WEBINARIA GRC

Zarządzanie ryzykiem w bezpieczeństwie informacji

Damian Bielecki

GRC LEGAL

Agenda spotkania

- Definicja i rodzaje ryzyka
- Szacowanie ryzyka
- Zarządzanie ryzykiem
- Plan zachowania ciągłości działania

GRC LEGAL

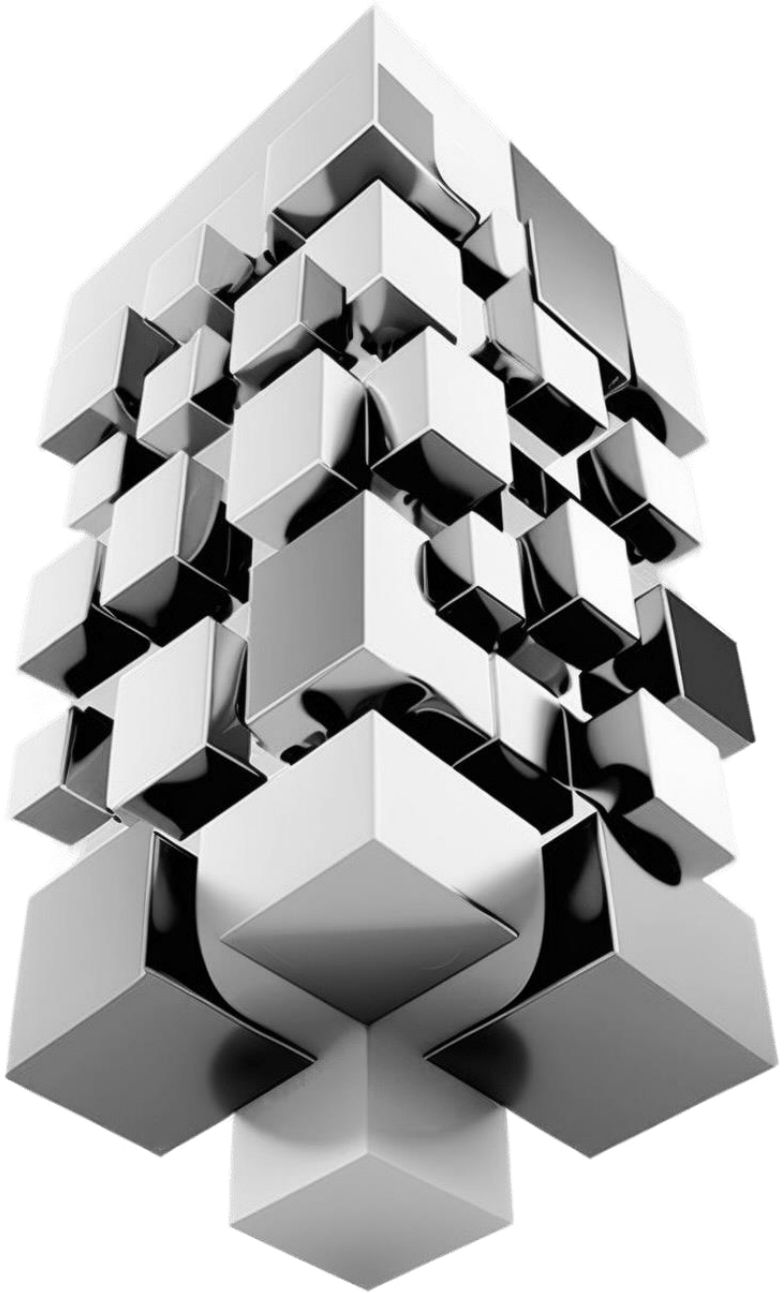
Definicja ryzyka

GRC LEGAL

Definicja ryzyka

Ryzyko to **prawdopodobieństwo** wystąpienia **zdarzenia**, które wywołuje negatywny **wpływ**.

