Praktyczne aspekty szacowania ryzyka w bezpieczeństwie IT

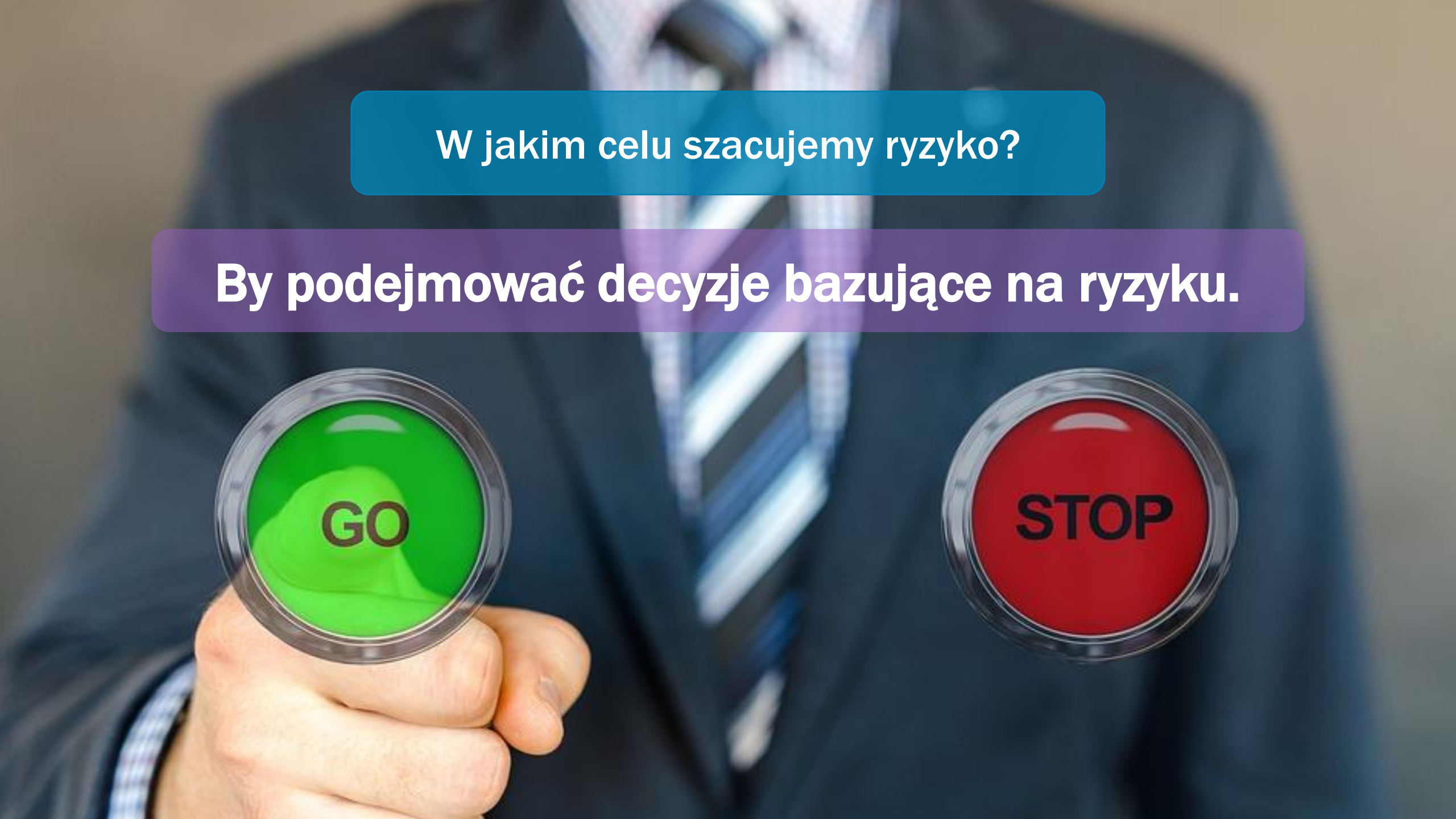
Sebastian Pikur

sebastian.pikur@riskit.pl
Tel. 506 017 114

Agenda

- Szacowania ryzyka – od teorii...
- ... do praktyki - aspekty praktyczne
- Podsumowanie

sebastian.pikur@riskit.pl


W jakim celu szacujemy ryzyko?
By podejmować decyzje bazujące na ryzyku.
GO
STOP

W jakim celu szacujemy ryzyko?

