Bezpieczeństwo łańcucha dostaw: ryzyka, ataki i strategie obrony

Jan Anisimowicz CRISC, CISM, PMP

Sebastian Burgemeister CISA, CISM, CRISC, CDPSE, CCAK (…)

29.05.2025

Kilka słów o nas. Zapraszamy do kontaktu z nami (Linkedin, email)

Jan Anisimowicz
C&F SA
Warsaw ISACA Chapter
IIA Polska
Jan.Anisimowicz@candf.com

www.adaptivegrc.com
www.candf.com

Skontaktuj się ze mną na Linkedin!

Sebastian Burgemeister
BW Advisory Sp. z o.o.
IIA UAE (Dubai)
Former President of IIA Polska
s.burgemejster@itgrc.pl

www.itgrc.pl
www.akademiaitgrc.pl

Skontaktuj się ze mną na Linkedin!

O czym dzisiaj powiemy

01 Łańcuch Dostaw

02 Ataki na Łańcuch Dostaw

03 Zarządzanie ryzykiem dostawców

04 Przyszłość: Wykorzystanie QC i blockchain

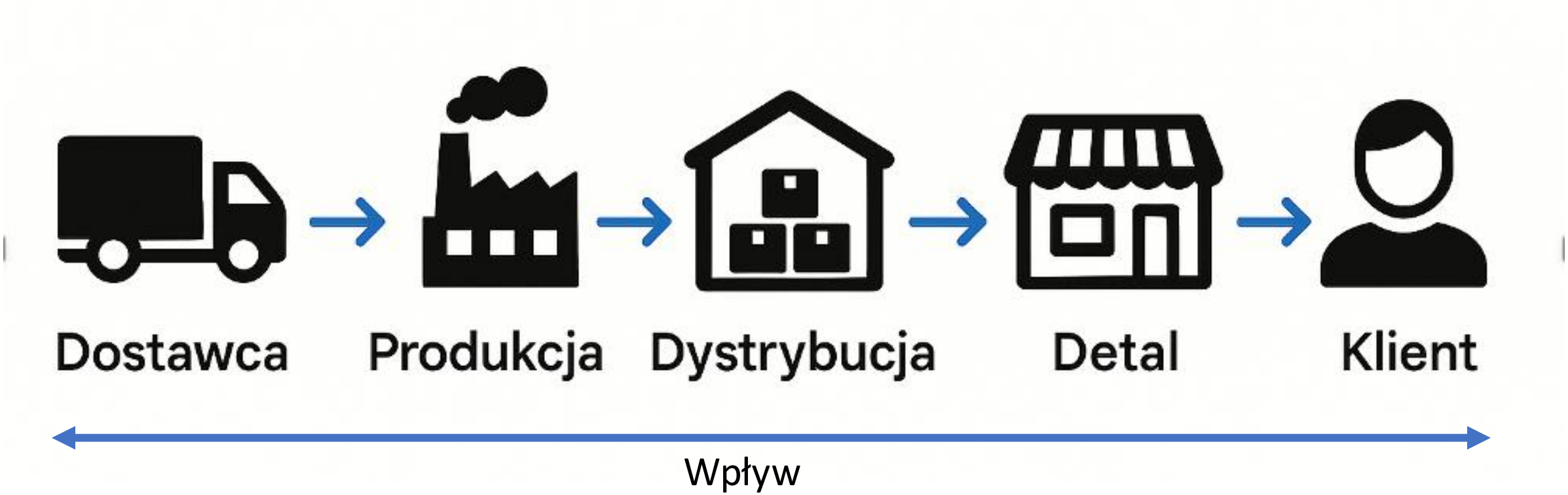
05 Studium przypadku

06 Pytania i odpowiedzi

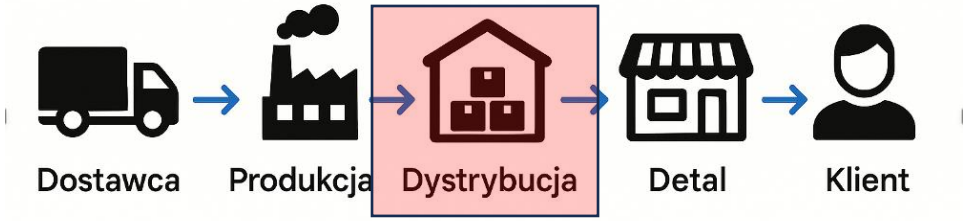
01 Łańcuch Dostaw

Łańcuch dostaw to sieć organizacji zaangażowanych, poprzez powiązania z dostawcami i odbiorcami, w różne procesy i działania, które tworzą wartość w **postaci produktów i usług** dostarczanych ostatecznym konsumentom.

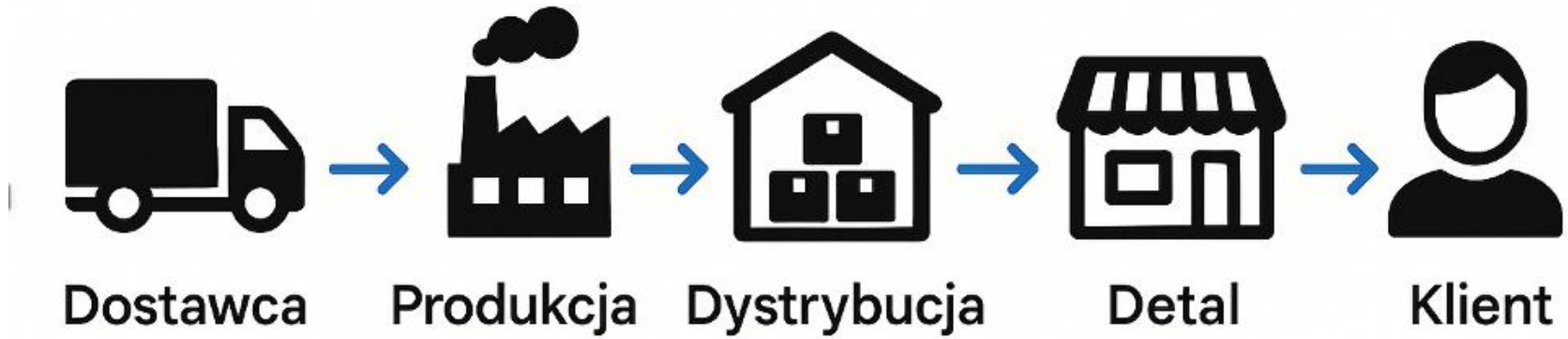
Łańcuch dostaw to sieć organizacji zaangażowanych, poprzez powiązania z dostawcami i odbiorcami, w różne procesy i działania, które tworzą wartość w postaci produktów i usług dostarczanych ostatecznym konsumentom.

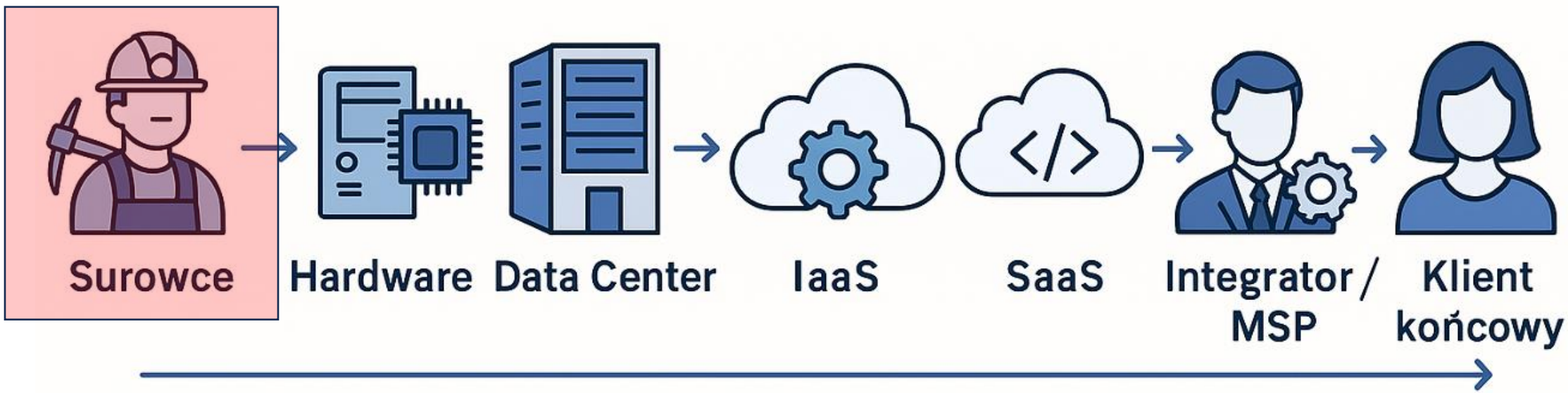


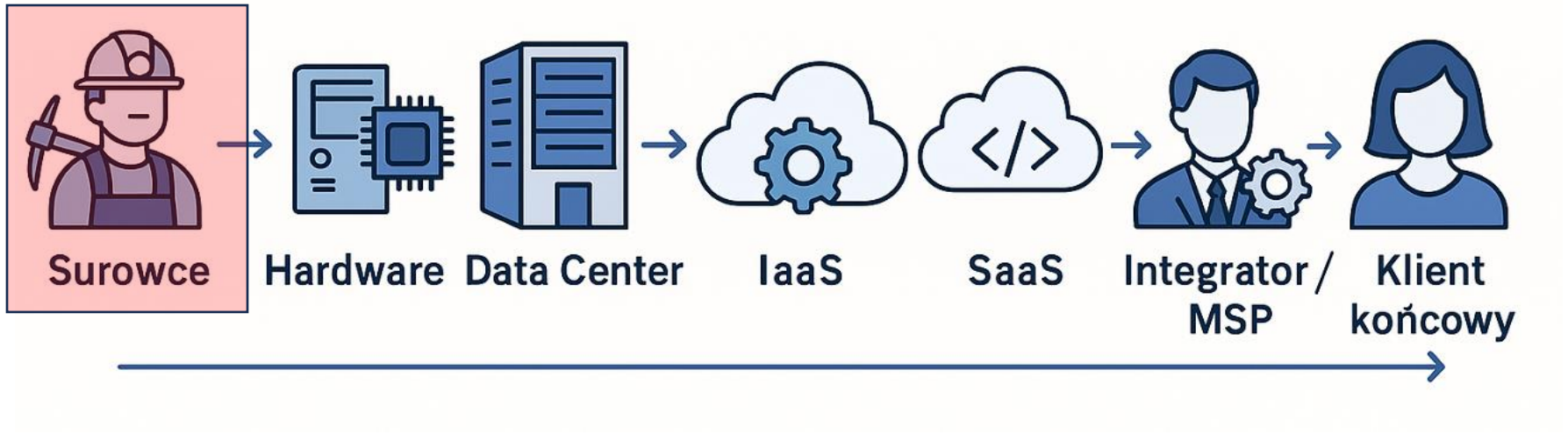
**Uproszczony diagram*


Dostawca
Produkcja
Dystrybucja
Detal
Klient

EVERGREEN


Dostawca
Produkcja
Dystrybucja
Detal
Klient

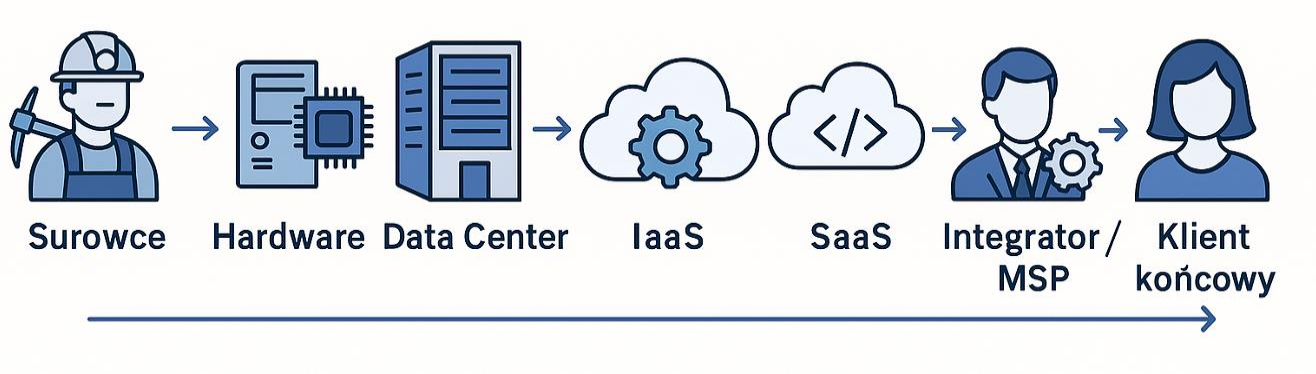

Surowce
Hardware
Data Center
IaaS
SaaS
Integrator / MSP
Klient końcowy



Pierwiastek	Symbol	Zastosowanie
Neodym	Nd	Magnesy w dyskach twardych, wentylatorach, głośnikach
Prazeodym	Pr	Stopy z neodymem w magnesach
Dysproz	Dy	Dodatek do magnesów Nd–Fe–B
Terb	Tb	Luminofory w ekranach LCD i LED
Europ	Eu	Czerwony luminofor w monitorach
Itr	Y	Kondensatory, materiały dielektryczne
Cer	Ce	Polerowanie wafli krzemowych

Pierwiastek	Symbol	Zastosowanie
Lantan	La	W kondensatorach i stopach
Samar	Sm	Magnesy trwałe (SmCo)
Gadolin	Gd	Czujniki termiczne, chłodzenie
Holm	Ho	Materiały magnetyczne
Tul	Tm	Luminofory specjalne
Złoto	Au	Połączenia elektryczne, styki, złącza procesora
Srebro	Ag	Pasty lutownicze, złącza, przewodniki

Łańcuch Dostaw to **sekwencja zdarzeń**, która ma na celu zaspokojenie popytu na określone **produkty i usługi**.



(*)Definicja własna, uproszczona ale pragmatyczna

02 Ataki na Łańcuch Dostaw

synnovis
A SYNLAB pathology partnership

solarwinds

Ques Diagnos

Kaseya®

Colonial Pipeline Company

AIRBUS
DEFENCE & SPACE

LOG4J

NHS

Exchange

Microso

okta

UnitedHealth Group

www.itgrc.pl

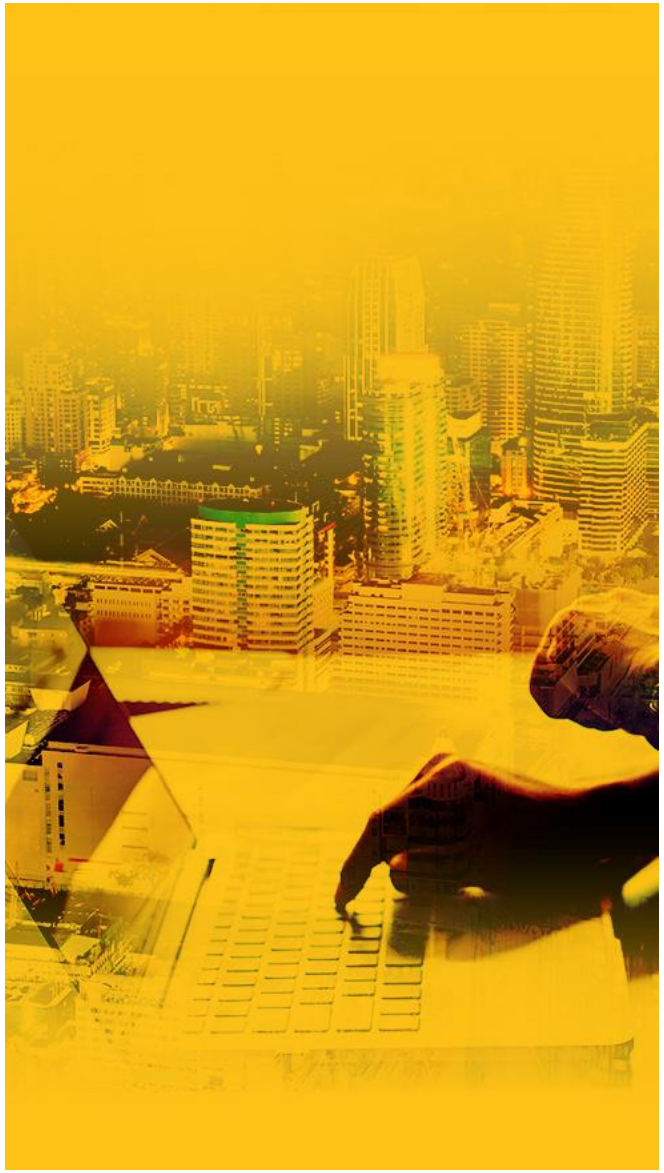
BW advisory
Przez naszą wiedzę do Twojej wartości.

ENISA Threat Landskape 2024, ENISA

WYMAGANIA PRAWNE

www.itgrc.pl

BW advisory
Przez naszą wiedzę do Twojej wartości.