- Ocena wpływu zależy od punktu odniesienia
- Każda ocena ryzyka uwzględnia prawdopodobieństwo oraz wpływ
- W większości są ze sobą niekompatybilne



Przykłady ryzyk

Biznesowe

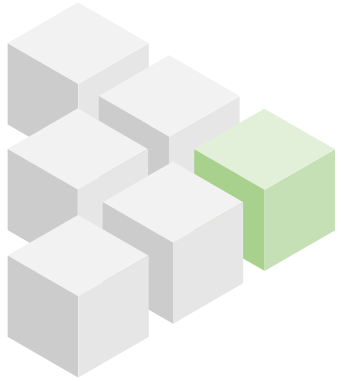
Prawne

Dla podmiotu danych

Dla pracownika

Metodyka analizy ryzyka

Autorska



ISO

NIST

ENISA

Złote zasady analiz ryzyka

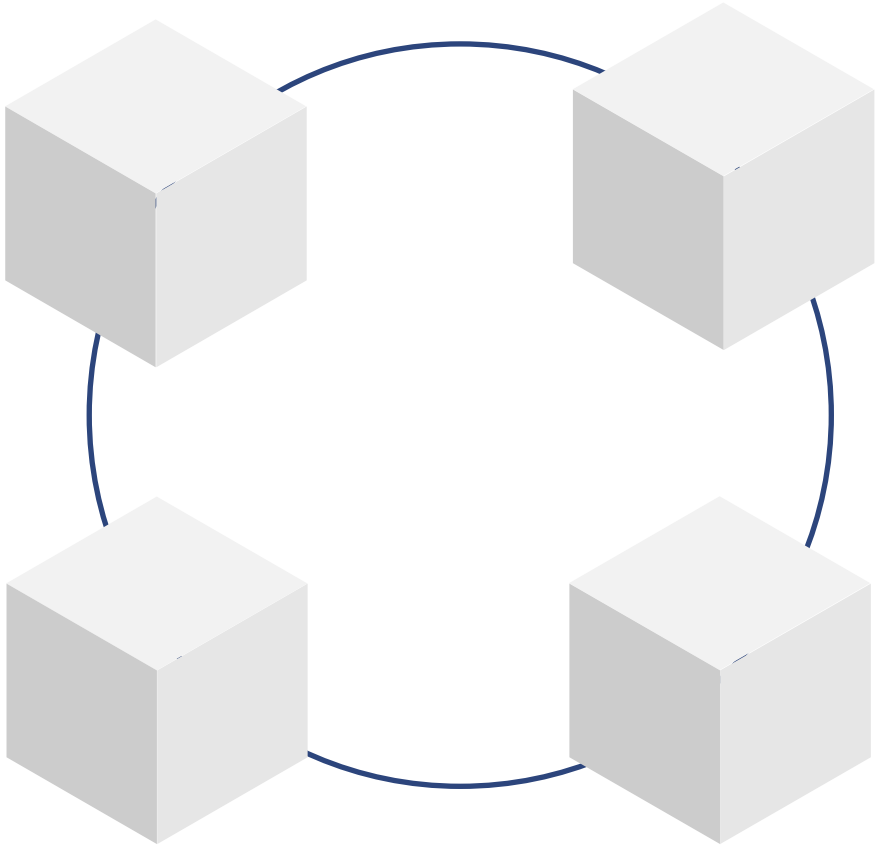
Zarządzanie ryzykiem

GRC LEGAL

Zarządzanie ryzykiem

Identyfikacja ryzyk 1

Szacowanie ryzyk 2



Reagowanie na ryzyka 3

4 **Monitorowanie** ryzyk

Co może być objęte analizą?

A

Proces

B

Projekt

C

System informatyczny

Co może być ryzykiem?