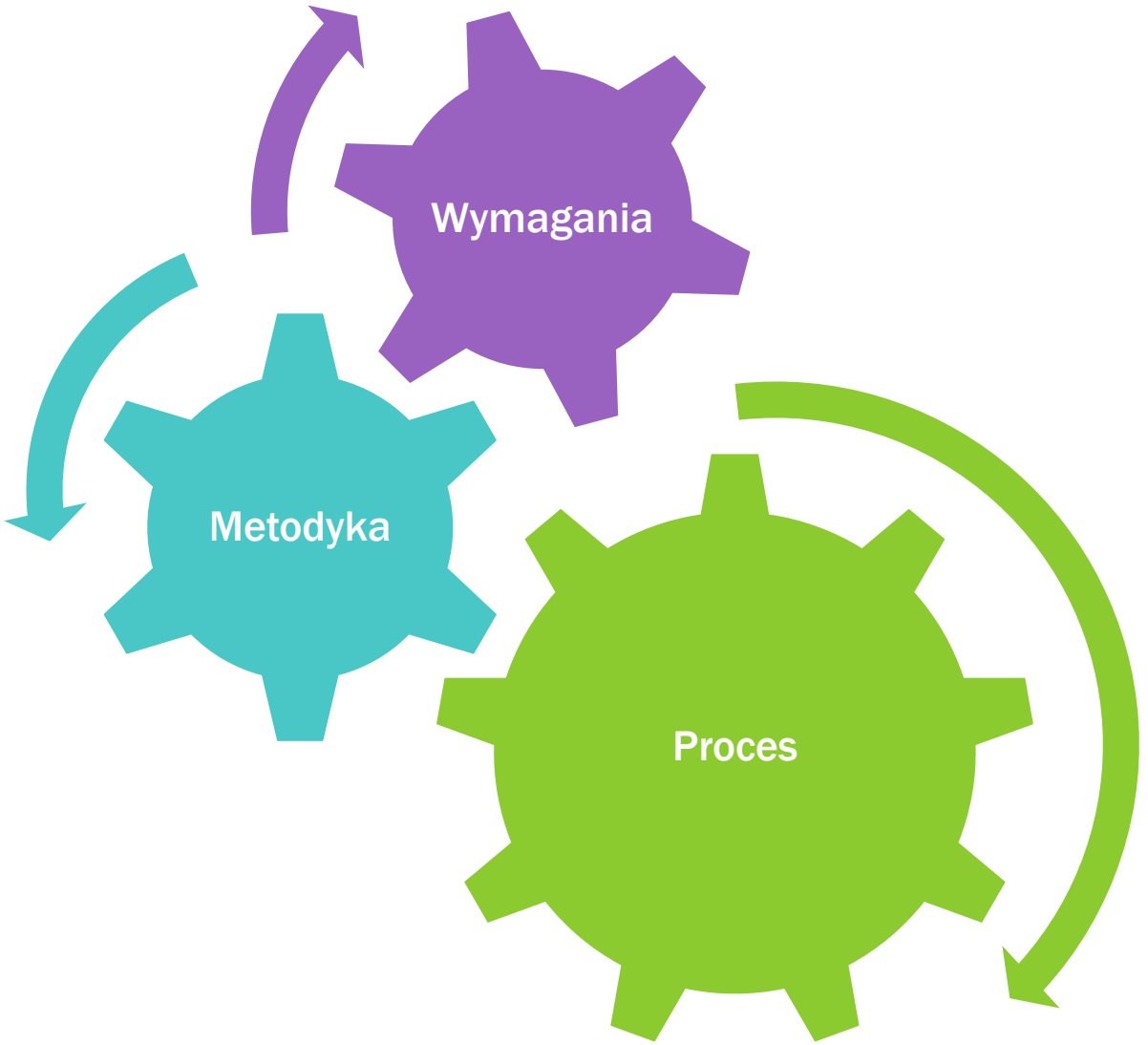
By podejmować decyzje bazujące na ryzyku.

Szacowanie ryzyka

Postępowanie z ryzykiem

Szacowanie ryzyka – od teorii...

- Prawo
  - RODO
- System Zarządzania
  - Bezpieczeństwem
  - Ciągłością działania
  - ...
- Normy
  - ISO 31000
  - ISO/IEC 27005
- ...