RODO

NIS 2.0

DORA

CRA

CER

AI Act

GLOBALNE / LOKALNE
w zakresie cyber i ochrony prywatności

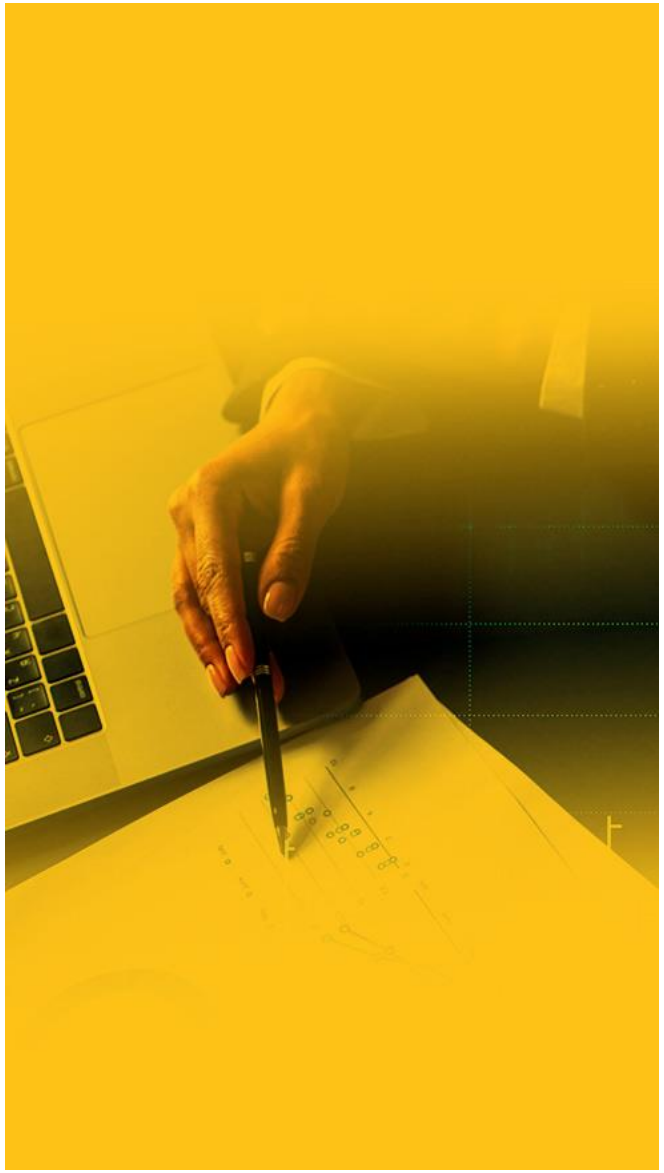
www.itgrc.pl

BW advisory
Przez naszą wiedzę do Twojej wartości.

ŁAŃCUCH DOSTAW

www.itgrc.pl

BW advisory
Przez naszą wiedzę do Twojej wartości.



Kategorie Łańcucha Dostaw

Organizacje

Partnerzy i zależności: Identyfikacja organizacji, z którymi współpracujemy, od których jesteśmy zależni, oraz charakteru tych zależności.

Dostęp i przetwarzanie danych: Zrozumienie, kto ma dostęp do naszych systemów i danych oraz jakie dane są przez nich przetwarzane.

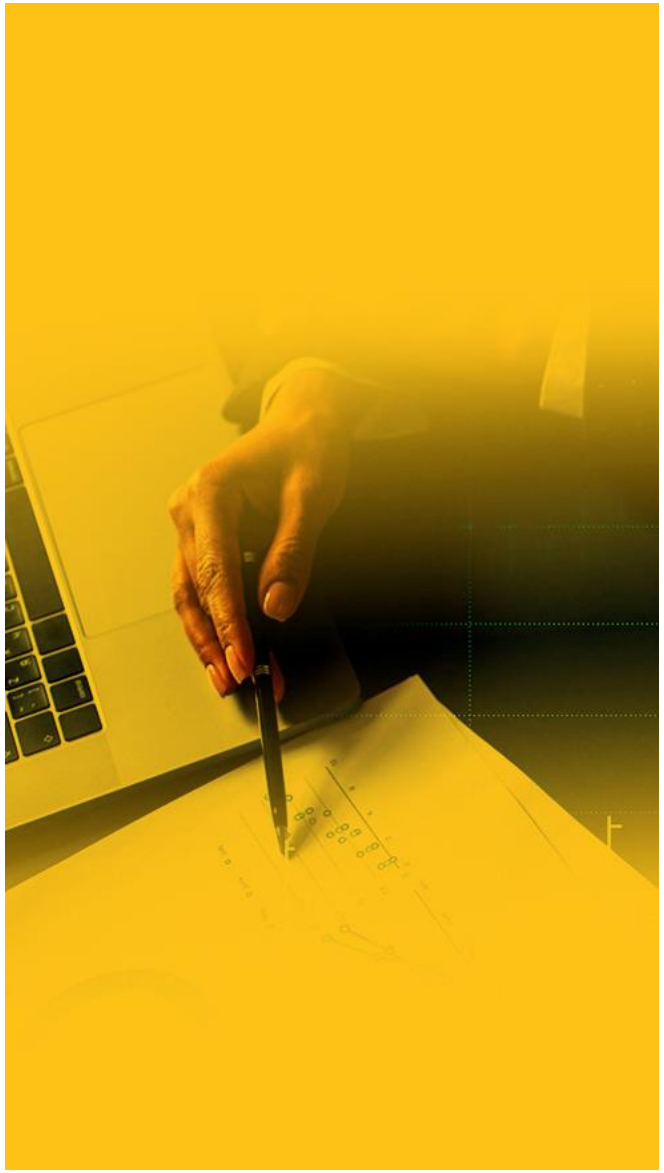
Oprogramowanie

Komponenty oprogramowania stron trzecich: Sporządzenie listy komponentów oprogramowania dostarczanych przez strony trzecie, na których polegamy, oraz identyfikacja elementów zewnętrznych zintegrowanych z naszym oprogramowaniem.

Zależności oprogramowania: Rozpoznanie zależności od rozwiązań stron trzecich, które są osadzone w naszym stosie technologicznym.

Sprzęt

Komponenty sprzętowe stron trzecich: Zrozumienie, które komponenty sprzętowe pochodzą od stron trzecich oraz ocena ich pochodzenia i potencjalnych implikacji dla bezpieczeństwa w naszej infrastrukturze.



Przegląd Bezpieczeństwa Łańcucha Dostaw Oprogramowania

Świadomość komponentów

Znajomość komponentów oprogramowania: Pełne zrozumienie wszystkich wykorzystywanych komponentów oprogramowania, zarówno autorskich, jak i pochodzących od stron trzecich.

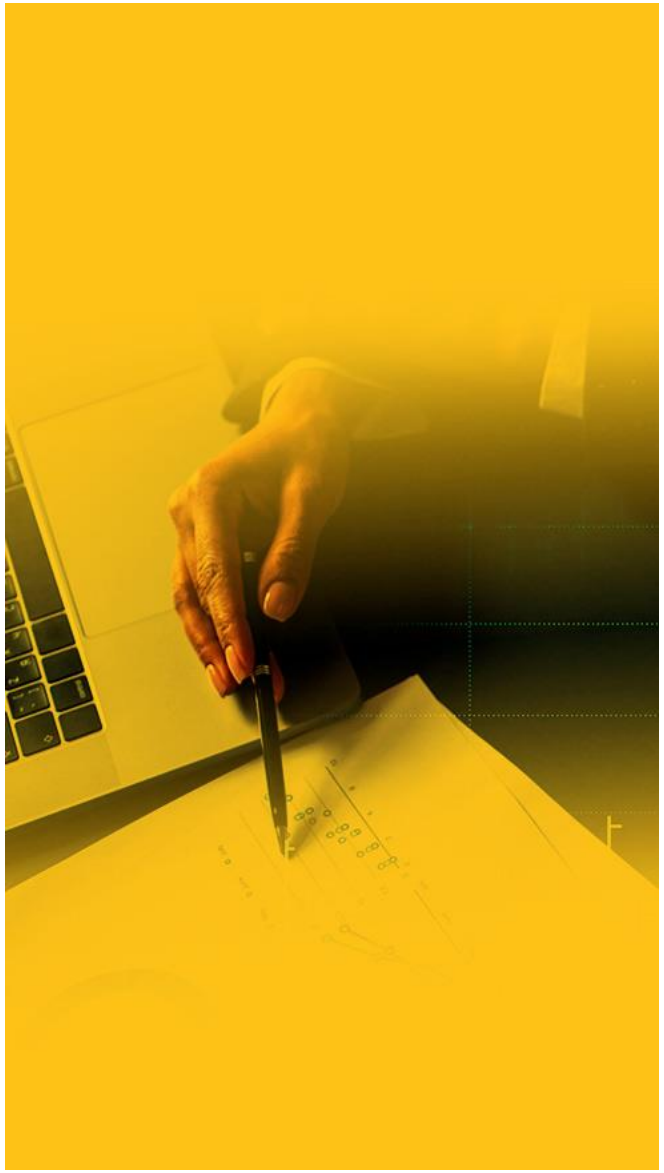
Lista materiałów oprogramowania (SBOM): Tworzenie szczegółowej ewidencji (SBOM) wszystkich komponentów oprogramowania, wraz z wersjami i pochodzeniem, w celu zapewnienia przejrzystości i ułatwienia zarządzania bezpieczeństwem.

Biblioteki open source: Zarządzanie i monitorowanie bibliotek open source w celu zapewnienia zgodności i ograniczenia potencjalnych zagrożeń.

Zarządzanie zależnościami i podatnościami

Skanowanie zależności: Identyfikacja i zarządzanie zależnościami w oprogramowaniu w celu eliminacji ukrytych ryzyk.

Skanowanie podatności: Regularne skanowanie wszystkich komponentów pod kątem znanych podatności, aby zapewnić ich szybkie usuwanie.



Przegląd Bezpieczeństwa Łańcucha Dostaw Oprogramowania

SBOM dla zgodności i bezpieczeństwa

Zarządzanie SBOM: Wykorzystywanie listy materiałów oprogramowania (SBOM) do śledzenia wszystkich bibliotek, komponentów i zależności w celu zapewnienia zgodności regulacyjnej i oceny ryzyka.

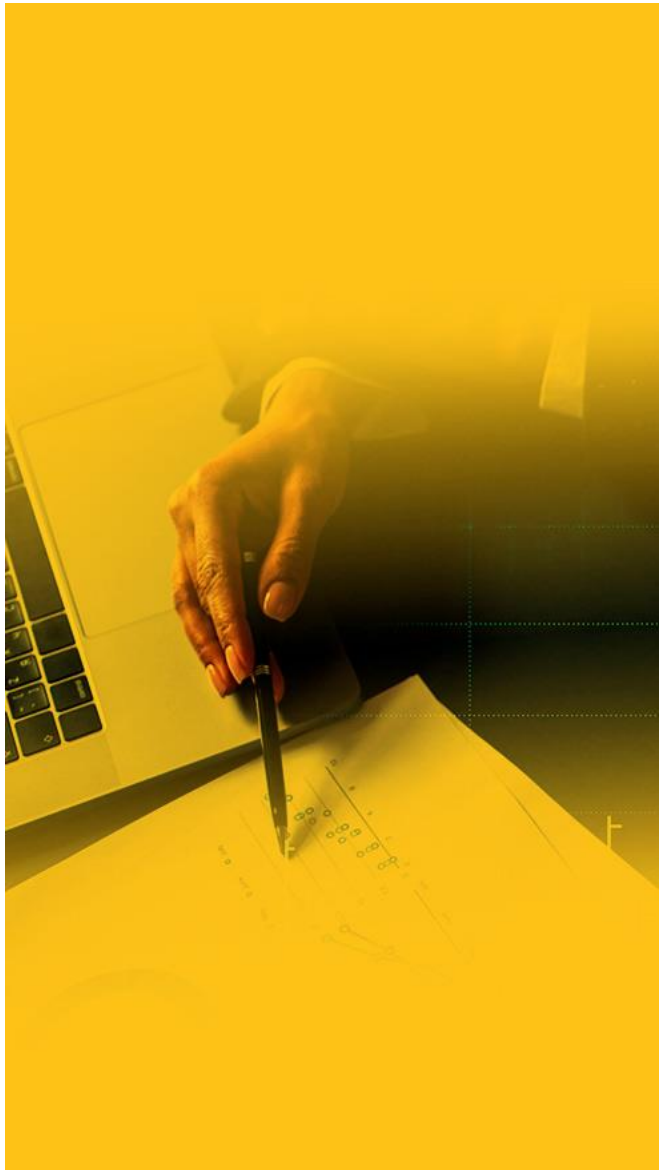
Skanowanie prawne i bezpieczeństwa: Wykorzystanie danych SBOM do weryfikacji zgodności licencyjnej oraz identyfikacji podatności bezpieczeństwa we wszystkich komponentach oprogramowania.

Analiza kodu statyczna i dynamiczna: Przeprowadzanie zarówno statycznej, jak i dynamicznej analizy kodu w celu wykrycia potencjalnych luk bezpieczeństwa w środowiskach produkcyjnych i testowych.

Bezpieczny Cykl Życia Tworzenia Oprogramowania (SDLC)

Integracja SBOM z SDLC: Wykorzystywanie SBOM na każdym etapie cyklu życia tworzenia oprogramowania w celu zapewnienia, że wszystkie komponenty zostały sprawdzone pod kątem bezpieczeństwa i zgodności.

Zwiększona przejrzystość: SBOM dostarcza przejrzystą, aktualną listę wszystkich komponentów oprogramowania, co wspomaga identyfikację ryzyk, ułatwia audyty i zwiększa odporność systemu.



Najlepsze praktyki w zakresie bezpieczeństwa łańcucha dostaw sprzętu

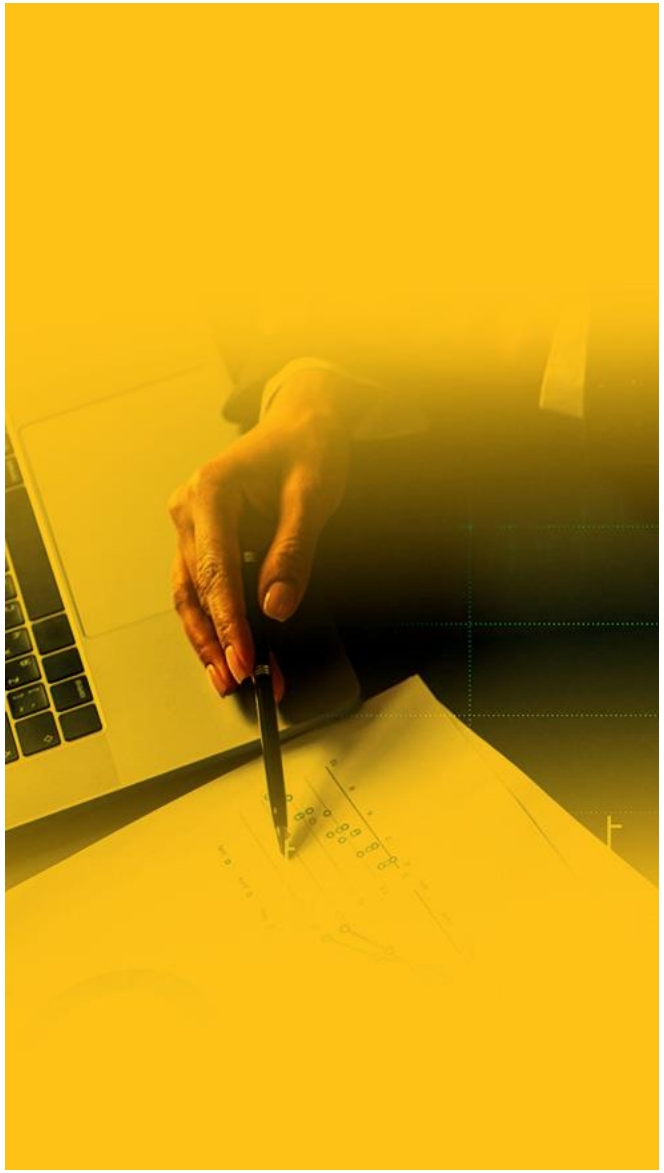
Znajomość komponentów sprzętowych

Zarządzanie rejestrem:
Utrzymuj kompletną i dokładną ewidencję wszystkich komponentów sprzętowych wykorzystywanych w organizacji.

Identyfikowalność komponentów:
Zapewnij możliwość śledzenia pochodzenia każdego komponentu.

Certyfikacja urządzeń

Certyfikowane i bezpieczne urządzenia:
Używaj sprzętu spełniającego uznane w branży normy bezpieczeństwa, takie jak FIPS czy Common Criteria.