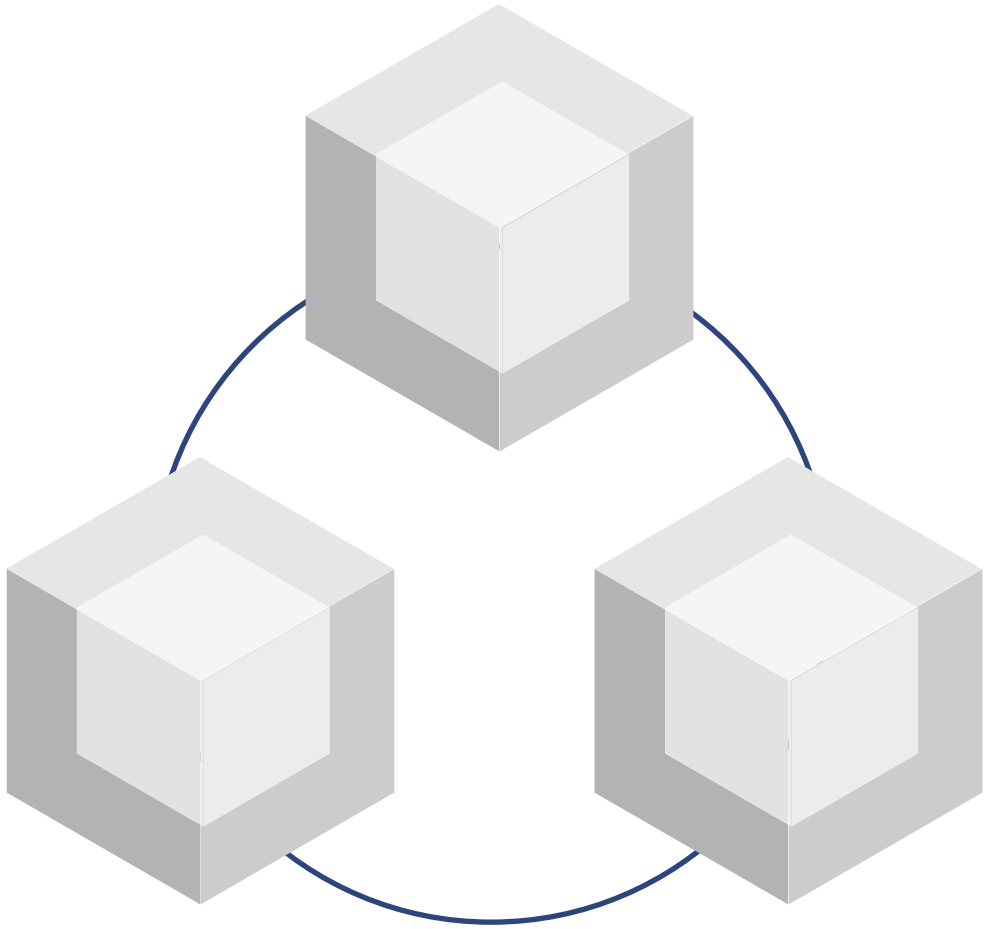
Zdarzenia oparte na **doświadczeniu życiowym**

Zdarzenia **bardzo mało prawdopodobne, ale o katastrofalnych skutkach**

Zdarzenia oparte na **dotychczasowej historii firmy**

Zagrożenia **wskazywane przez ekspertów**

Jak wykryć ryzyka?