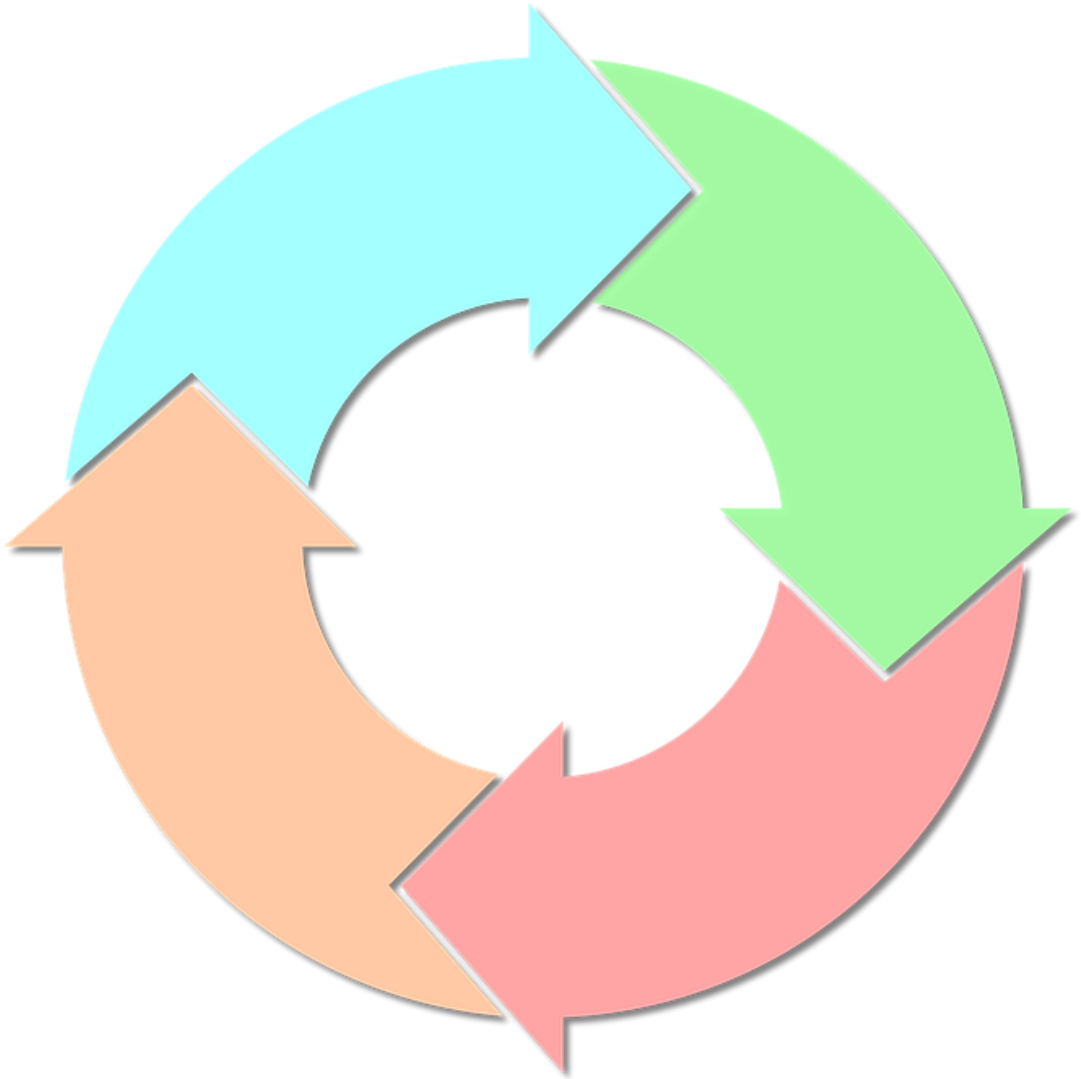


Aspekty praktyczne

... do praktyki

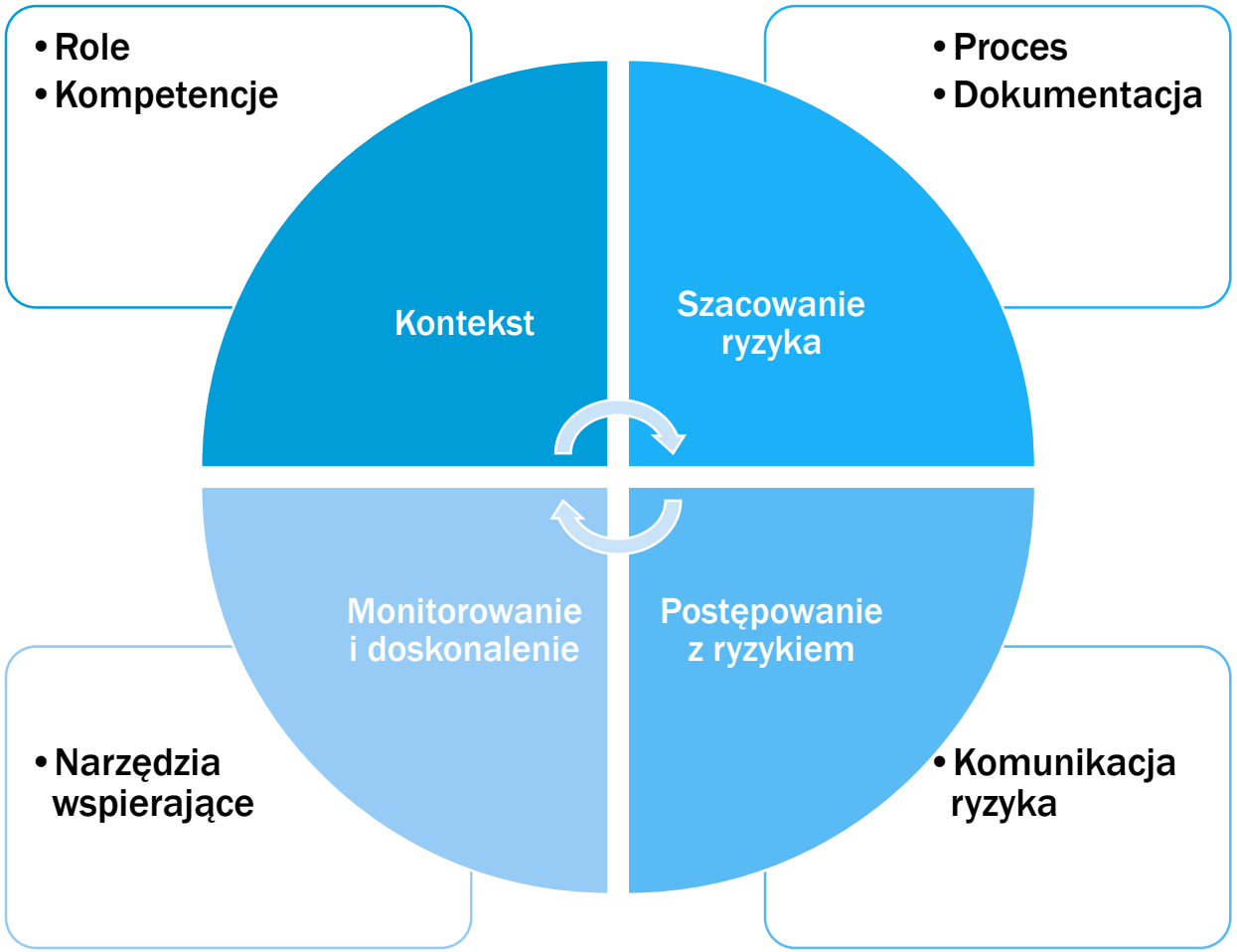
Funkcjonujący proces

Zarządzanie ryzykiem ma być funkcjonującym procesem w organizacji, który podlega ciągłemu doskonaleniu.