Najlepsze Praktyki w Zakresie Bezpieczeństwa Łańcucha Dostaw Sprzętu

Zaufani partnerzy

Sieć zaufanych dostawców: Budowanie relacji z wiarygodnymi dostawcami oraz priorytetowe traktowanie partnerów wykazujących zaangażowanie w bezpieczeństwo łańcucha dostaw.

Należyta staranność i audyty: Regularna ocena praktyk bezpieczeństwa dostawców poprzez audyty i analizy.

Bezpieczny proces zakupowy: Wdrożenie bezpiecznego procesu pozyskiwania sprzętu.

Ostrzeżenia i rozpoznanie dotyczące zagrożeń

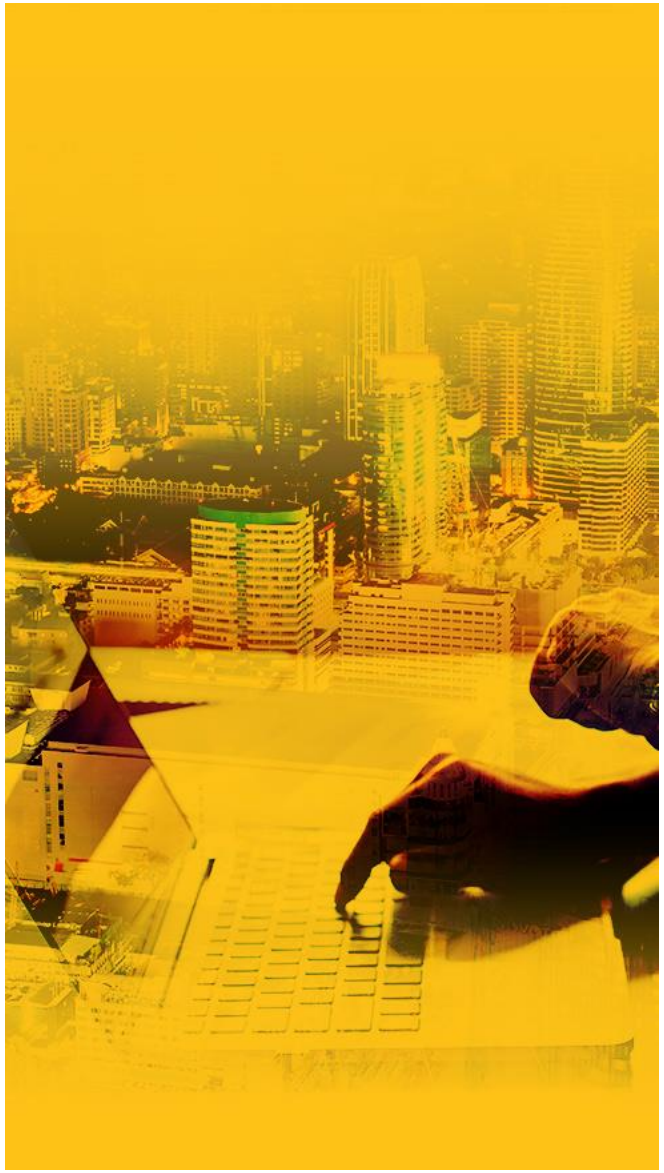
Źródła informacji o zagrożeniach: Monitorowanie źródeł informacji o zagrożeniach oraz ostrzeżeń rządowych dotyczących podatności sprzętowych i ryzyk związanych z konkretnymi dostawcami.

Lista ostrzeżeń sprzętowych: Utrzymywanie i regularna aktualizacja listy komponentów sprzętowych lub dostawców oznaczonych jako potencjalnie niebezpieczne, aby zapobiec ich wykorzystaniu w organizacji.

PROGRAM ZARZĄDZANIA RYZYKIEM STRON TRZECICH (TPRM)

www.itgrc.pl

BW advisory
Przez naszą wiedzę do Twojej wartości.



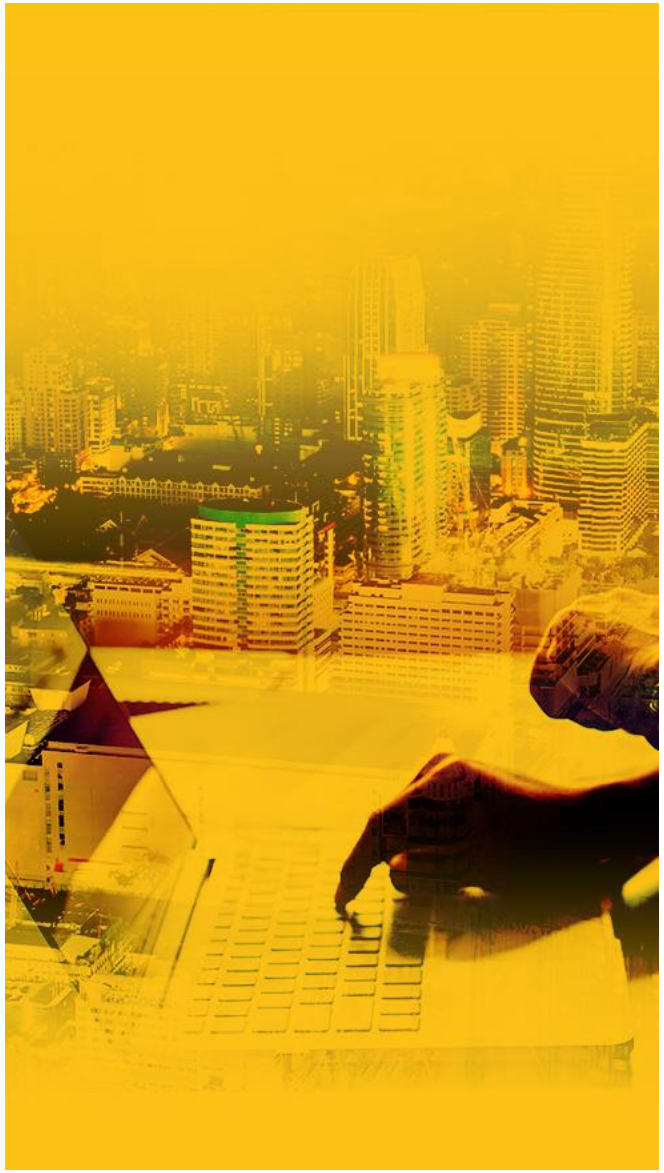
INICJACJA I KLASYFIKACJA RYZYKA

Obowiązki zespołów ds. relacji biznesowych i zarządzania relacjami z dostawcami (VRM) na tym etapie obejmują:

Definicja strategii biznesowej i wymagań
Punktem wyjścia każdej współpracy z podmiotem trzecim jest rozpoznanie potrzeby usprawnienia procesów, rozwiązań lub usług. Może to wynikać z wygasającej umowy lub potrzeby zwiększenia efektywności. Po zidentyfikowaniu konieczne jest jednoznaczne określenie wymagań biznesowych, aby zapewnić ich zgodność z celami organizacji.

Uruchomienie procesu TPRM i określenie ról
Po ustaleniu wymagań kluczowe jest wyznaczenie interesariuszy, często określanych jako „pierwsza linia obrony", odpowiedzialnych za nadzorowanie, identyfikowanie i minimalizowanie ryzyk związanych z zaangażowaniem stron trzecich — ze względu na ich bezpośrednią styczność z wynikami operacyjnymi i ekspozycją na ryzyko.

Wstępna ocena i klasyfikacja ryzyka
Na podstawie rodzaju usług świadczonych przez podmiot trzeci przeprowadzana jest wstępna ocena mająca na celu identyfikację ryzyk wrodzonych. Relacja jest następnie klasyfikowana zgodnie z poziomem ryzyka.



NALEŻYTA STARANNOŚĆ I WYBÓR DOSTAWCY

Zespoły ds. zaopatrzenia, biznesu i relacji z dostawcami (VRM) są odpowiedzialne za działania na tym etapie, w tym dokładną ocenę celów strony trzeciej, nierozstrzygniętych kwestii prawnych, zgodności z przepisami, reputacji w branży oraz praktyk zarządzania ryzykiem.

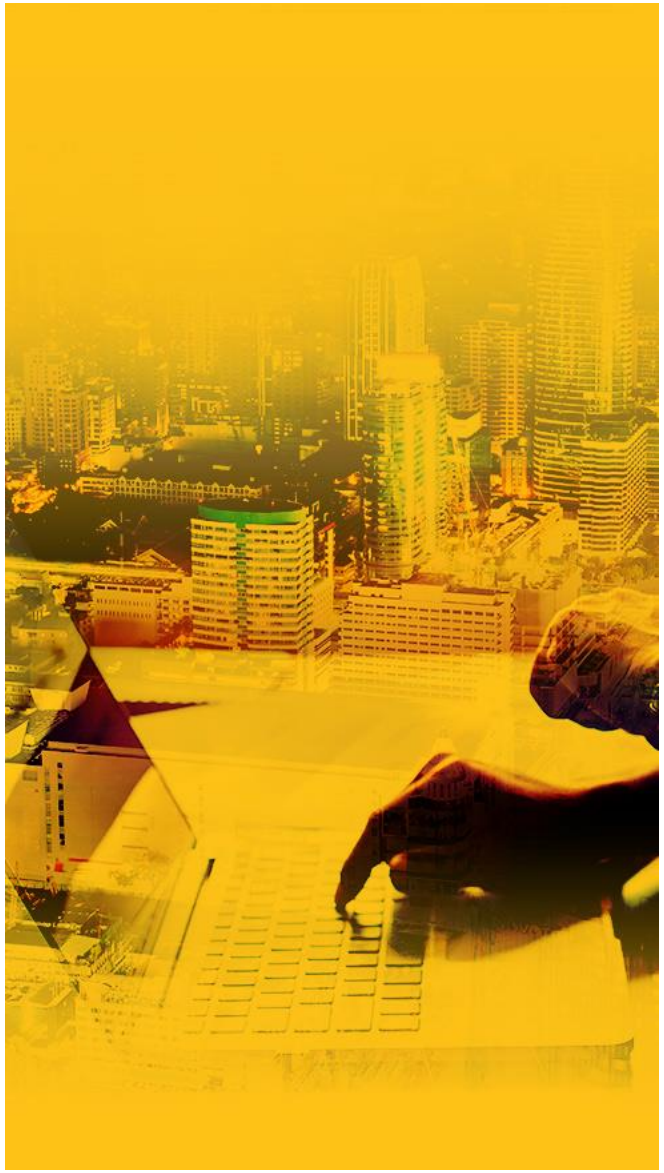
Opracowanie oceny ryzyka dostawców zewnętrznych
Stworzenie kompleksowych ram oceny ryzyka, obejmujących wszystkie kluczowe aspekty niezbędne do oceny zagrożeń związanych z relacjami ze stronami trzecimi.

Przeprowadzenie oceny ryzyka
Przekazanie szablonu oceny ryzyka kluczowym interesariuszom w celu analizy potencjalnych zagrożeń związanych z planowaną współpracą z dostawcą.

Ocena specjalistyczna i raportowanie
Analitycy i menedżerowie ds. ryzyka dokonują przeglądu wyników oceny, opracowując punktacje i kategoryzując ryzyka stron trzecich w odpowiedni sposób.

Wdrożenie środków kontrolnych
Wprowadzenie egzekwowalnych mechanizmów kontrolnych mających na celu ograniczenie, zarządzanie lub eliminację zidentyfikowanych ryzyk.

Wybór dostawcy
Wybór odpowiedniego partnera zewnętrznego ma kluczowe znaczenie, ponieważ może znacząco wpłynąć na działalność organizacji, przekształcając potencjalne zobowiązanie w cenny zasób.



NEGOCJACJE KONTRAKTOWE I WDROŻENIE DOSTAWCY

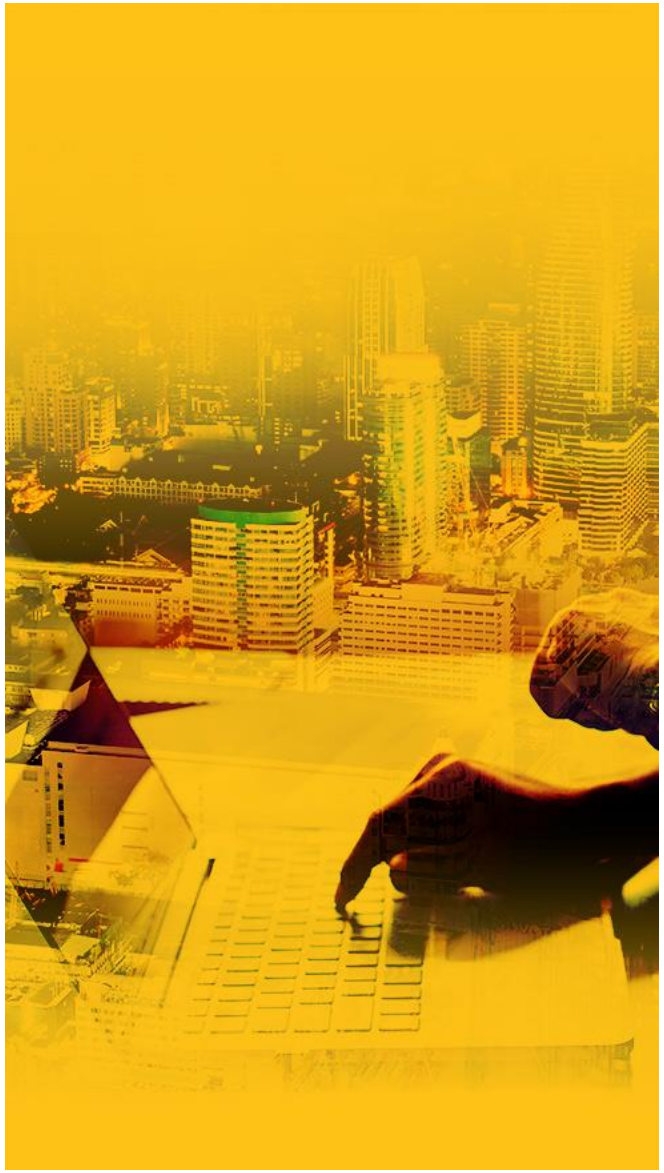
Zespoły prawne, ds. zarządzania umowami, biznesowe oraz VRM nadzorują działania w tej fazie.

Negocjacje kontraktu
Jasne, precyzyjne umowy, pozbawione nadmiernie skomplikowanego języka prawniczego, są kluczowe dla skutecznego zarządzania ryzykiem. Umowy powinny określać zakres współpracy, prawa własności intelektualnej, uprawnienia audytowe, klauzule poufności oraz wymagania dotyczące prywatności danych.

Przegląd ryzyka rezydualnego
Ryzyko rezydualne, czyli pozostałe po wdrożeniu mechanizmów kontrolnych, powinno być okresowo analizowane w celu oceny, czy obecne środki zaradcze są wystarczające.

Zatwierdzenie ryzyka rezydualnego
Najlepszą praktyką jest przegląd i zatwierdzenie poziomu ryzyka rezydualnego przez stronę biznesową po każdej ocenie, w celu podjęcia decyzji, czy potrzebne są dodatkowe kontrole.

Wdrożenie kontraktu
Umowy są integrowane z platformą lub systemem cyfrowym, obejmującym całość dokumentacji dotyczącej ocen dostawców — w tym oceny ryzyka, punktacje, odpowiedzi i wdrożone środki kontrolne.



CIĄGŁE MONITOROWANIE I ZARZĄDZANIE

Biuro Zarządzania Dostawcami (VMO) odpowiada za bieżący nadzór, w tym zgodność kontraktową, kontrolę wydatków oraz zarządzanie relacjami. Zespoły VRM i biznesowe koncentrują się na monitorowaniu i zarządzaniu ryzykiem.

Nadzór nad ryzykiem i jego ograniczanie
Ciągłe monitorowanie ryzyka jest kluczowe, szczególnie w przypadku dostawców o dużym wpływie na działalność, aby wszystkie pojawiające się zagrożenia były niezwłocznie zarządzane.

Zarządzanie cyklem życia kontraktu
Obejmuje wsparcie administracyjne, narzędzia i procesy potrzebne do zarządzania złożonymi aspektami zobowiązań, dostarczanych usług, zmian i kwestii związanych z kontraktami.

