sobie



dr Łukasz Kister

- ☑ 19 lat w bezpieczeństwie
- ☑ biegły sądowy – zarządzanie bezpieczeństwem informacji
- ☑ audytor wiodący ISO 27001
- ☑ audytor wiodący ISO 22301
- ☑ risk manager ISO 31000 / 27005
- ☑ …

> ***Jeżeli potrafisz to zmierzyć,***
> ***to potrafisz tym zarządzać!***

Edwards Deming

o czym będziemy dyskutować?

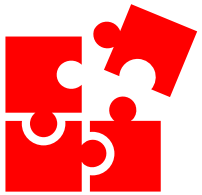
- ☑ szacowanie ryzyka – czym jest, a czym nie jest?
- ☑ kontekst Usługi Kluczowej – fundament szacowania ryzyka!
- ☑ analiza wpływu [biznesowego] – czyli szacujemy ryzyka tylko dla czegoś co ma znaczenie dla świadczenia Usługi Kluczowej!
- ☑ modele metodologiczne szacowania ryzyka dla cyberbezpieczeństwa – zalety i wady.

cyberbezpieczeństwo

Zdolność organizacji do normalnego funkcjonowania w otaczającym środowisku cybernetycznym:

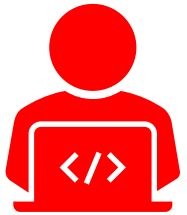
geopolityka

prawo



współzależność

uzależnienie



człowiek

„cyberbezpieczeństwo”

Odporność systemów informacyjnych na działania naruszające:

- ☑ **poufność**
- ☑ **integralność**
- ☑ **dostępność**
- ☑ **autentyczność**

przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

wymagania prawa

ustawa o krajowym systemie cyberbezpieczeństwa
(Dz.U. 2018 poz. 1560)

☑ prowadzenie systematycznego **szacowania ryzyka wystąpienia incydentu** oraz zarządzanie tym ryzykiem
(art. 8 pkt 1)

rozporządzenie w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
(Dz.U. 2018 poz. 2080)

☑ **szacowania ryzyka dla obiektów infrastruktury**
(§ 2 pkt 2 lit. b)

wymagania prawa

rozporządzenie w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo

(Dz.U. 2018 poz. 1780)

- ☑ **posiadać i utrzymywać w aktualności system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN-EN ISO/IEC 27001**
  (§ 1 ust. 1 pkt 1)
- ☑ **zapewnić ciągłość działania usłudze reagowania na incydenty, zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301**
  (§ 1 ust. 1 pkt 2)

definicje ustawowe

ustawa o krajowym systemie cyberbezpieczeństwa
(Dz.U. 2018 poz. 1560)

- ☑ **ryzyko – kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji**
  (art. 2 pkt 12)
- ☑ **szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka**
  (art. 2 pkt 13)
- ☑ **incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo**
  (art. 2 pkt 5)

definicje normatywne

Polska Norma PN-ISO/IEC 27005
Technika Informatyczna. Techniki bezpieczeństwa.
Zarządzanie ryzykiem w bezpieczeństwie informacji.
(2014)

- ☑ **ryzyko – wpływ niepewności na cele**
- ☑ **szacowanie ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka**
- ☑ **analiza ryzyka – proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka**
- ☑ **ocena ryzyka – proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane**