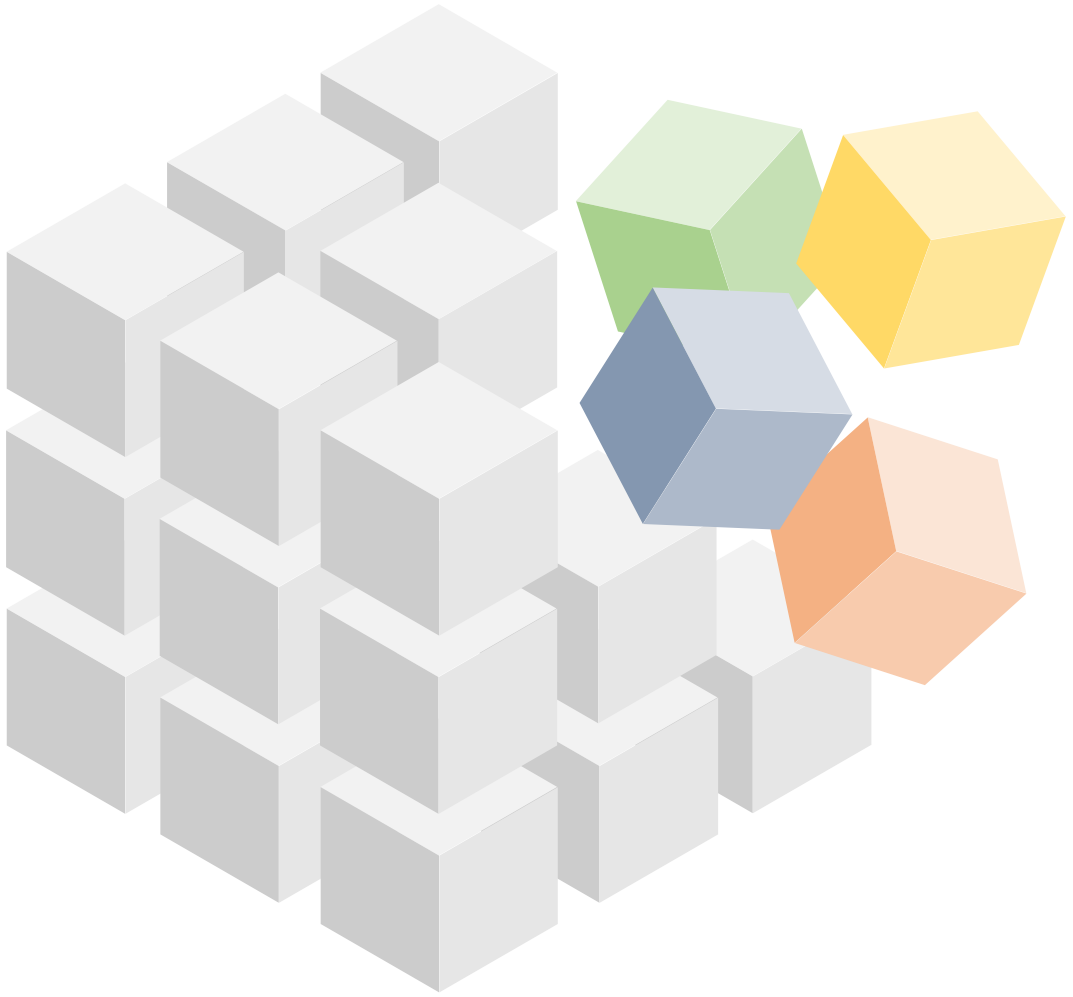


1 Audyty / kontrole

2 Wyciąganie wniosków

3 Teoretyzowanie

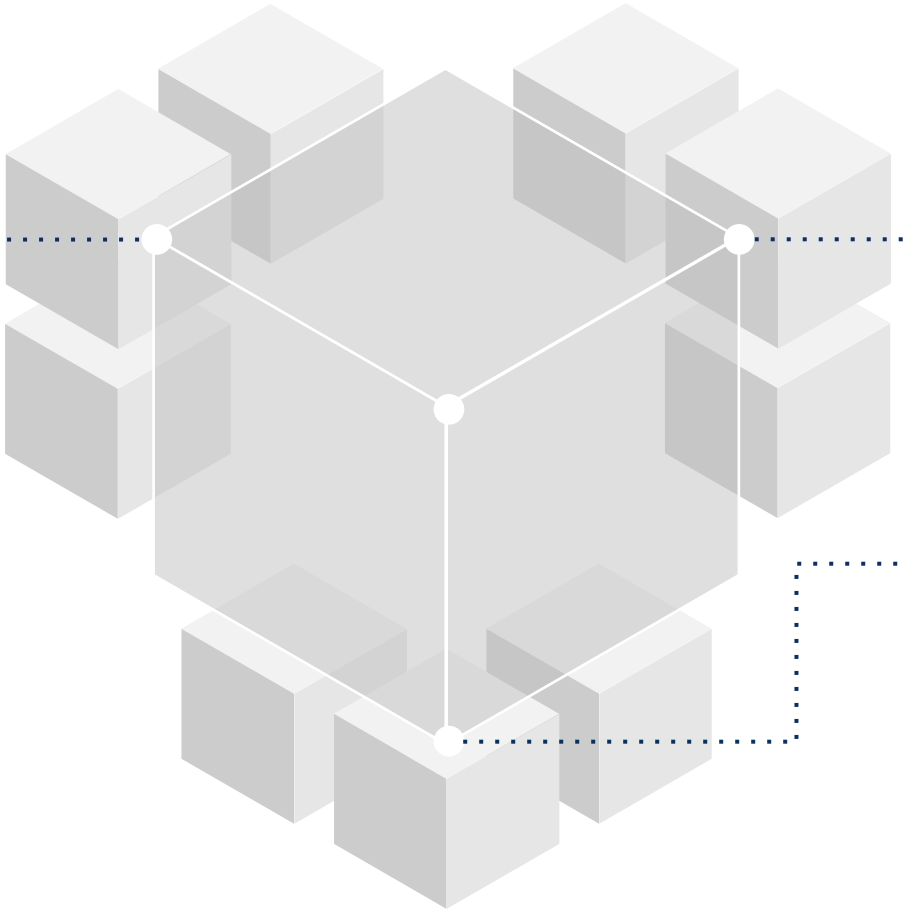
Szacowanie ryzyka



- Excel
- Aplikacja własna lub dostawcy
- Word