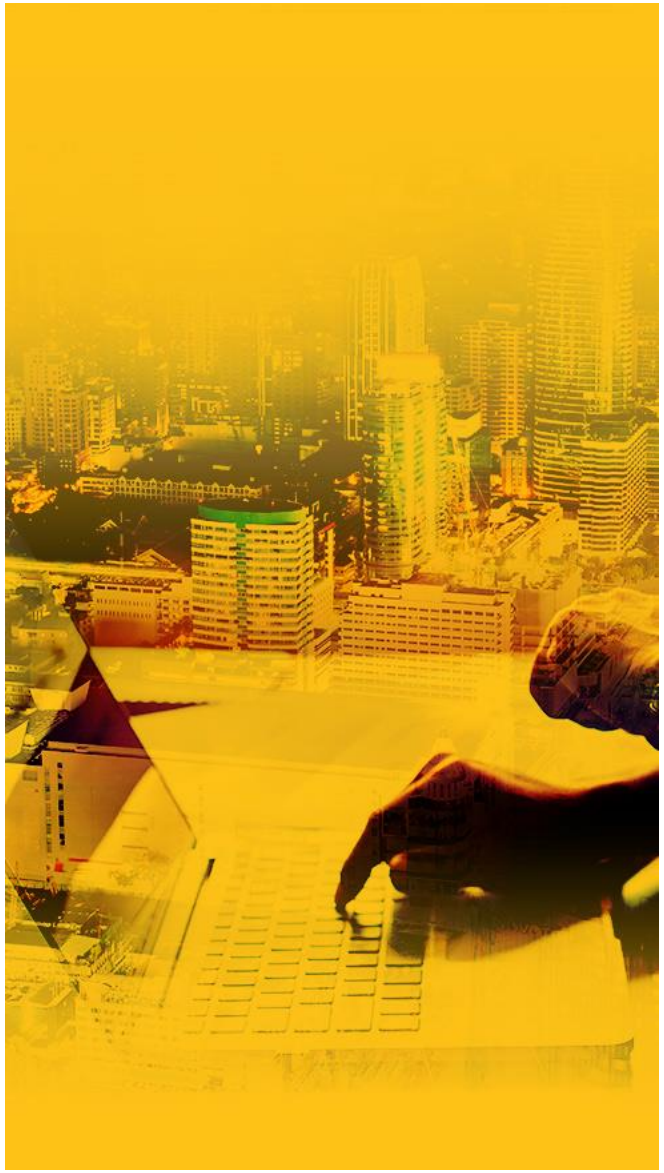
Nadzór nad relacjami
Ułatwia działania nadzorcze na różnych poziomach, tworząc ramy do śledzenia wydajności w odniesieniu do umów SLA (Service Level Agreement) i innych wskaźników.

Zarządzanie wydatkami
Zapewnia zgodność fakturowania z warunkami umowy, w tym stosowanie zatwierdzonych struktur cenowych.

Zarządzanie zakończeniem współpracy
Ustanawia uporządkowany proces zakończenia współpracy z dostawcą — zarówno w przypadku przeniesienia usług do wewnętrznych zasobów organizacji, jak i w sytuacji przejścia do nowego partnera.

TYPOWE PROBLEMY W PROGRAMACH TPRM

BW advisory
Przez naszą wiedzę do Twojej wartości.



Niewystarczająco zróżnicowane wymagania dla różnych kategorii dostawców

Problem:
Często stosuje się jeden zestaw wymagań wobec bardzo zróżnicowanych kategorii dostawców (np. dostawcy centrów danych, usługi SaaS, agencje marketingowe bez dostępu do danych wrażliwych), bez uwzględnienia specyficznego profilu ryzyka każdej z tych grup.

Wpływ:
Takie podejście może prowadzić do: nadmiernych wymagań wobec dostawców niskiego ryzyka, niewystarczającej kontroli nad dostawcami wysokiego ryzyka,
co znacząco ogranicza skuteczność programu TPRM.

Ograniczona możliwość weryfikacji odpowiedzi dostawców na podstawie dowodów

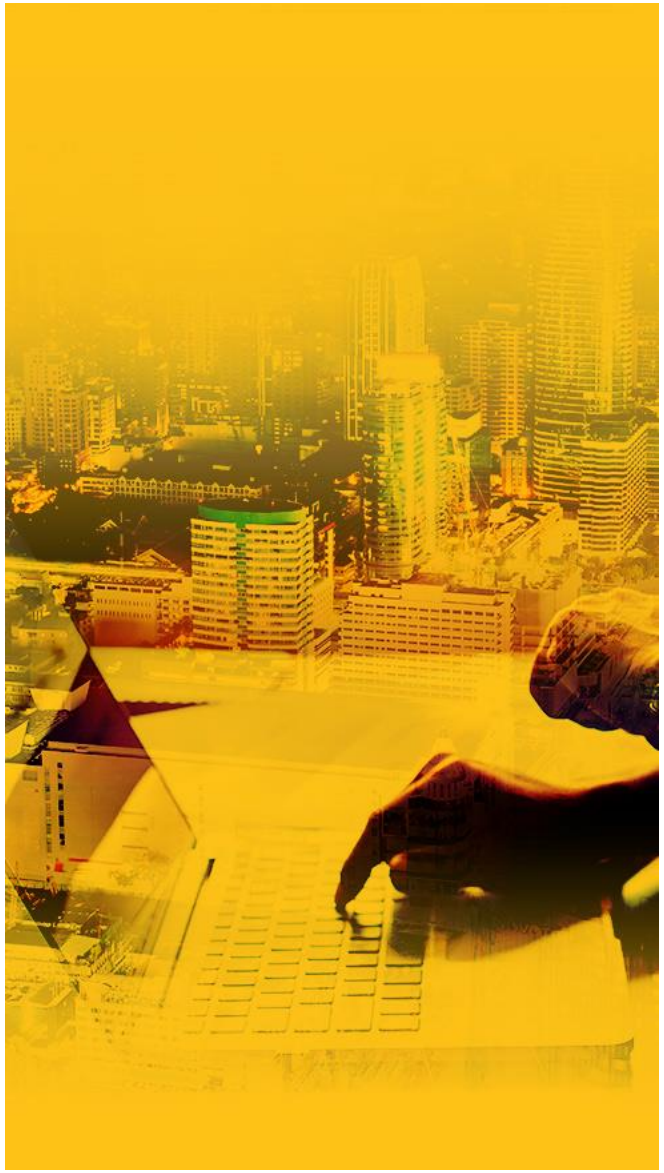
Problem:
Oceny dostawców często opierają się wyłącznie na ich deklaracjach zawartych w kwestionariuszach, bez pozyskiwania odpowiednich dowodów potwierdzających zgodność tych deklaracji z rzeczywistą praktyką.

Wpływ:
Może to prowadzić do fałszywego poczucia bezpieczeństwa, ponieważ deklaracje dostawcy mogą nie odzwierciedlać jego rzeczywistego poziomu zabezpieczeń.

Brak dopasowania odpowiedzialności Biura Zarządzania Dostawcami (VMO)

Problem:
Biuro VMO odpowiada za zbieranie informacji od dostawców, ale może nie posiadać odpowiednich kompetencji do ich szczegółowej oceny lub nie traktować tego jako elementu swojej odpowiedzialności.

Wpływ:
Może to skutkować niepełnymi lub powierzchownymi ocenami, ponieważ VMO może nie ponosić pełnej odpowiedzialności za jakość i dokładność analizowanych odpowiedzi.



Podejście zorientowane na zgodność zamiast na rzeczywiste bezpieczeństwo

Problem:
Programy TPRM często koncentrują się na spełnianiu wymogów formalnych (compliance), zamiast na faktycznym bezpieczeństwie. Główny nacisk kładzie się na dokumentację, a nie na weryfikację wdrożenia i skuteczności mechanizmów kontrolnych.

Wpływ:
Prowadzi to do tzw. „odhaczania punktów kontrolnych" — gdzie wymogi są spełnione na papierze, ale realne praktyki bezpieczeństwa pozostają nieweryfikowane, co stwarza ryzyko poważnych luk w zabezpieczeniach.

Nieskuteczne narzędzia weryfikacyjne

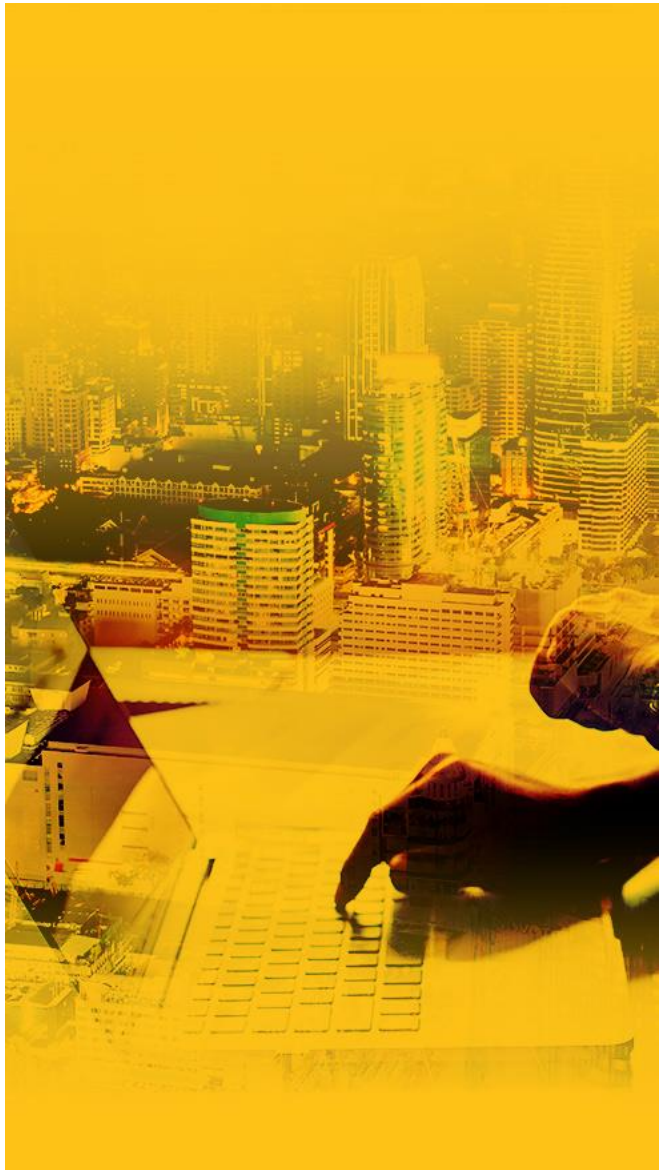
Problem:
Wiele programów TPRM nadal polega na arkuszach Excel lub papierowych/elektronicznych kwestionariuszach do przeprowadzania ocen dostawców. Metody te są nieefektywne i nie zapewniają pełnego obrazu ryzyka.

Wpływ:
Ogranicza to dokładność i głębokość ocen, utrudnia śledzenie zmian w czasie i porównywanie odpowiedzi, a także zwiększa ryzyko przeoczenia istotnych zagrożeń.

Brak jasno określonych praw audytowych i dostępu dla audytorów

Problem:
Programy TPRM często nie zawierają precyzyjnych wymagań dotyczących praw audytowych – nie wiadomo, do jakich danych i systemów audytorzy mają mieć dostęp podczas audytów dostawców przeprowadzanych w imieniu klienta.

Wpływ:
Taka niejasność ogranicza skuteczność audytu, ponieważ audytorzy mogą mieć utrudniony dostęp do kluczowych informacji, co obniża wartość audytu i możliwość wykrycia realnych zagrożeń.



Brak jasno określonych wymagań dotyczących bezpieczeństwa, prywatności i ciągłości w umowach

Problem:
Umowy mogą nie zawierać precyzyjnych kryteriów dotyczących bezpieczeństwa, prywatności i ciągłości działania, ani listy konkretnych mechanizmów kontrolnych, które dostawca musi wdrożyć.

Wpływ:
Utrudnia to egzekwowanie standardów bezpieczeństwa i monitorowanie zgodności, ponieważ dostawca nie ma określonych wytycznych, których musi przestrzegać.

Brak potwierdzenia od dostawcy wdrożenia wymaganych kontroli

Problem:
Dostawcy często nie są zobowiązani do dostarczenia dowodów na wdrożenie mechanizmów kontroli bezpieczeństwa, prywatności i ciągłości, określonych w umowie.

Wpływ:
Brak takiego potwierdzenia oznacza brak pewności, że wymagania zostały rzeczywiście spełnione, co pozostawia potencjalne luki w zabezpieczeniach.

Brak bieżącej widoczności środowiska kontrolnego dostawcy po podpisaniu umowy

Problem:
Po podpisaniu umowy organizacje często tracą możliwość monitorowania zmian w środowisku kontrolnym dostawcy.

Wpływ:
Brak ciągłego nadzoru może prowadzić do niezidentyfikowanych zagrożeń, ponieważ zmiany w postawie bezpieczeństwa dostawcy mogą pozostać niezauważone, co naraża bezpieczeństwo, prywatność i ciągłość działania.

MODEL KOMPETENCYJNY
WIEDZA UMIEJĘTNOŚCI POSTAWY

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

AW2.0
AUDYT WEWNĘTRZNY

BW advisory
Przez naszą wiedzę do Twojej wartości.

C&F

Ministerstwo
Finansów

03 Zarządzanie ryzykiem dostawców

01 *Wyzwania*

FAKTY NA ŚCIANIE PŁACZU

Photographer: NASA via Getty Images

Business

NASA Says Metals Fraud Caused $700 Million Satellite Failure

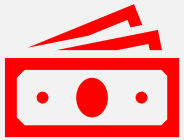
By David Stringer

May 1, 2019, 3:34 AM GMT+2

Updated on May 1, 2019, 11:53 AM GMT+2

KONSEKWENCJE

Utrata reputacji



Kary za brak zgodności

Odpowiedzialność prawna

Zaburzenia w prowadzeniu biznesu

FAKTY NA ŚCIANIE PŁĄCZU

ZADANIE: Uruchomienie platformy internetowej zdolnej do liczenia głosów z ponad 25 tys. komisji wyborczych (31 mln możliwych głosów).

KRYTERIA WYBORU DOSTAWCY: najniższa cena.

CZAS ROZWOJU: bardzo krótki.

PROFIL RYZYKA DOSTAWCY: nieprzygotowany.

- **WYNIK:**
- **System wygenerował błędne dane, a później... uległ awarii (przeciążeniu).**

- **WPŁYW:**
- **Ogłoszenie wyników opóźniło się o kilka dni.**
- **Ogromny skandal społeczny i polityczny.**
- **Firma sprzedająca zbankrutowała.**

https://niezalezna.pl/85801-spowodowali-chaos-wyborczy-nabino-i-romuald-d-maja-pokryc-szkody-awarii

DLACZEGO POTRZEBUJEMY DOSTAWCÓW?

KLUCZOWE CZYNNIKI

DLACZEGO POTRZEBUJEMY DOSTAWCÓW?

500 tys osób

92% dostawcy, ok 400 podmiotów

https://news

DLACZEGO POTRZEBUJEMY DOSTAWCÓW?

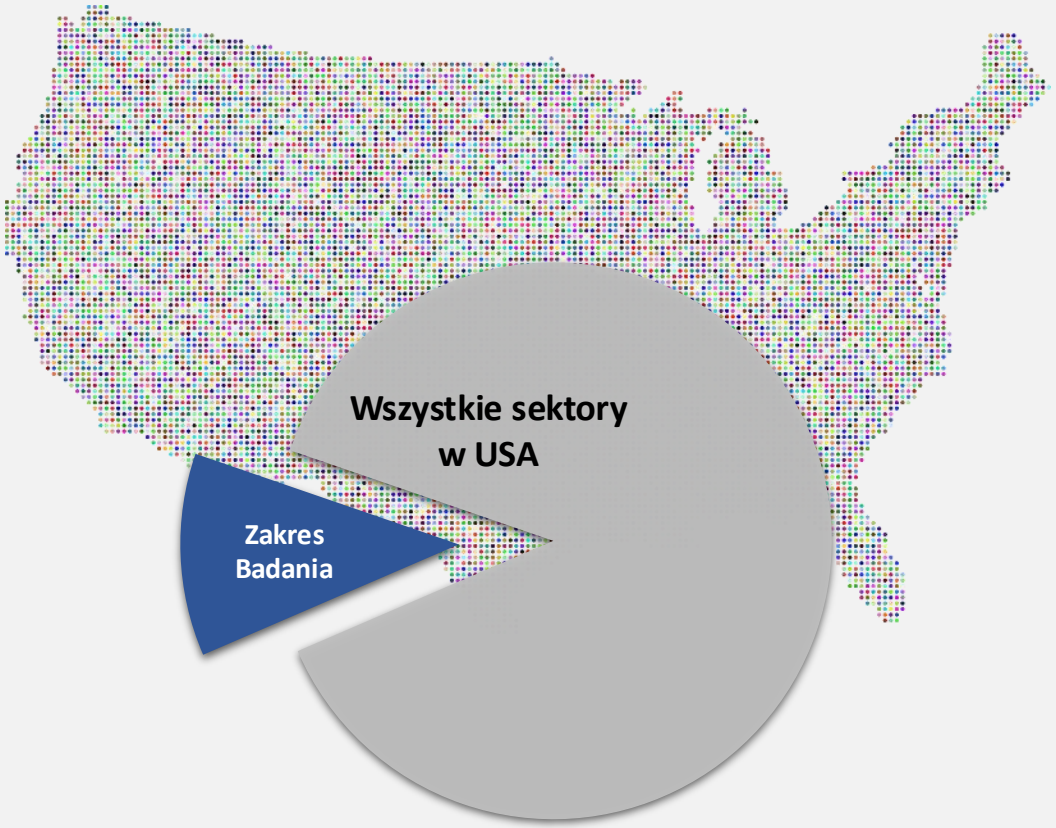
~80M
~~100M~~
Telefonów

SAMSUNG

+$9
~~+$11~~
Miliardów

*) Szczegółowe statystyki nie są dostępne. Szacunkowe wyniki przygotowane w oparciu o różne źródła informacji.