kontekst Usługi Kluczowej

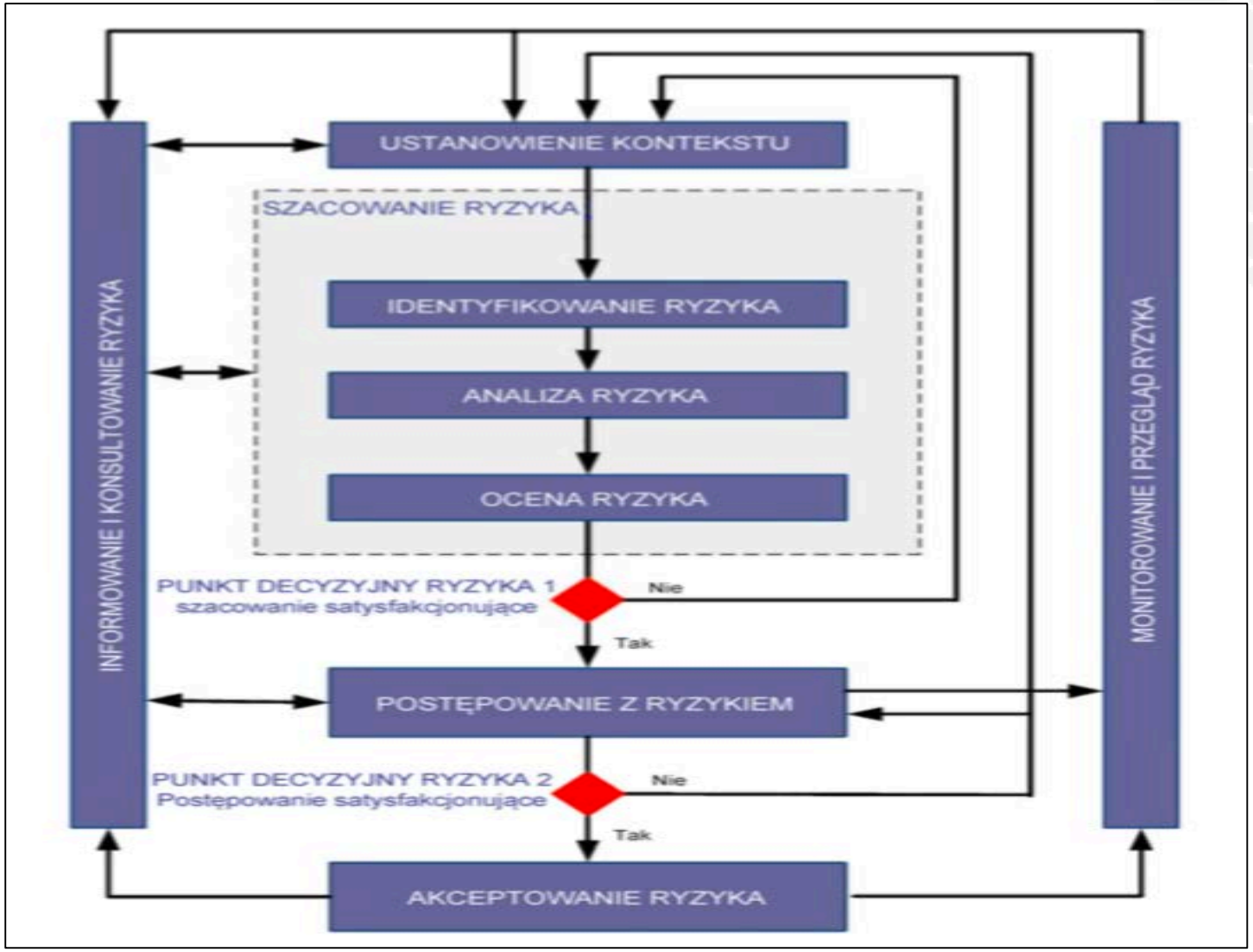
**środowisko wewnętrzne i zewnętrzne,
w którym realizowana jest Usługa Kluczowa**

- ☑ **kontekst Operatora Usługi Kluczowej**
- ☑ **kontekst Usługi Kluczowej**
- ☑ **kontekst Systemów Informacyjnych**

kontekst Usługi Kluczowej

- ☑ wielkość organizacji
- ☑ pozycja rynkowa
- ☑ lokalizacja
- ☑ rodzaj Usługi Kluczowej
- ☑ współzależność z innymi procesami
- ☑ zależność od innych usług, w tym Usług Kluczowych
- ☑ wpływ na inne Usługi Kluczowe
- ☑ rodzaj Systemu Informacyjnego – IT vs. OT
- ☑ skomplikowanie Systemów Informacyjnych
- ☑ zależności Systemów Informacyjnych od systemów zewnętrznych
- ☑ …

kontekst Usługi Kluczowej



„cyberbezpieczeństwo”

Odporność systemów informacyjnych na działania naruszające:

- ☑ **poufność**
- ☑ **integralność**
- ☑ **dostępność**
- ☑ **autentyczność**

przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

ciągłość działania (BCM)

Polska Norma PN-ISO 22301
Bezpieczeństwo powszechne.
Systemy zarządzania ciągłością działania. Wymagania.
(2012)

- ☑ **ciągłość działania – zdolność organizacji do kontynuacji dostarczania wyrobów i świadczenia usług na akceptowalnych, zdefiniowanych poziomach po wystąpieniu incydentu zakłócającego działanie**
- ☑ **działalności priorytetowe – działalności, którym należy nadać** [wysoki] **priorytet po wystąpieniu incydentu, aby złagodzić jego skutki**

analiza wpływu (BIA)

proces analizy Usługi Kluczowej, poprzez ocenę roli Systemów Informacyjnych oraz skutków jakie mogą wywierać incydenty na jej niezakłócone działanie