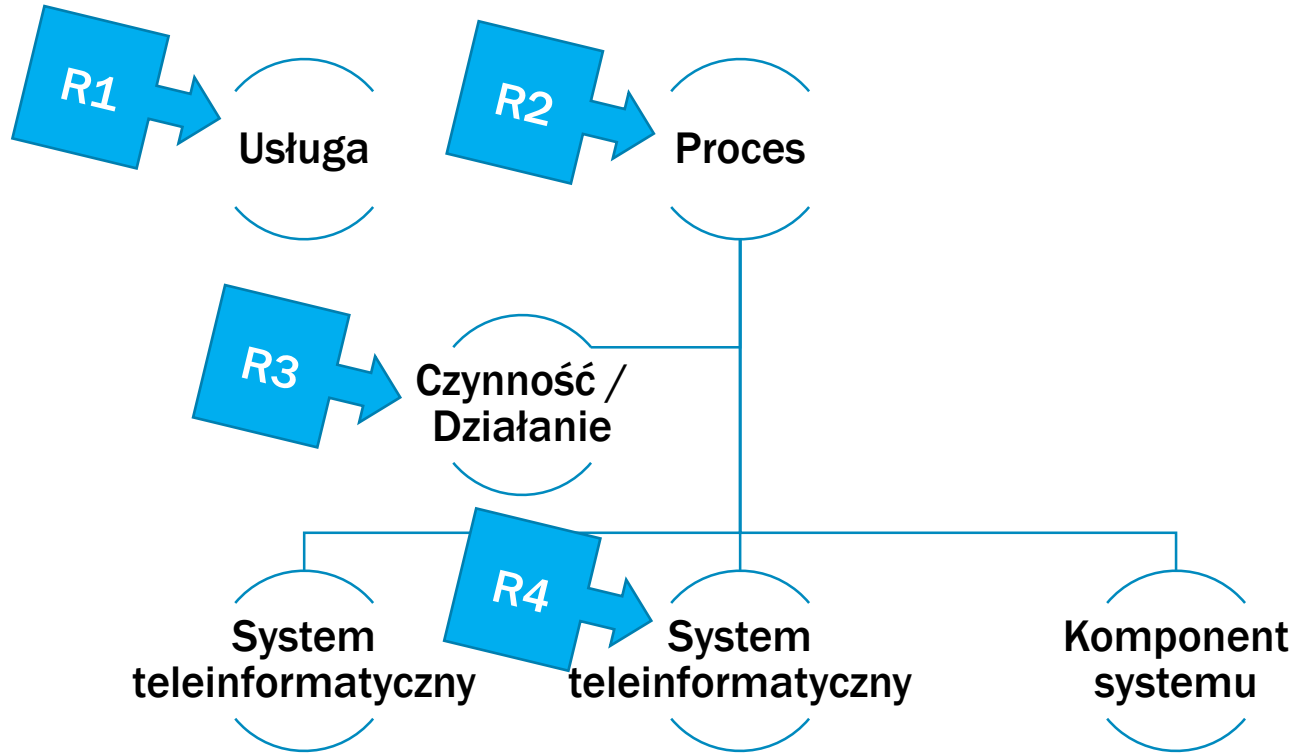
Metodyka

Metodyka zarządzania ryzykiem, w tym szacowania ryzyka musi być dostosowana do dojrzałości organizacji.