BADANIE W USA DOTYCZĄCE RYNKU NA USŁUGI GRC/TPRM



Mniej niż 12%

~30% 😟

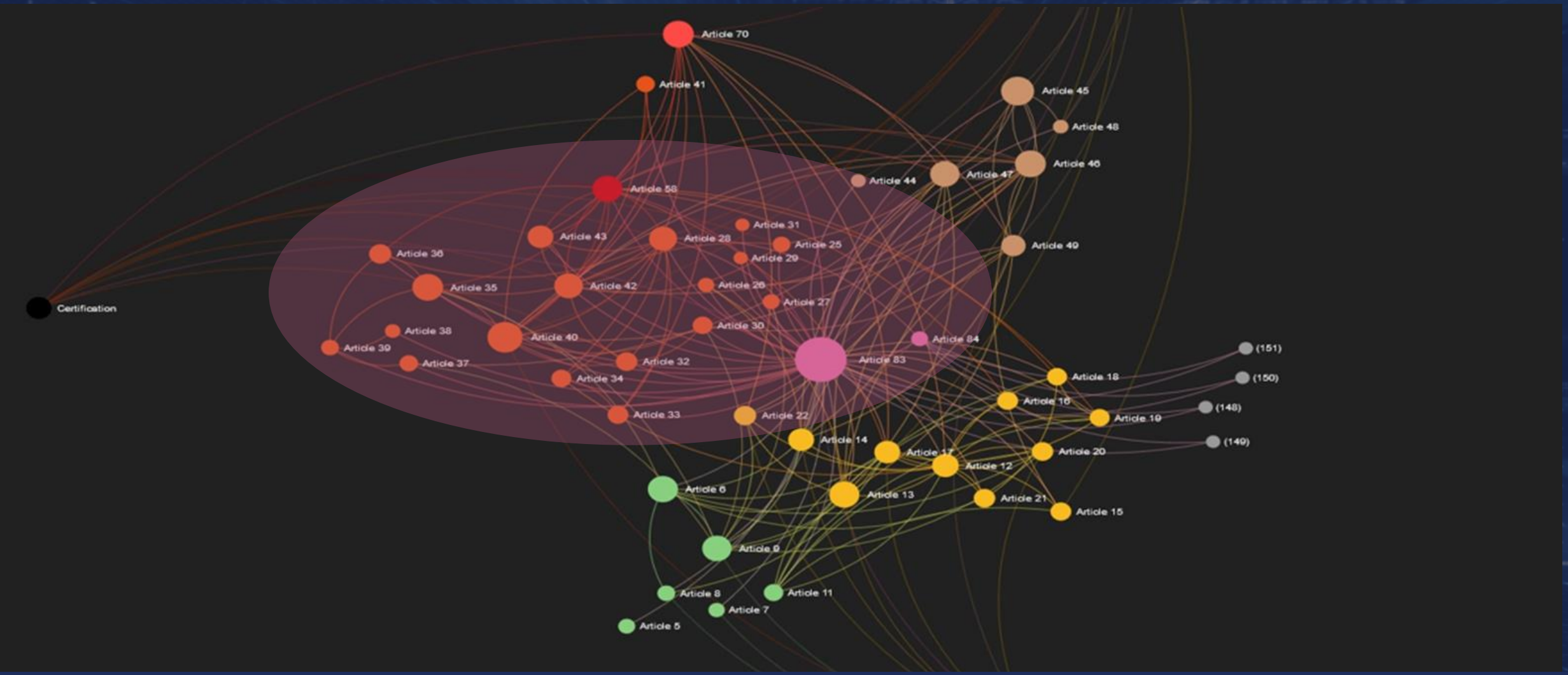
WYBRANE WYZWANIA

Perspektywa operacyjna

KTO WIE, CO TO ZA SIEĆ

Artykuł 83 ”Ogólne warunki nakładania kar administracyjnych"

RODO


Article 70
Article 41
Article 45
Article 48
Article 46
Article 47
Article 44
Article 58
Article 31
Article 43
Article 28
Article 25
Article 29
Article 49
Article 36
Article 35
Article 42
Article 26
Article 27
Certification
Article 38
Article 30
Article 84
Article 40
Article 39
Article 37
Article 32
Article 83
Article 34
(151)
Article 18
(150)
Article 16
(148)
Article 19
Article 33
Article 22
Article 14
(149)
Article 17
Article 20
Article 12
Article 6
Article 13
Article 21
Article 15
Article 9
Article 8
Article 11
Article 7
Article 5

RODO

Artykuł 83 ”Ogólne warunki nakładania kar administracyjnych"

02

Rekomendowane kroki do efektywnego zarządzania dostawcami

CYKL ŻYCIA DOSTAWCY

POTENCJALNA ŚCIEŻKA DLA ODWAŻNYCH…

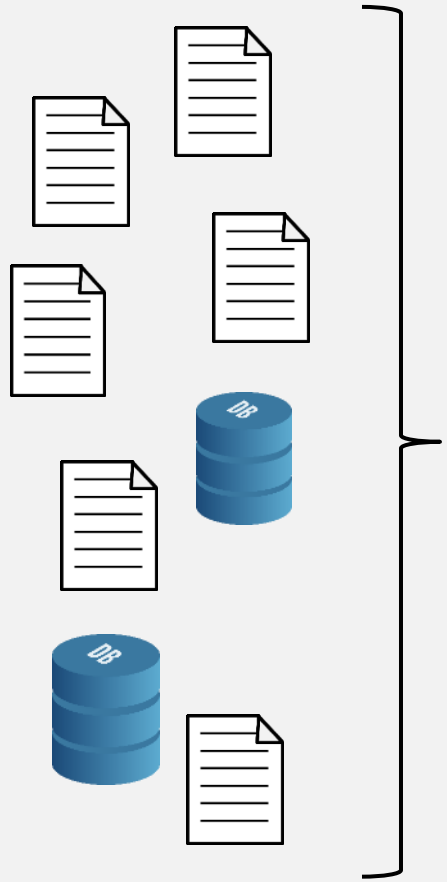
8 KROKÓW

DO EFEKTYWNEGO ZARZĄDZANIA DOSTAWCAMI

Jan Anisimowicz (PMP, CISM, CRISC)

STWÓRZ LISTĘ DOSTAWCÓW

KROK 1



ŹRÓDŁA WEWNĘTRZNE

TIP 1

Czasem to działanie byłoby łatwiejsze do zrealizowania w ramach Projektu Konsolidacji Dostawców (racjonalizacji kosztów w organizacji)

Nazwa dostawcy	Kontakt	Email	Adres	(...)
AdaptiveGRC SA	...	...	...	...
IT ADVISORY SP Zoo	...	...	...	...
C&F SA	...	...	...	...

TIP 2

Pomocne byłoby posiadanie podobnych informacji o wszystkich dostawcach

STWÓRZ LISTĘ USŁUG

KROK 2

- **Outsourced business functions**
  (IT services, Accounting, cleaning service)
- Subcontracting
- Data hosting
- Data processing
- System Maintenance
- Pizza delivery service
- Cloud applications
- Transportation
- Facilities Management
- And many, many more …

TIP 3

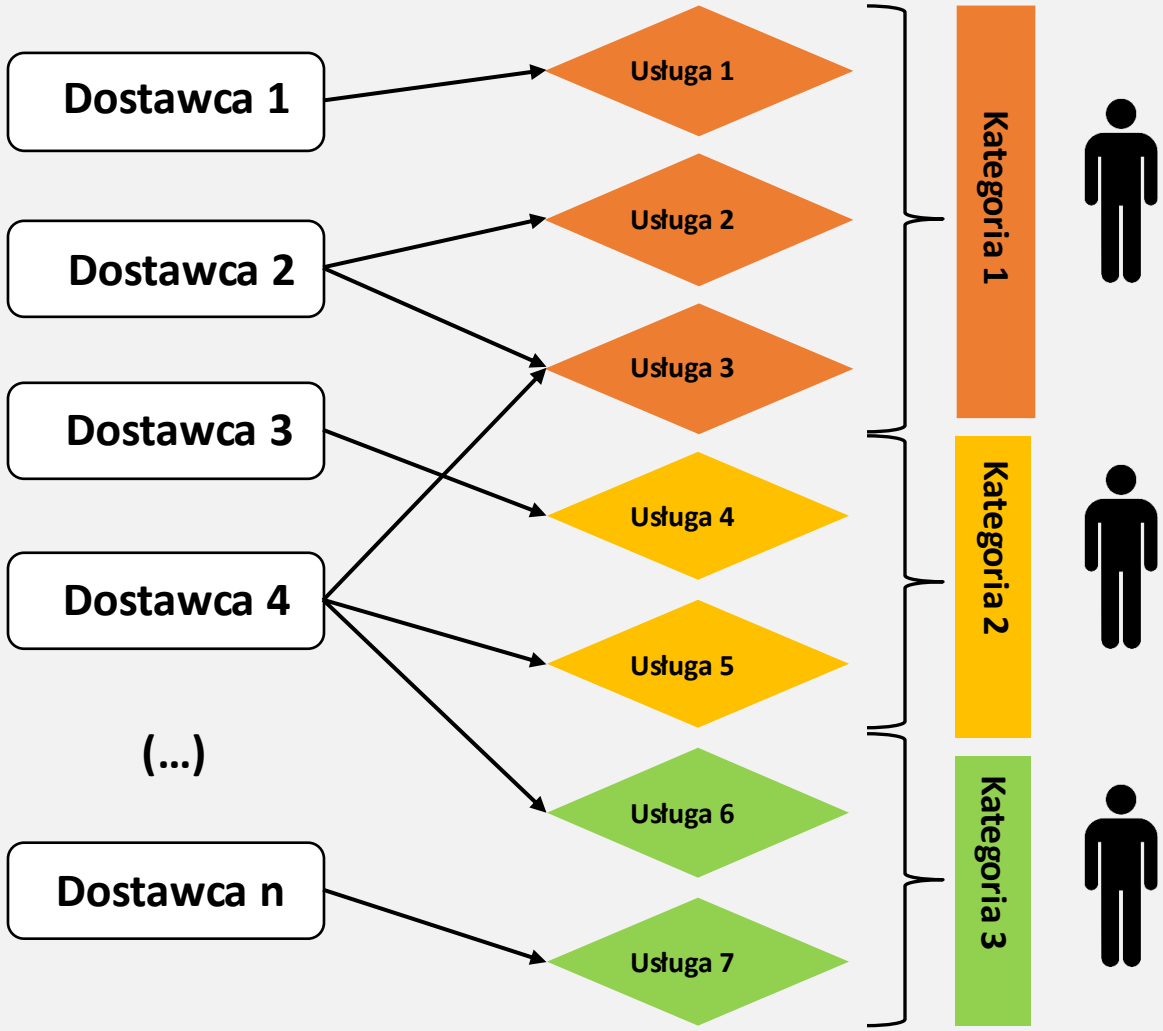
W dłuższej perspektywie korzystne dla organizacji byłoby posiadanie hierarchii usług

TIP 4

Przydatne byłoby przypisanie priorytetu dla usługi dla organizacji

ZARZĄDZAJ RELACJAMI: DOSTAWCY I USŁUGI

KROK 3

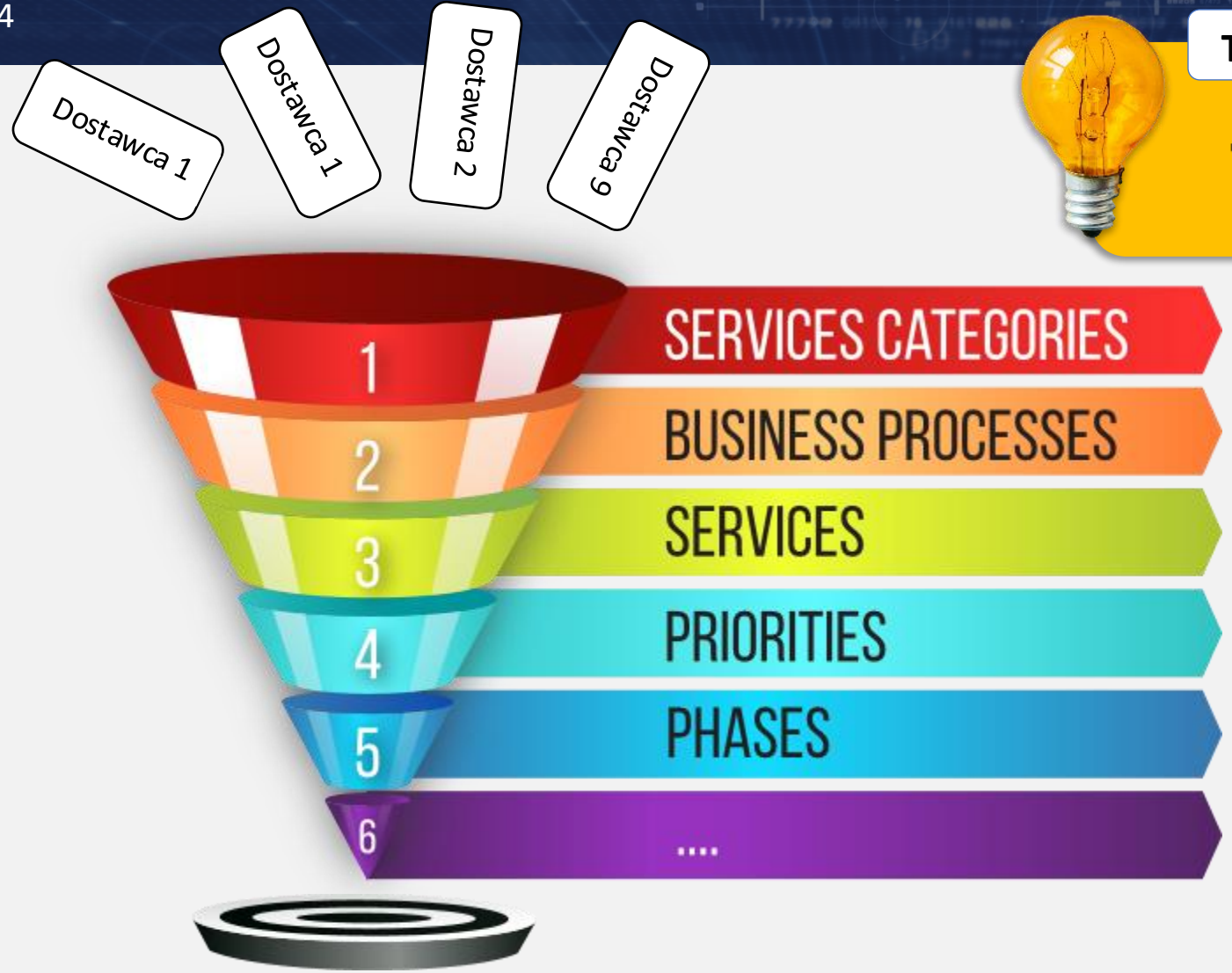


TIP 5

Na podstawie kategoryzacji można przypisać odpowiedzialność biznesową różnym współpracownikom w organizacji (lepszy proces akceptacji).

ZWERYFIKUJ CZY TWORZYĆ PROFIL RYZYKA

KROK 4



TIP 6

Kryteria filtrowania powinny być zharmonizowane w organizacji. Bez wyjątków.

STWÓRZ PROFIL RYZYKA

STEP 5

RYZYKO USŁUGI:

- ★ Ryzyko zgodności z przepisami i ryzyka regulacyjne związane z usługą
- ★ Wpływ na klienta i finanse
- ★ Poziom krytyczności usługi świadczonej przez dostawcę dla naszej firmy
- ★ Przetwarzane transakcje finansowe
- ★ W grę wchodzą dane osobowe i wrażliwe?
- ★ Dojrzałość usługi?...