- PowerPoint

Prawdopodobieństwo

Czas istnienia ryzyka

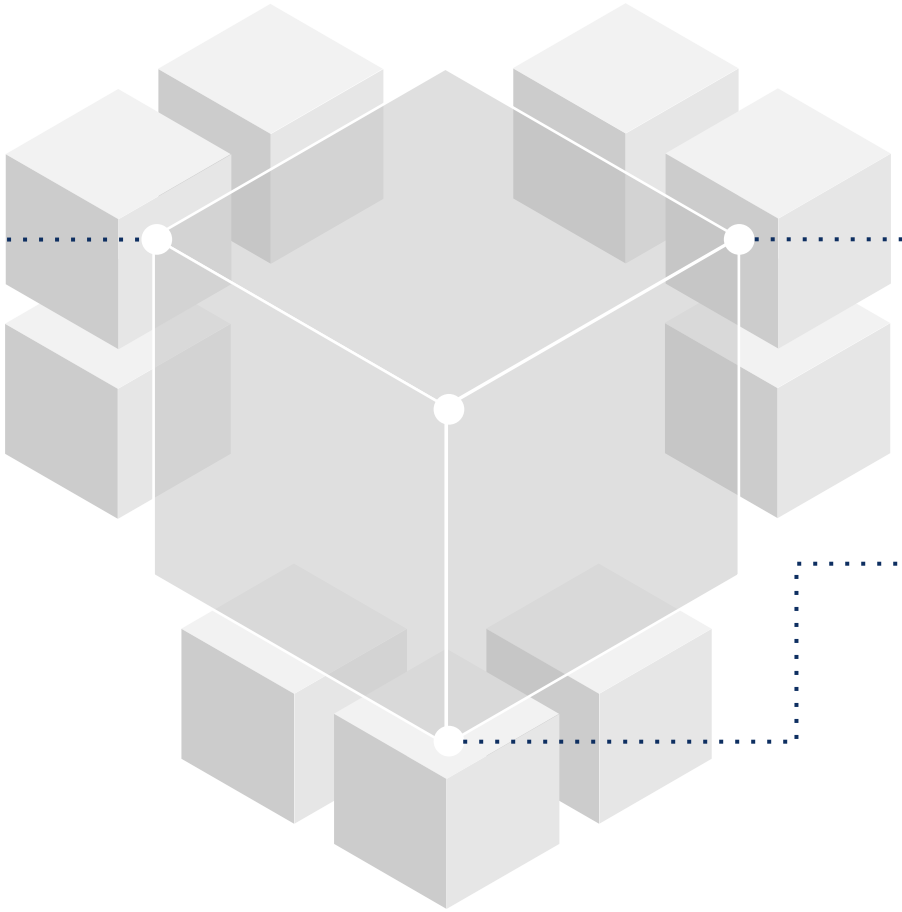


Częstotliwość występowania

Pewność wystąpienia

Wpływ

Poufność

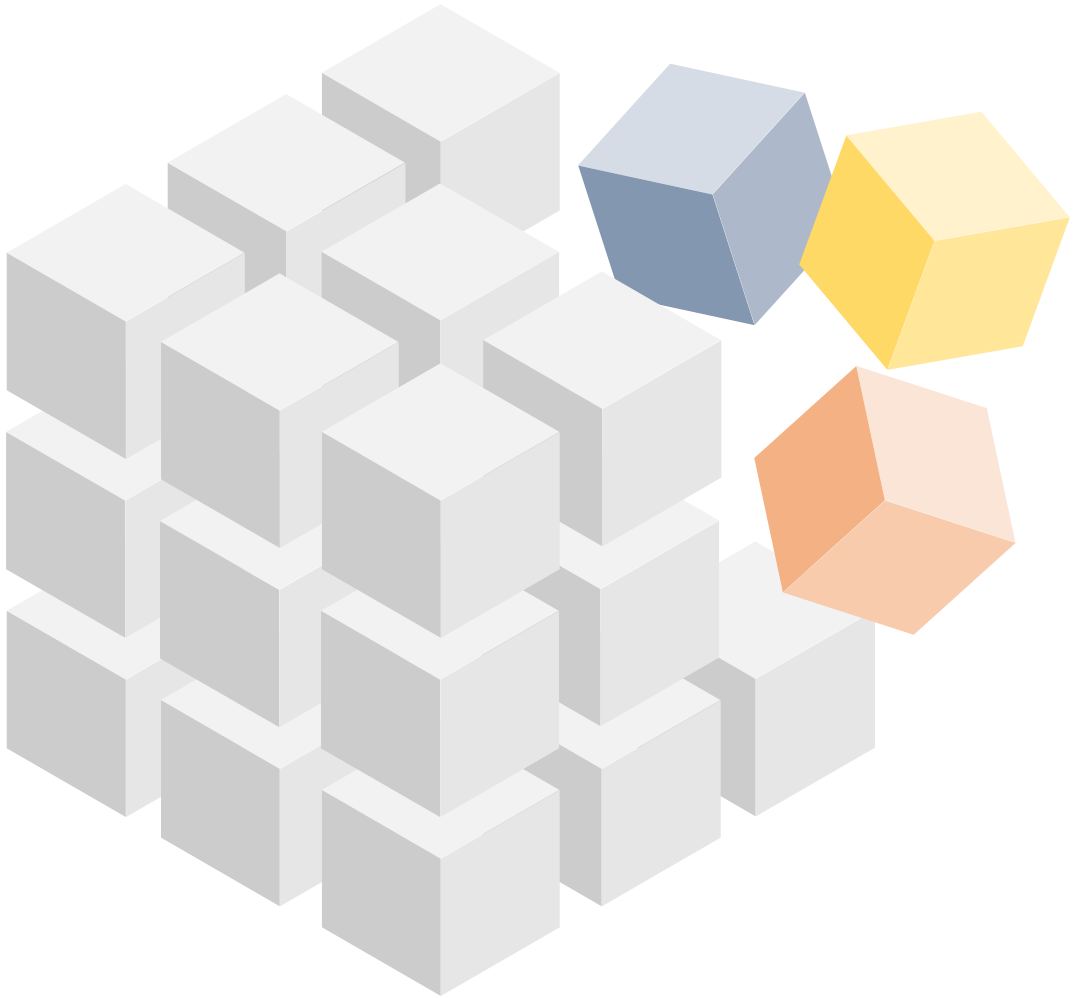