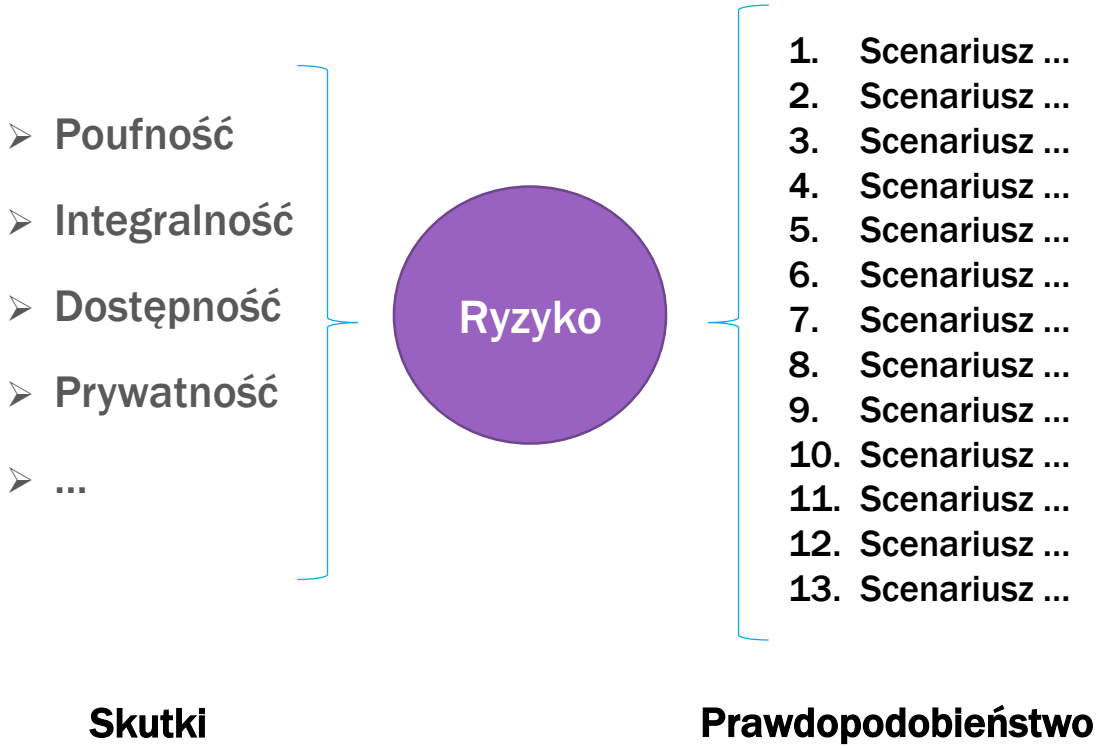
Aktywa

Ryzyko należy szacować wobec aktywa, rozumianego jako proces, działanie, usługa, system teleinformatyczny czy komponent systemu teleinformatycznego.



Analiza ryzyka

Analiza ryzyka musi umożliwić oszacowanie skutków zdarzeń i prawdopodobieństwa ich wystąpienia.



Ryzyko = Skutki * Prawdopodobieństwo

Poziomy analizy ryzyka

Wysokopoziomowa analiza ryzyka

- Szerokie spojrzenie
- Maksymalne uproszczenie analizy
- Selekcja ryzyk do analizy
- Metoda jakościowa

Analiza ryzyka

- Wybrane ryzyka do analizy
- Metoda jakościowa

Szczegółowa analiza ryzyka

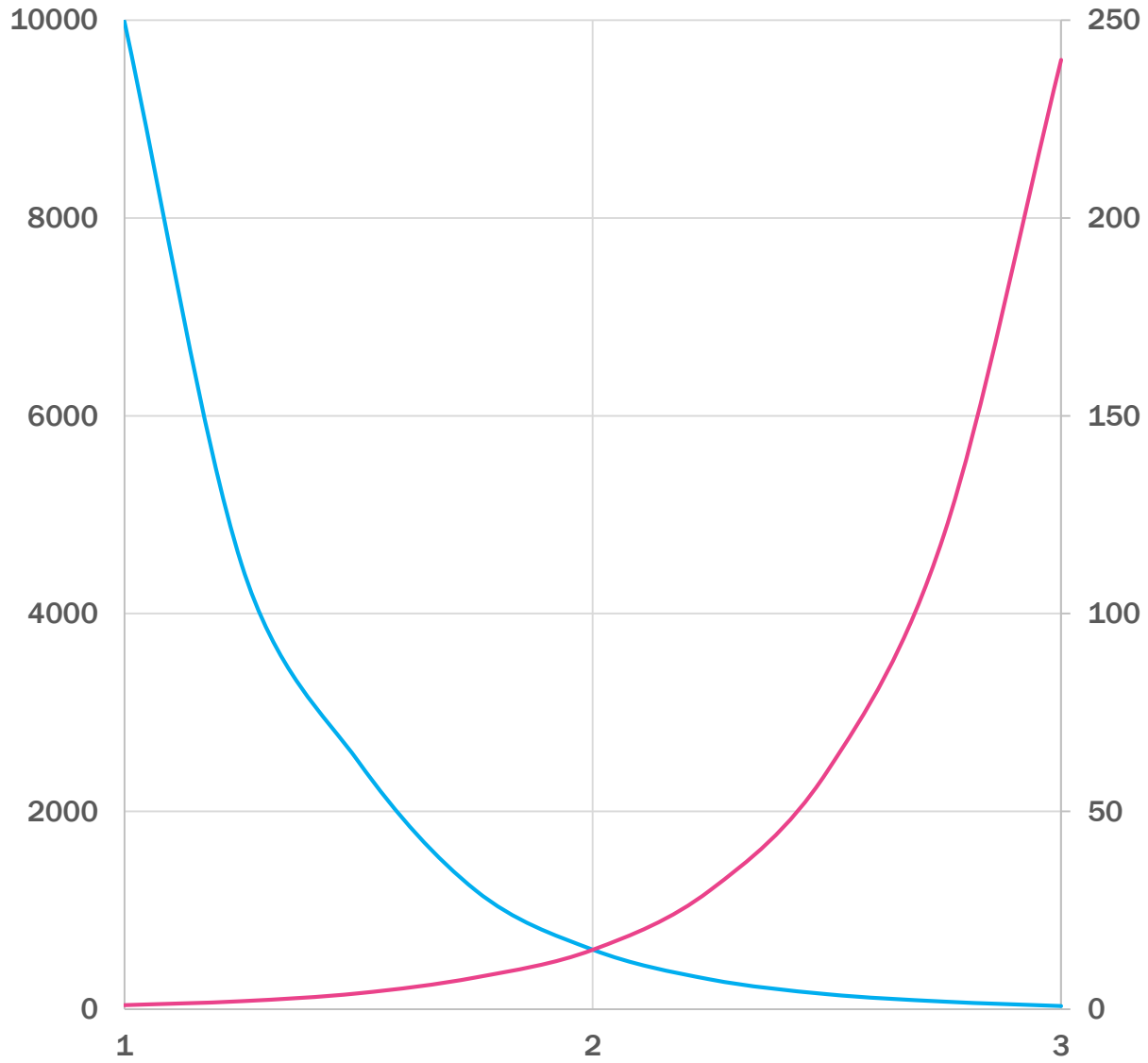
- Ryzyka w których podjęcie decyzji jest trudne
- Metoda ilościowa
- DPIA?