RYZYKO DOSTAWCY:

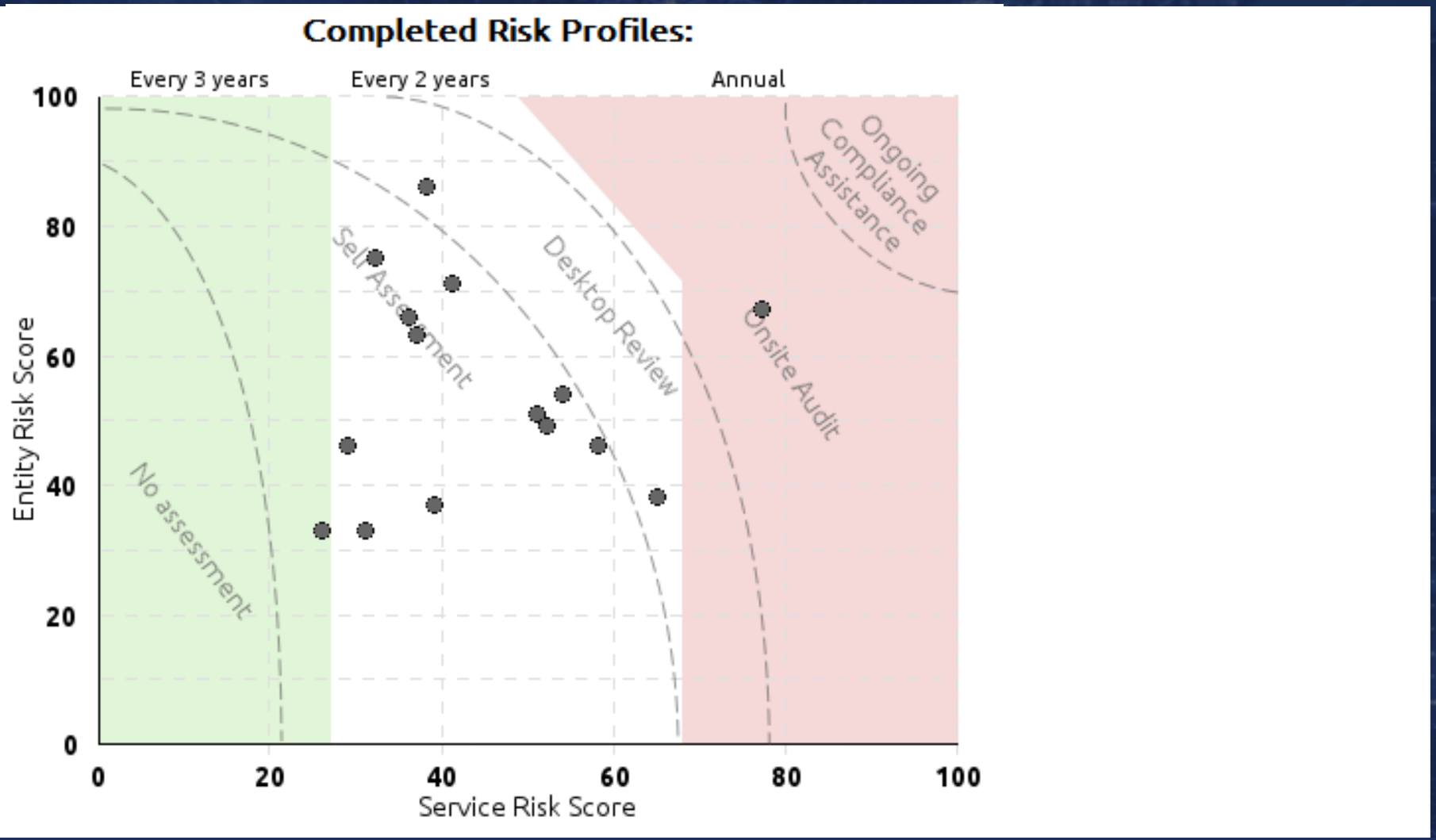
- ★ Lokalizacja dostawcy
- ★ Znane zdarzenia związane z bezpieczeństwem
- ★ Wielkość firmy
- ★ Sytuacja finansowa
- ★ Historia występów
- ★ ...

TIP 7

Musisz wykorzystać wiedzę dostępną w Twojej organizacji (Ważne). Możesz wzbogacić dane o dodatkowe źródła informacji (takie jak D&B, Bisnode itp.)

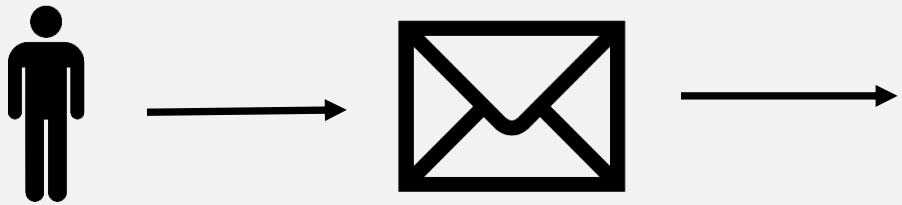
STWÓRZ PROFIL RYZYKA

KROK 5 PRZYKŁAD

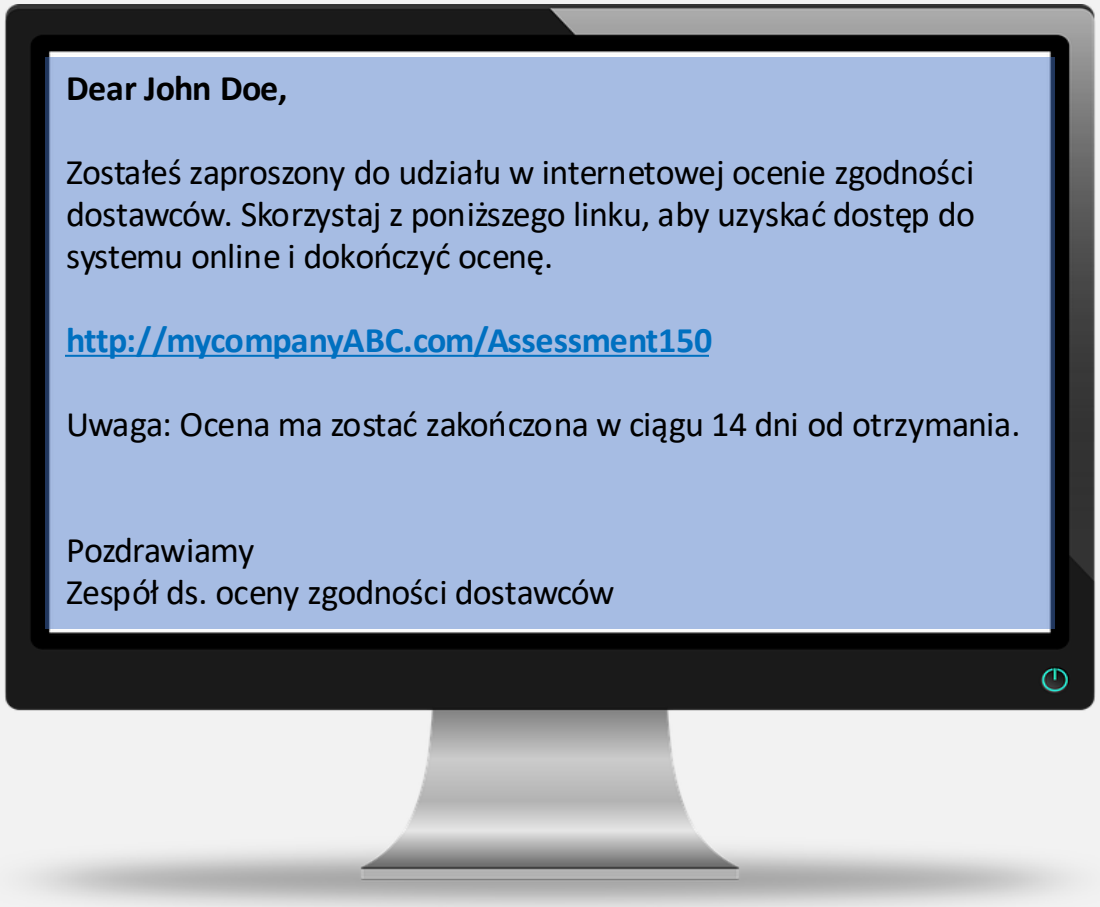


ZWERYFIKUJĄ DOSTAWCĘ ZA POMOCĄ ŚRODKÓW ELEKTRONICZNYCH

KROK 6



Dostawca



WYNIK BADANIA

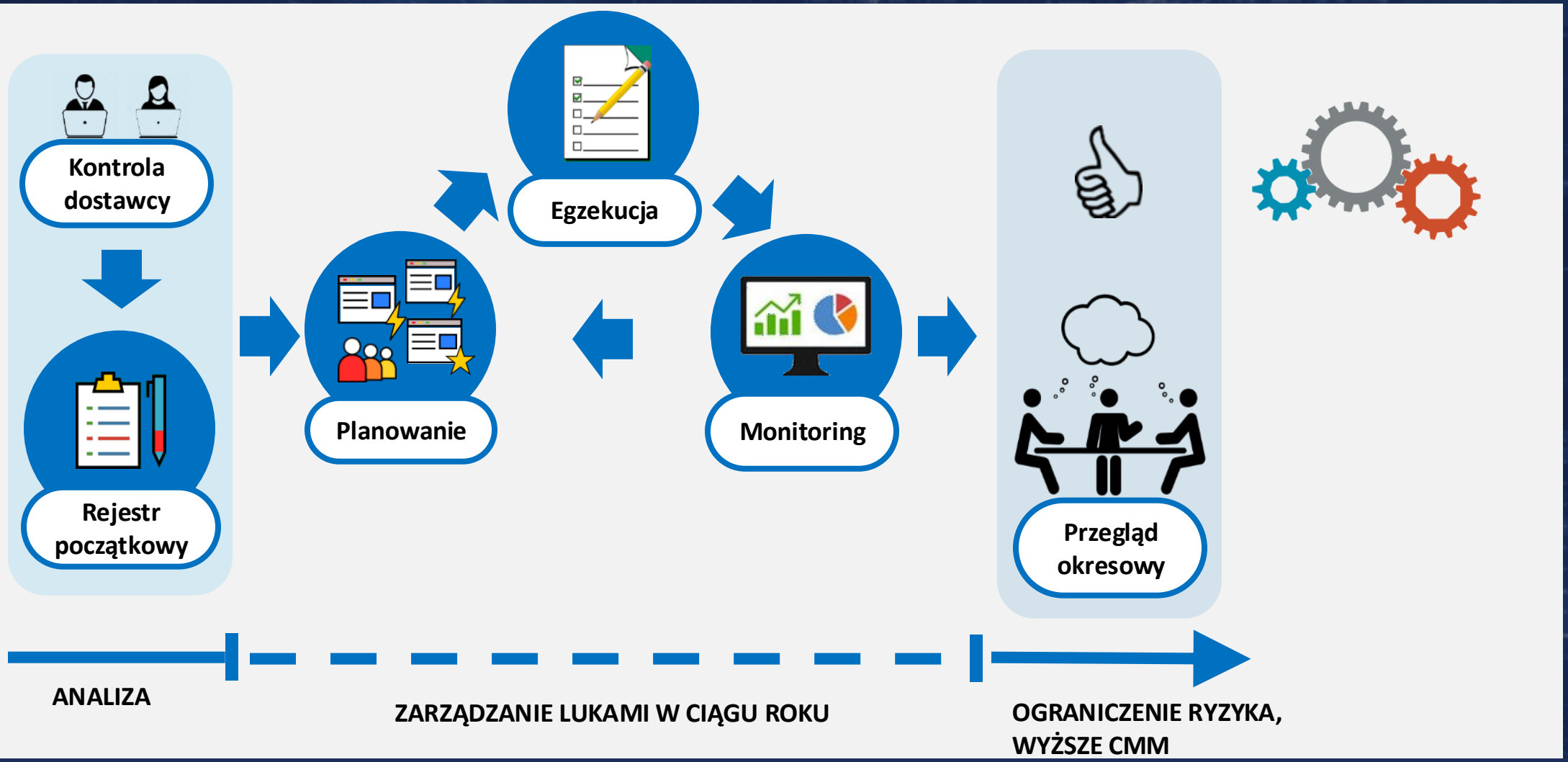
KROK 6

Preview Assessment results

Objective Id	Activity Group Parent	Activity Group	Compliance Objective	Risk Rating	Response
COB101	Information Protection	Media Security	Whenever physical media containing sensitive or regulated data is moved between locations, a movement log must track and verify that the media safely reaches the required destination and custodian.	Critical	Yes
COB141	Information Protection	Incident Management	All reported events must be captured in a secure incident log or incident management system with the following information: • date and time of event • location, systems and information affected • disposition of event: classified as incident or non-incident with rationale • containment, notification and recovery outcomes. • the information/data owner	Very High	Yes
COB120	Information Protection	Information Security Management	The organization must have a documented Information Security policy. The contents of the policy includes (but is not limited to): - The identification of a single individual as the head of Information Security, with overall accountability for delivery of the information security objectives. - The organizations high-level commitment, sponsorship and strategy to assure the ongoing protection of information. - A commitment to assure that information security training is provided to all appropriate resources.	Critical	No
COB121	Information Protection	Information Security Management	The security policy of the Service Organization must state that networks are required to be protected from unauthorized access and also identify the network availability requirements. The network availability and integrity requirements must comply with prevailing contractual and regulatory requirements.	Critical	Partial
COB124	Information Protection	Data Exchange	All software and data imports from a non trusted source must be checked for viruses and verified as clean before being made available in the organizations network or systems.	Critical	No
COB126	Information Protection	Information Security Management	Normal operational access privileges to workstations must prevent unauthorized software from being installed. Unauthorized software includes, but is not limited to, any software that can facilitate unauthorized access into any part of the organizations network. Installation of software without a valid software license is also prohibited.	Very High	Yes