- ☑ **minimalny cel ciągłości działania (MBCO)**
- ☑ **maksymalny tolerowany czas zakłócenia (MTPD)**
- ☑ **maksymalny akceptowalny przestój (MAO)**
- ☑ **docelowy czas wznowienia działania (RTO)**

metodologia

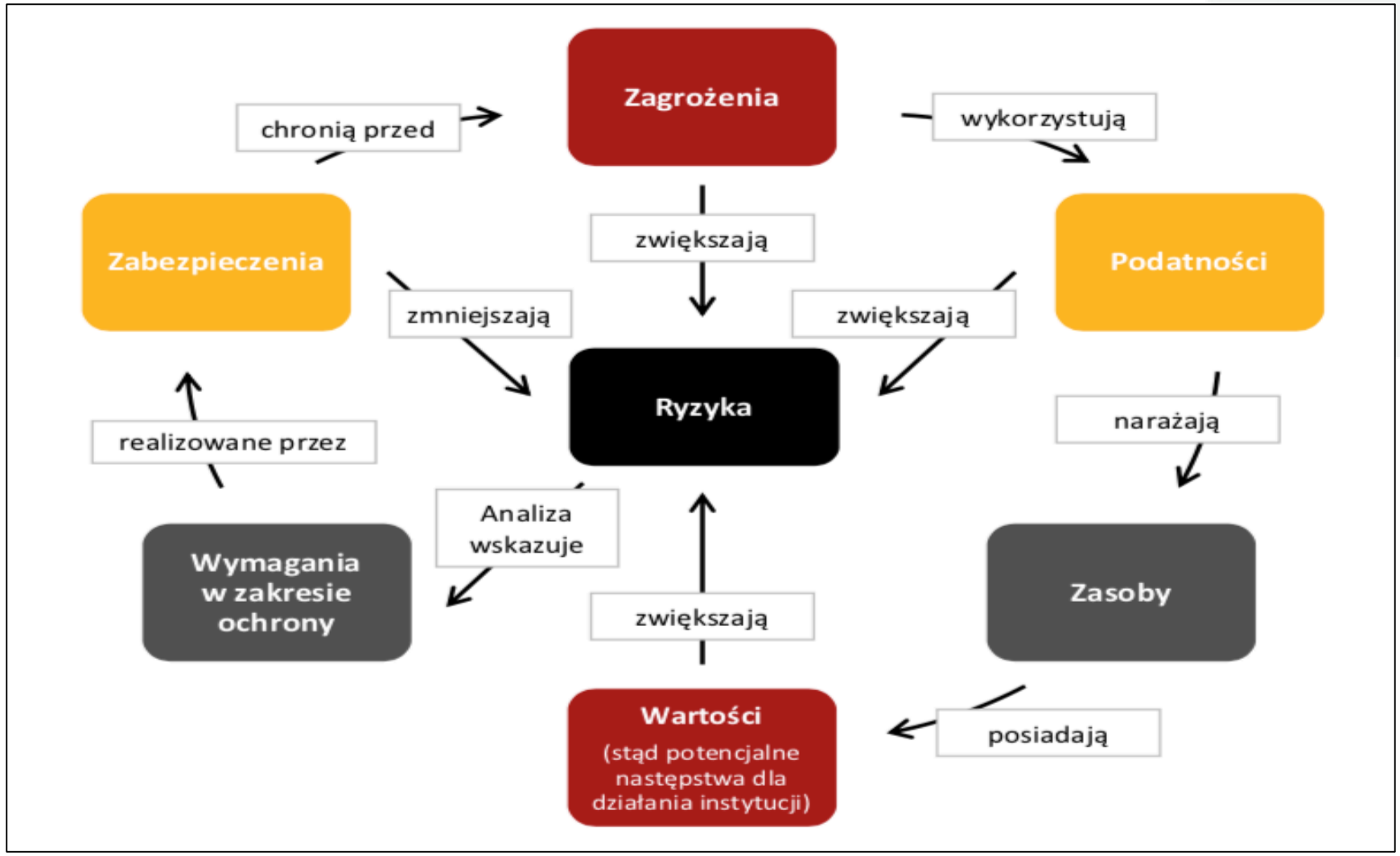
- ☑ PN EN ISO 31000
- ☑ **PN EN ISO / IEC ISO 27005**
- ☑ **MC: Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych**
- ☑ NPC: Metodyka statycznej i dynamicznej analizy ryzyka
- ☑ NIST: Risk Management Framework for Information Systems and Organizations

cel szacowanie ryzyka

Uzyskanie miarodajnej wiedzy o charakterze i poziomie ryzyk dla systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej oraz infrastruktury, z wykorzystaniem której jest ona świadczona.

- ☑ inwentaryzacja i agregacja aktywów
- ☑ identyfikacja zagrożeń i prawdopodobieństwa ich wystąpienia
- ☑ poznanie podatności
- ☑ analiza zabezpieczeń wraz z oceną ich skuteczności
- ☑ **zrozumienie ryzyk dla Usługi Kluczowej**
- ☑ **możliwość zarządzania cyberbezpieczeństwem Usługi Kluczowej**

szacowanie ryzyka



Kto nie zna ani wroga, ani siebie, nieuchronnie ponosi klęskę w każdej walce!

Sun Tzu