sebastian.pikur@riskit.pl

Prace w ramach poziomów analizy ryzyka

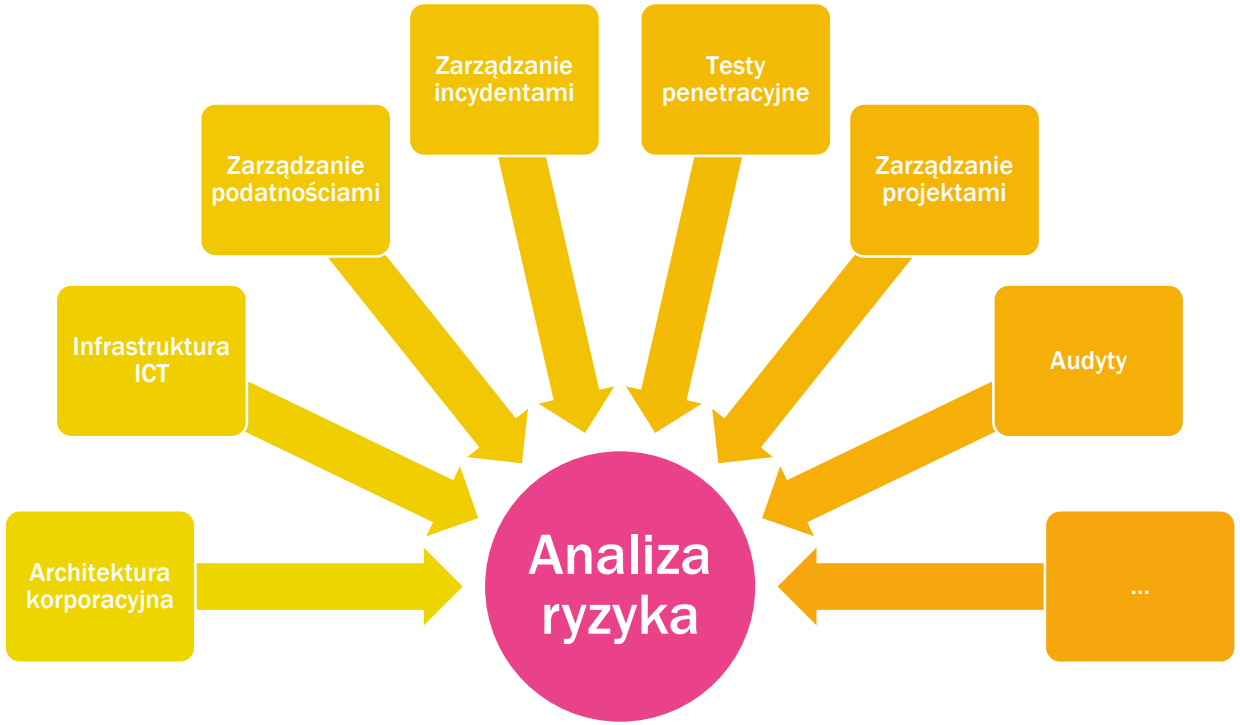
Ilość analizowanych scenariuszy zmniejsza się wraz z przechodzeniem do kolejnych poziomów szacowania ryzyka.

Czas poświęcony na oszacowanie pojedynczego ryzyka rośnie wraz z przechodzeniem do kolejnych poziomów szacowania ryzyka.