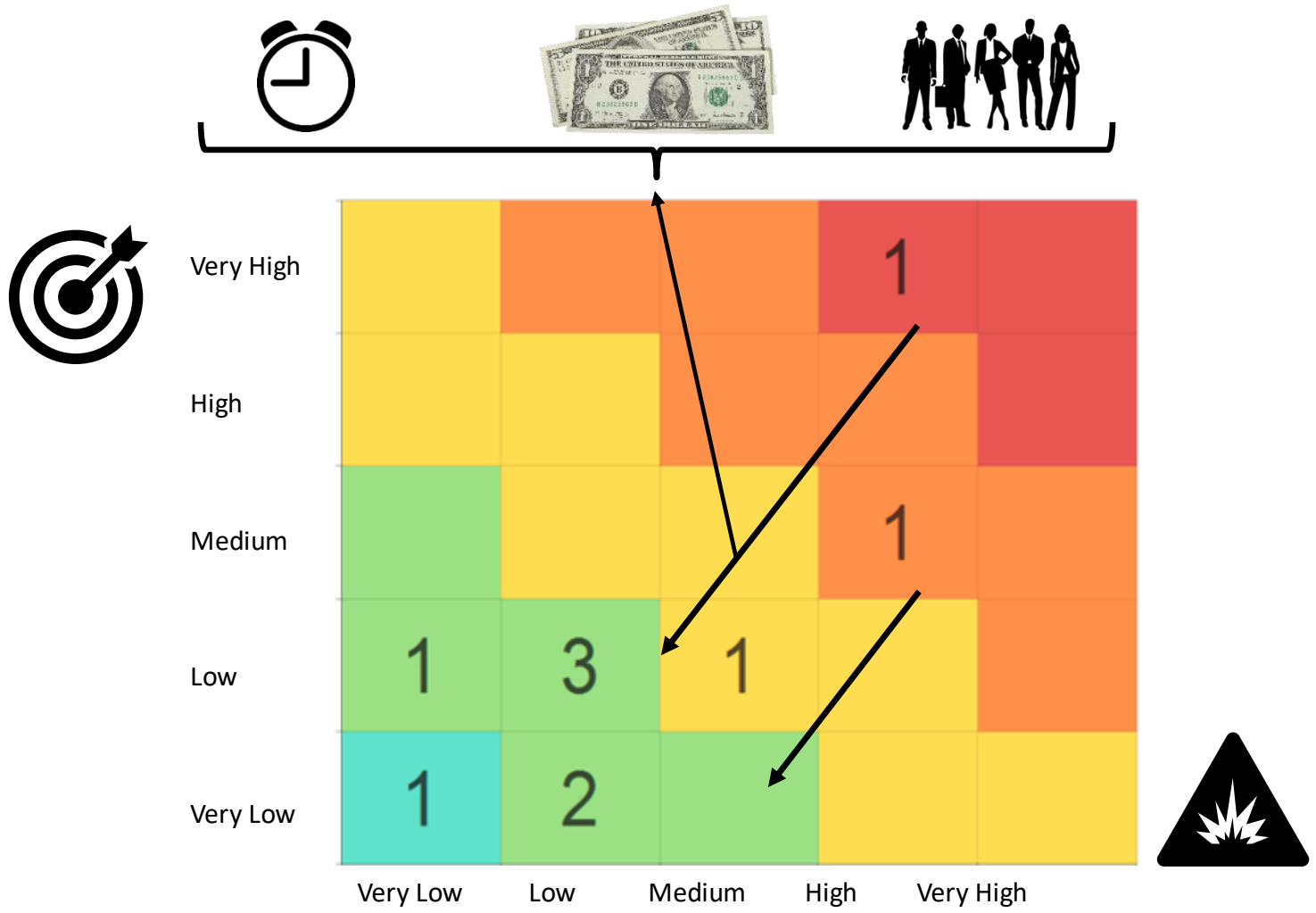
ZARZĄDZANIE LUKAMI I USTALENIAMI

KROK 7

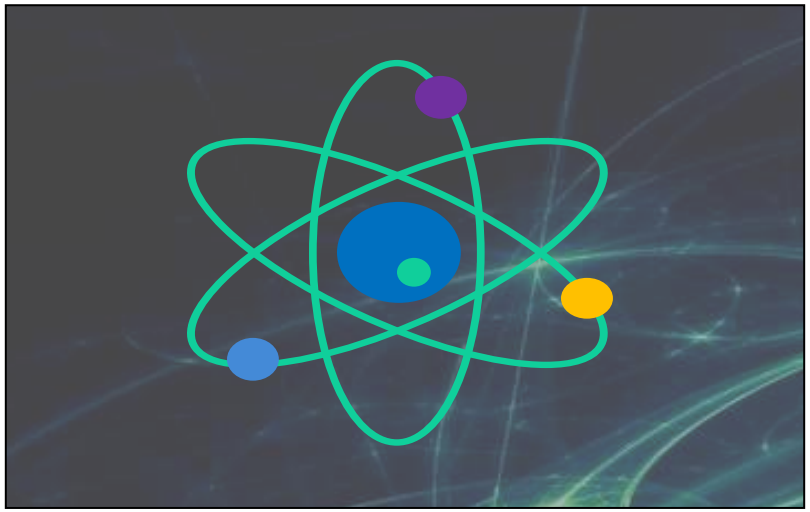


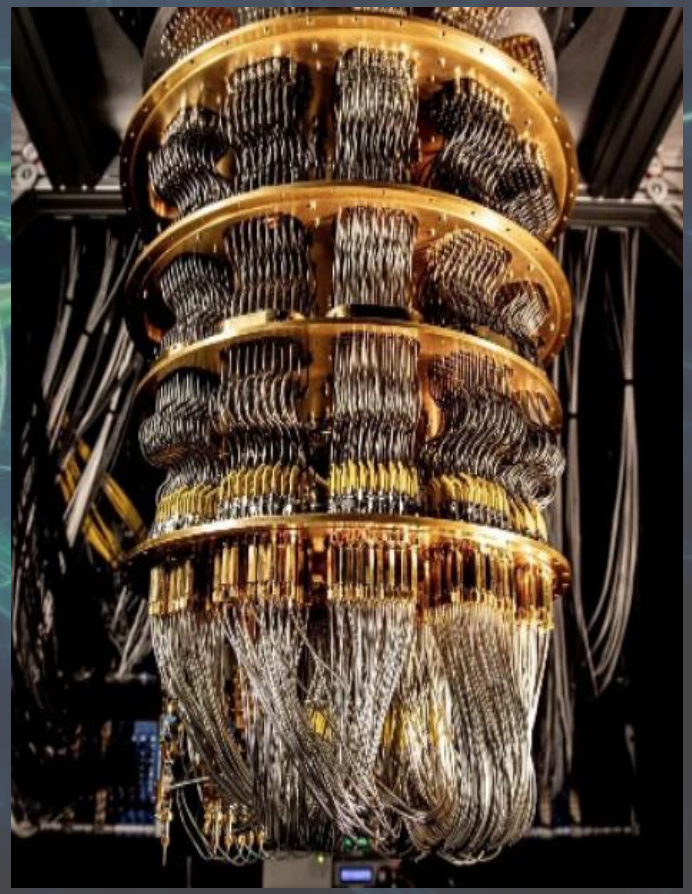
OGRANICZANIE RYZYKA W STOSUNKU DO ZIDENTYFIKOWANYCH USTALEŃ

KROK 8



04 Przyszłość: Wykorzystanie QC i blockchain





Moc: 2^n

n – Liczba qubitów

20 Qubitów - 1M stanów równocześnie

21 Qubitów - 2M stanów równocześnie


ANGRY BIRDS

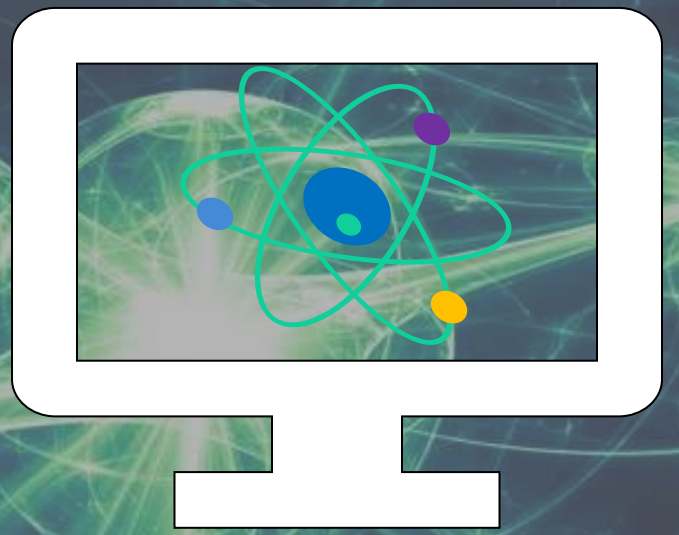
Komputer Klasyczny

Analizuje bibliotekę parametrów, weryfikowaną na podstawie zdefiniowanego oprogramowania (deterministyczne reguły i algorytmy)

Komputer Klasyczny

Analizuje bibliotekę parametrów, weryfikowaną na podstawie zdefiniowanego oprogramowania (deterministyczne reguły i algorytmy)

Komputer Kwantowy



Równoległa analiza wszystkich stanów wybór optymalnego

Ważna informacja!

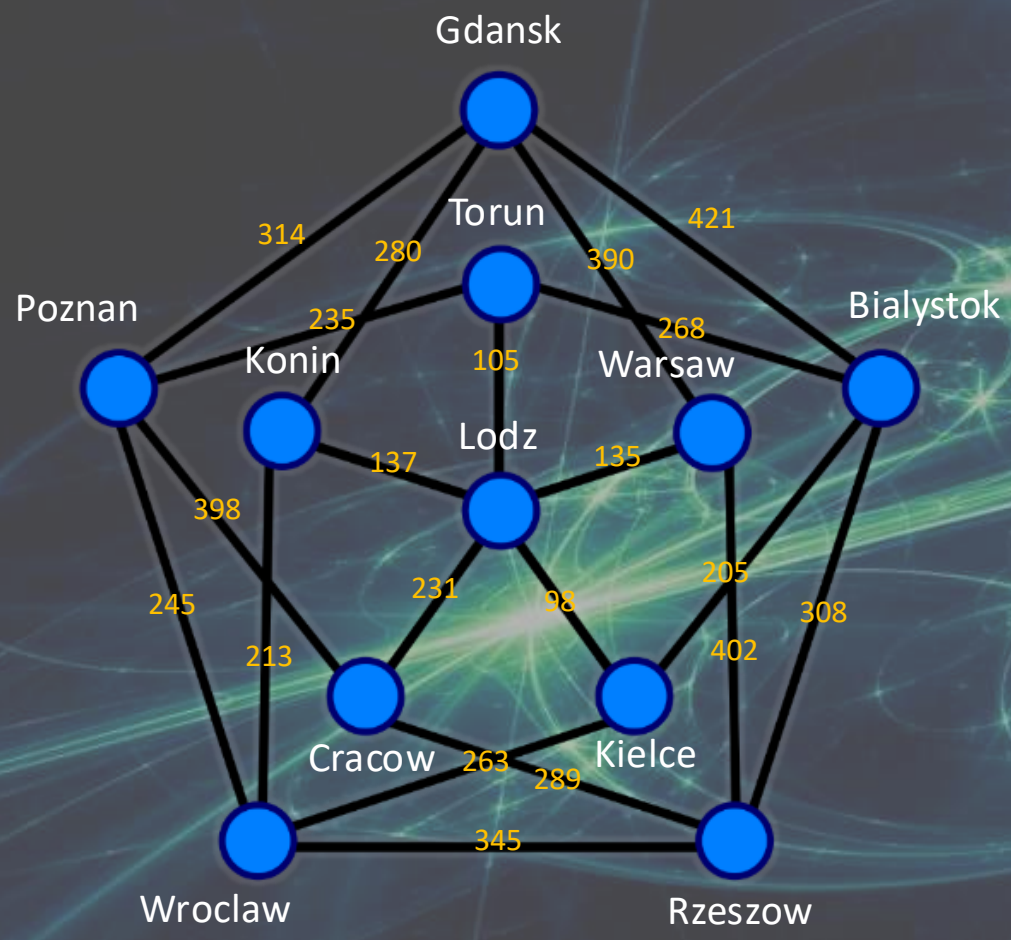
Obszar problemu do rozwiązania

Komputery kwantowe

KOMPUTERY KLASYCZNE

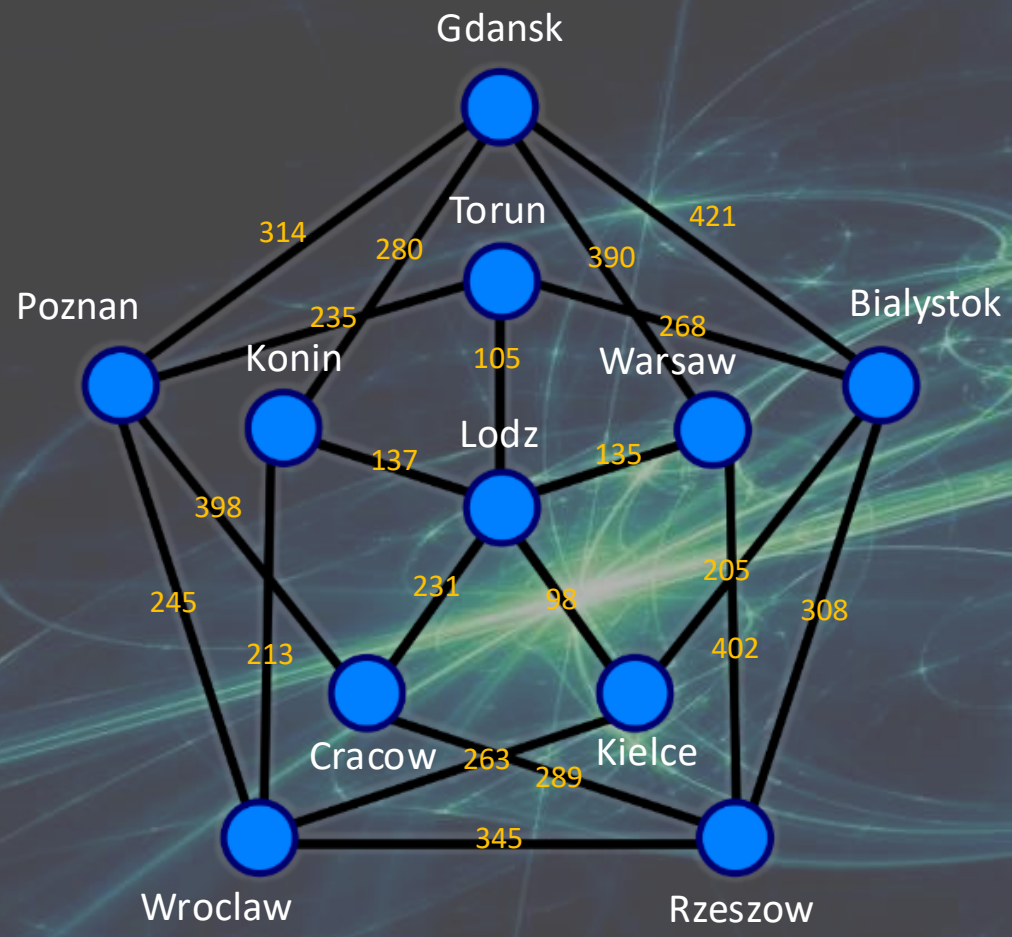

EVERGREEN

Zagadnienie planowania transportu



- Miasta są połaczone
- Komiwojażer może odwiedzić miasto tylko raz
- Cel: Minimalny koszt

Zagadnienie planowania transportu



- 20 Miast (n=20)
- Liczba kombinacji

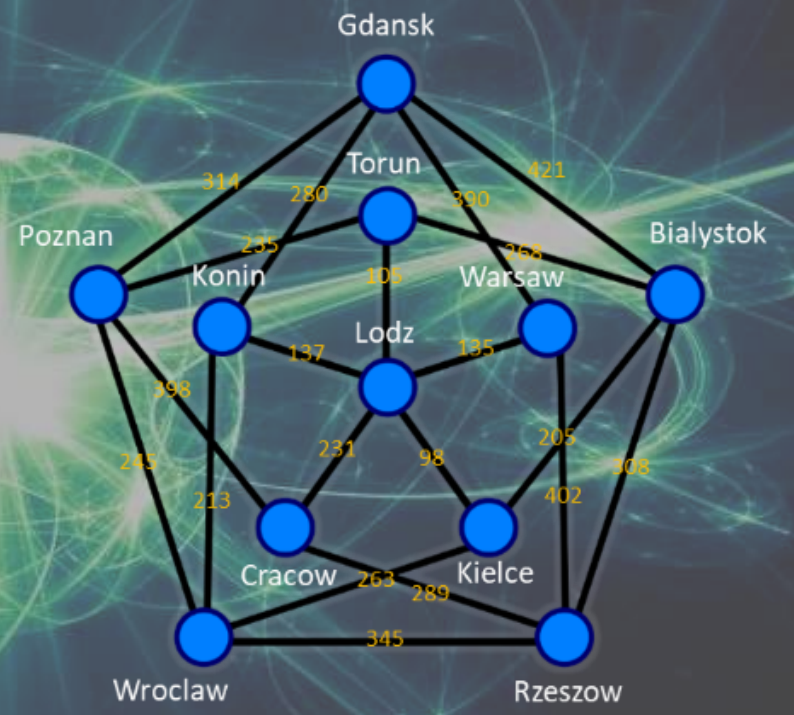
$(n-1)!/2 =$ 60 822 550 204 416 000

Zagadnienie planowania transportu

- 20 miast (n=20)
- Liczba kombinacji= (n-1)!/2
- 60 822 550 204 416 000

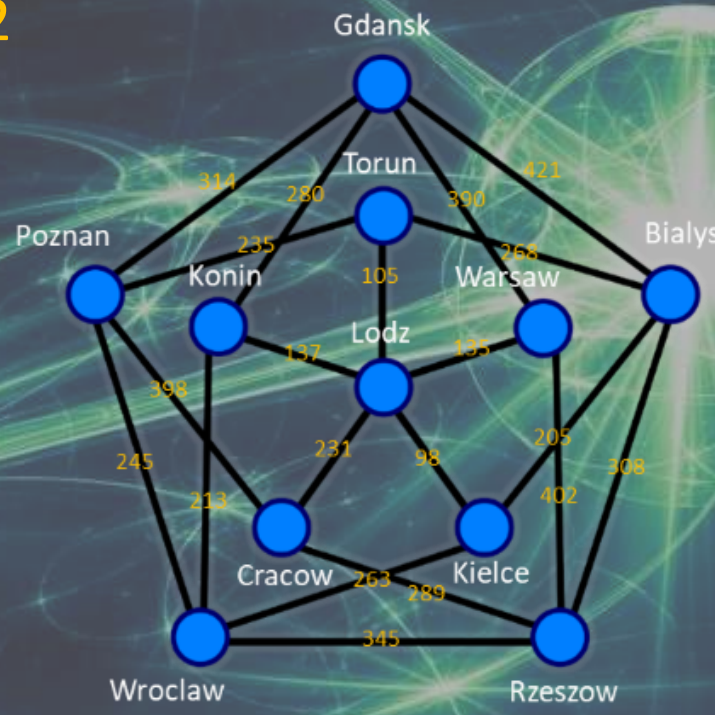
- Komputer klasyczny
- 1 Miliard op/sek,
- Czas: ok. 69 dni

- **Komputer Kwantowy**
- **1 op/sek, 57 qubitów**
- **Czas: Kilka minut (*)**



Zagadnienie planowania transportu

- 20 miast (n=20)
- Liczba kombinacji= (n-1)!/2
- 60 822 550 204 416 000



25 miast?

- Komputer klasyczny
- 1 Miliard op/sek,
- Czas: ok. 69 dni

Klasyczny
250.000 years

- **Komputer Kwantowy**
- **1 op/sek, 57 qubitów**
- **Czas: Kilka minut (*)**

Kwantowy
83 qubits
Czas: Kilka minut (*)

MODEL KOMPETENCYJNY
WIEDZA UMIEJĘTNOŚCI POSTAWY

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

AUDYT WEWNĘTRZNY

BW advisory
Przez naszą wiedzę do Twojej wartości.