Integralność

Dostępność

GRC LEGAL

Ryzyko



- Niskie
- Średnie
- Wysokie

GRC LEGAL

Reagowanie na ryzyka

A Unikanie

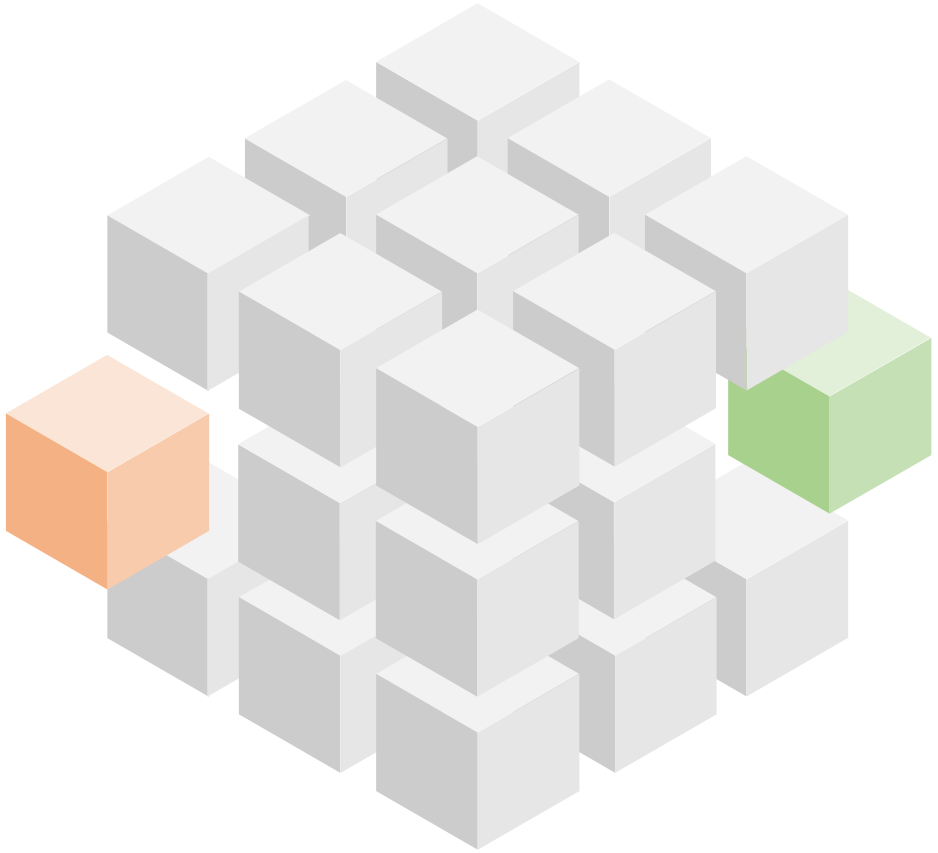
B Redukowanie

C Przeniesienie

D Akceptacja

Monitorowanie ryzyk

Ustalenie daty **wdrożenia środków naprawczych**



Ustalenie daty **ponownej analizy ryzyk**

Plan zachowania ciągłości działania

GRC
LEGAL

Damian Bielecki
+48 539 941 927
damian.bielecki@grclegal.pl