Agregowanie informacji o ryzyku

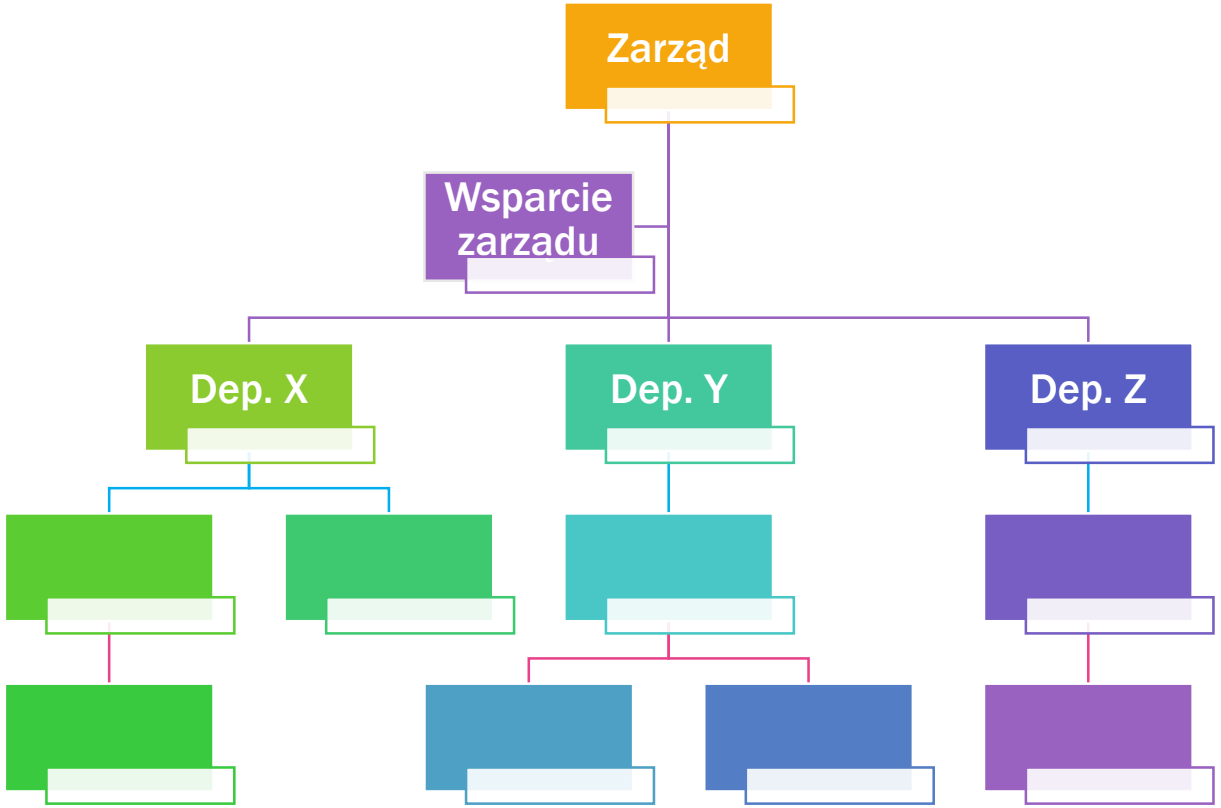
W trakcie analizy ryzyka należy agregować informacje o ryzyku z posiadanych źródeł.



Poparcie zarządu i kierownictwa

Aktywna współpraca z zaangażowanym personelem.

Bardzo istotne jest zaangażowanie niskiego szczebla menadżerskiego – posiadają cenną wiedzę o ryzyku

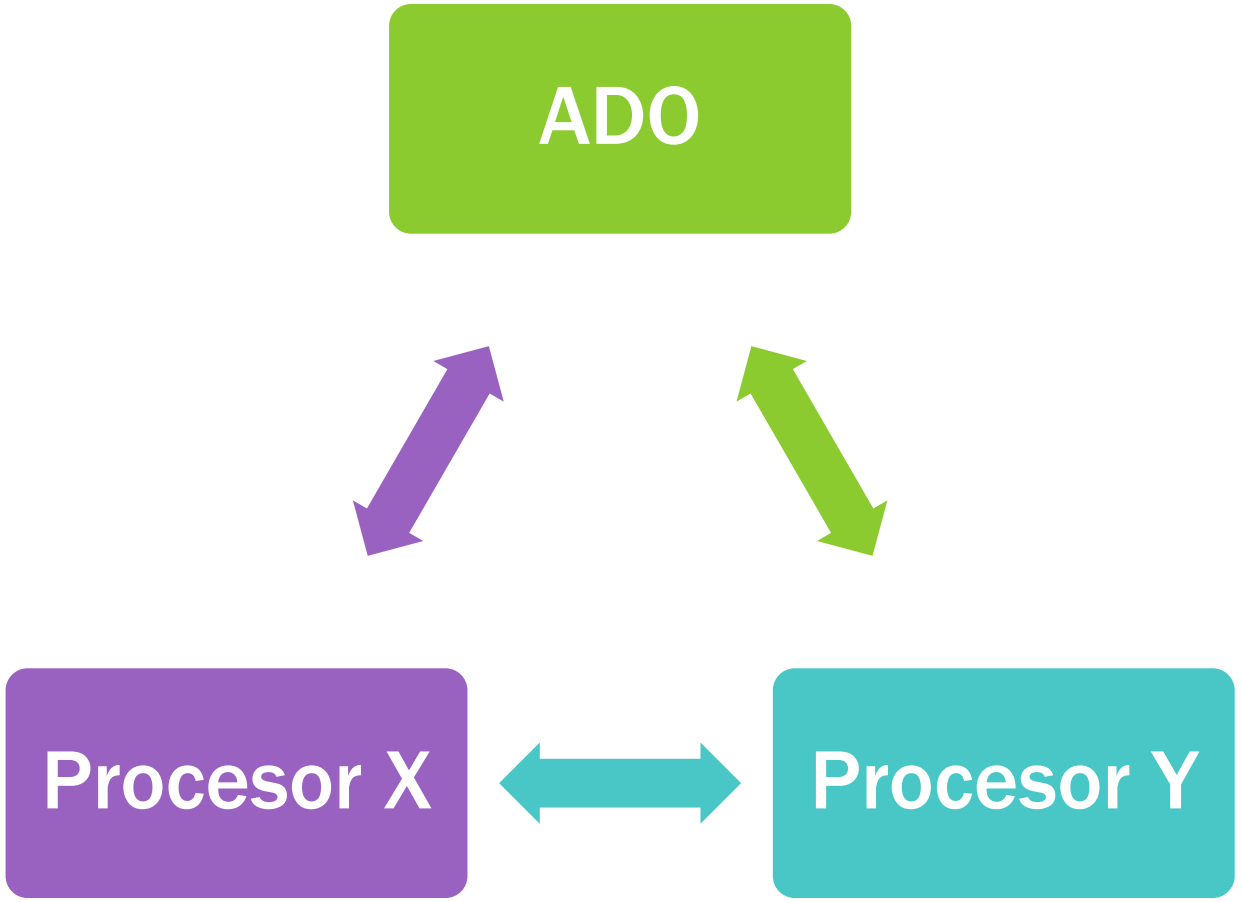


Adaptatywne wdrożenie

Wdrożenie procesu powinno być spiralne, obejmując stopniowo kolejne aspekty.

Komunikowanie ryzyka

Koniecznie należy informować o ryzyku, w szczególności ryzyku IT, które wykracza poza możliwości zarządzania ryzykiem.



Podsumowanie

Podsumowanie

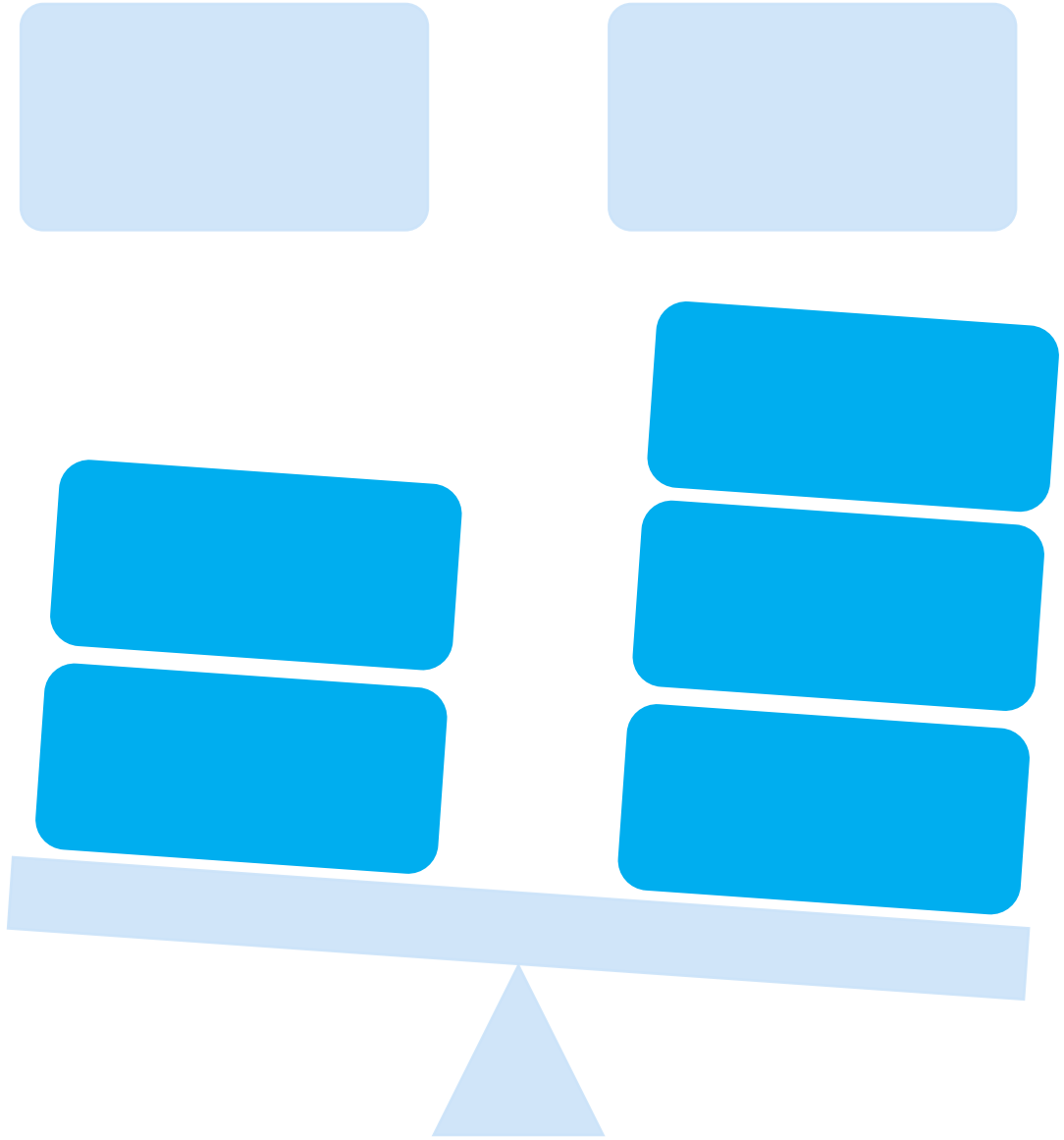
- Celem szacowania ryzyka jest podejmowanie decyzji bazując na ryzyku.
- Zarządzanie ryzykiem jest skuteczne, jeżeli ryzyko jest komunikowane

- Metodyka dopasowana do organizacji
- Proces wdrażany adaptatywnie
- Zaangażowanie zarządu i kluczowego personelu
- Określone aktywa wobec których szacujemy ryzyka
- Agregowanie informacji o ryzyku

sebastian.pikur@riskit.pl

Zrównoważone podejście

Balans pomiędzy oczekiwanymi efektami procesu zarządzania ryzykiem, a posiadanymi zasobami i zdolnościami.



Dziękuję za uwagę

Sebastian Pikur

sebastian.pikur@riskit.pl
Tel. 506 017 114