C&F

Ministerstwo
Finansów

Blockchain i wykorzystanie do śledzenia transportu

Blockchain – kluczowe cechy

Blockchain zapewnia:

- **niezmienność** danych – brak możliwości fałszowania historii zdarzeń
- **przejrzystość** – każdy uczestnik widzi te same, wiarygodne dane
- **rozproszony dostęp** – brak jednej, centralnej instytucji

Jakie daje możliwości:

- **Śledzenie pochodzenia produktów (traceability)**
- **Zarządzanie certyfikatami i zgodnością (compliance)**
- **Zautomatyzowane rozliczenia i płatności (Smart kontrakty)**
- **Zwalczanie podróbek i nadużyć**
- **Wspólna platforma danych dla konkurujących firm**

Blockchain – przykład wsparcia łańcuch dostaw

- Rolnik zbiera i oznacza ziarna RFID
- Zrzeszenie producentów rejestruje certyfikat jakości
- Eksporter zapisuje dane o eksporcie i kontenerze
- Czujniki IoT w kontenerze logują temperaturę, wilgotność – dane przesyłane do blockchaina
- Importer zatwierdza odbiór, **smart kontrakt** zwalnia płatność
- Klient w sklepie skanuje kod QR – widzi cały łańcuch dostaw (np. farmę, trasę, czas dostawy)

MODEL KOMPETENCYJNY
WIEDZA UMIEJĘTNOŚCI POSTAWY

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

AW2.0
AUDYT WEWNĘTRZNY

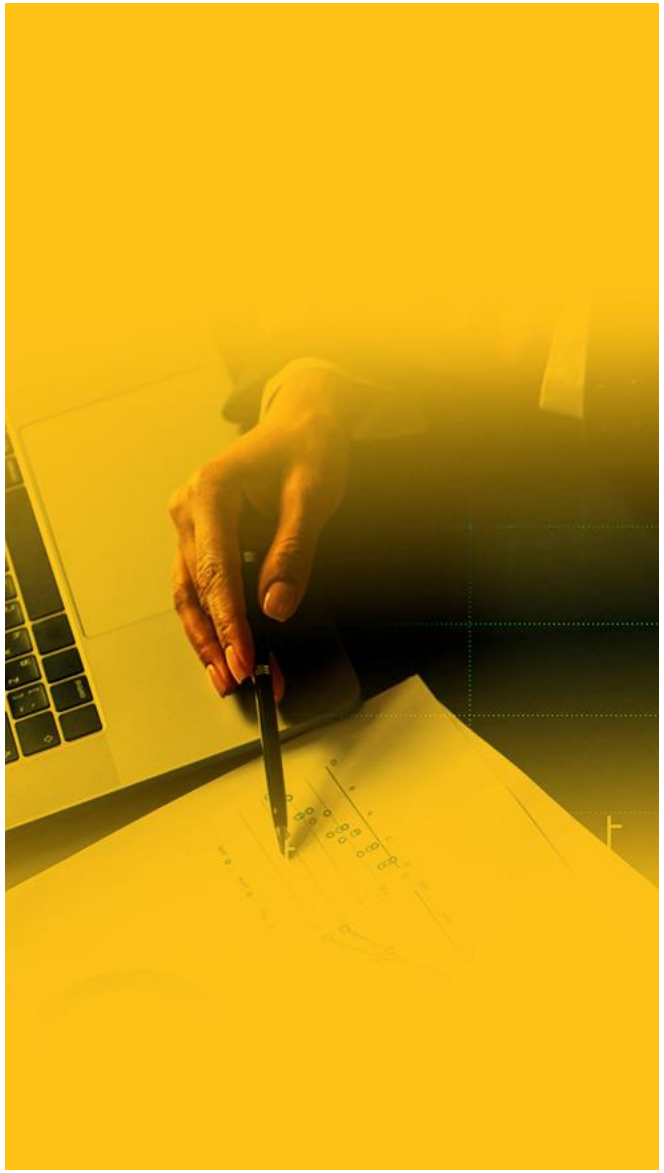
BW advisory
Przez naszą wiedzę do Twojej wartości.

C&F

Ministerstwo
Finansów

05 Studium przypadku

STUDIUM PRZYPADKU 1
NOTPETYA



Tło: Hybrydowa Wojna Rosji

2014: Rosja anektuje Krym, co prowadzi do eskalacji konfliktu z Ukrainą.

Następuje **przejście od wojny kinetycznej do cyberwojny**, będące częścią szerszej strategii Rosji mającej na celu destabilizację Ukrainy.

Eskalacja Cyberataków

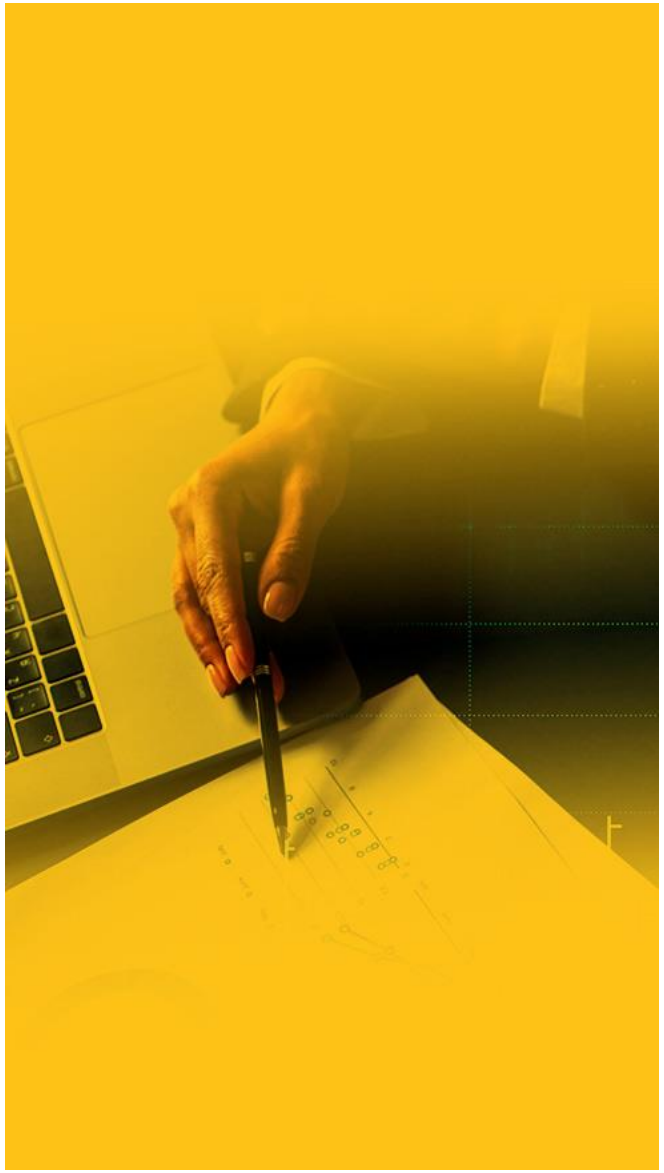
2015 i 2016: Ataki na infrastrukturę energetyczną Ukrainy sygnalizują wykorzystanie cyberprzestrzeni jako narzędzia militarnego.

Czerwiec 2017: Wypuszczenie złośliwego oprogramowania **NotPetya** — początkowo wymierzonego w ukraińską infrastrukturę, ale rozprzestrzenionego na cały świat.

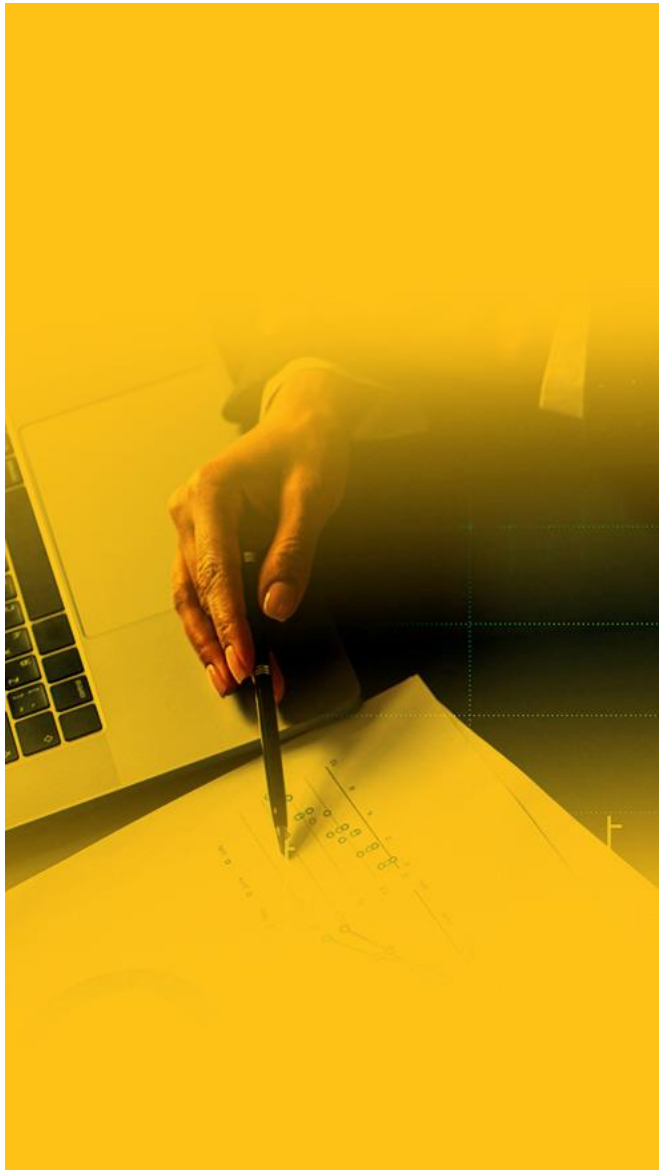
Cel Strategiczny

Operacja była **sabotażem ukrytym pod postacią ransomware**.

Celem NotPetya nie był zysk finansowy, lecz **sparaliżowanie ukraińskiej gospodarki** i wysłanie **globalnego sygnału**.



Data	Wydarzenie
Marzec 2014	Rosja anektuje Krym; rozpoczyna się konflikt z Ukrainą
2015–2016	Cyberataki na ukraińską sieć energetyczną pokazują rosnące możliwości
7 marca 2017	Wycieka zestaw narzędzi hakerskich CIA (Vault 7)
14 marca 2017	Microsoft publikuje poprawkę dla EternalBlue (MS17-010)
14 kwietnia 2017	Narzędzia hakerskie NSA (EternalBlue, DoublePulsar) ujawnione przez Shadow Brokers
12 maja 2017	Atak WannaCry ukazuje globalne zagrożenie związane z narzędziami NSA
27 czerwca 2017	NotPetya rozpowszechniona przez aktualizację M.E.Doc
Czerwiec–lipiec 2017	Maersk, Merck, FedEx i inne firmy doświadczają poważnych zakłóceń
2020	USA oskarżają 6 oficerów GRU o cyberataki związane z NotPetya



Wykorzystane Wycieki Informacji Wywiadowczych:

Vault 7 (CIA): Ujawnił ofensywne zdolności cybernetyczne amerykańskiego wywiadu.

Shadow Brokers (NSA): Upublicznił zaawansowane exploity dla systemu Windows, które zostały wykorzystane m.in. w ataku NotPetya.

Exploit	Cel	Data wydania poprawki	Uwagi
EternalBlue	SMBv1 (Windows XP–8, Server)	14 marca 2017 (MS17-010)	Kluczowy dla NotPetya i WannaCry
EternalRomance	Komponent SMB	Wówczas nie w pełni załatany	Używany razem z EternalBlue

Brak Aktualizacji (Failure to Patch):

Wiele przedsiębiorstw opóźniało instalację poprawek lub korzystało z niewspieranych, przestarzałych systemów.

Microsoft wydał awaryjne poprawki, jednak ich wdrażanie było opóźnione.

CISA i DHS później określiły opóźnienia w aktualizacjach jako krytyczne, systemowe zagrożenie.

STUDIUM PRZYPADKU 2

STUDIUM PRZYPADKU – BITWA O ANGLIĘ 1940

IN A NUTSHELL

Royal Air Force Benevolent Fund

BATTLE OF BRITAIN
10 JULY – 31 OCTOBER 1940

BATTLE OF BRITAIN

STUDIUM PRZYPADKU – OCENA RYZYKA DOSTAWCY

KROK 1

STUDIUM PRZYPADKU – OCENA RYZYKA DOSTAWCY

KROK 2

USŁUGA:

Piloci myśliwców

Piloci bombowców

STUDIUM PRZYPADKU – OCENA RYZYKA DOSTAWCY

KROK 3

Dostawca:

Polska

Usługi:

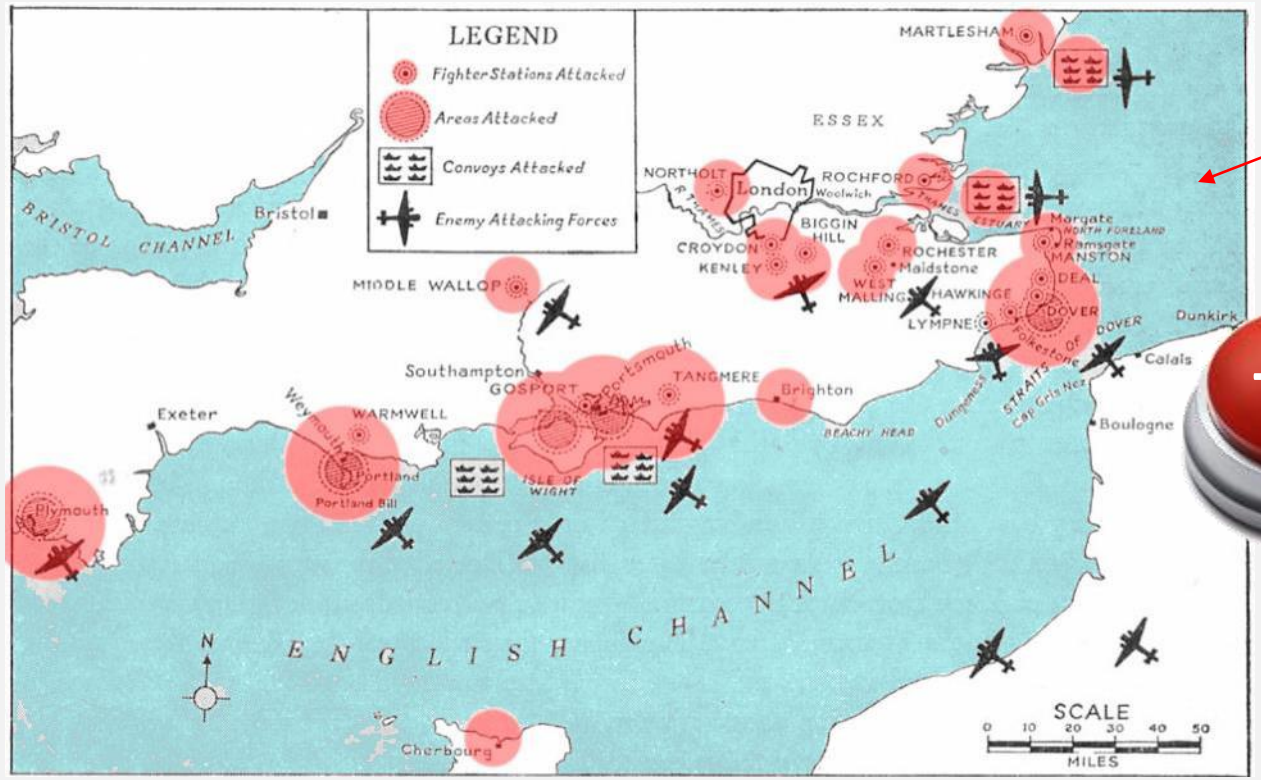
88 Piloci myśliwców

57 Piloci bombowców

STUDIUM PRZYPADKU – OCENA RYZYKA DOSTAWCY

KROK 4

CZY TO WAŻNA DLA NAS USŁUGA?



TAK!

STUDIUM PRZYPADKU – OCENA RYZYKA DOSTAWCY

KROK 5

PROFILE RYZYKA DOSTAWCY

Profil Ryzyka Dostawcy (Polscy Piloci):

- ☒ Nie znają brytyjskiej taktyki walki
- ☒ Nie mają doświadczenia z nowoczesnymi samolotami (Hurricane, Spitfire'y)
- ☒ Niewystarczająca znajomość języka angielskiego

STUDIUM PRZYPADKU – OCENA RYZYKA DOSTAWCY

KROK 5

PROFILE RYZYKA DOSTAWCY

Profil Ryzyka Dostawcy (Polscy Piloci):

- ☒ Nie znają brytyjskiej taktyki walki
- ☒ Nie mają doświadczenia z nowoczesnymi samolotami (Hurricane, Spitfire'y)
- ☒ Niewystarczająca znajomość języka angielskiego
- ☒ Zbyt chętni do walki z wrogiem ...

STUDIUM PRZYPADKU – OCENA RYZYKA DOSTAWCY

KROK 6

ASSESSMENT (DURING THE BATTLE).

- Niezwykle dobrzy piloci
- Szerokie doświadczenie bojowe
- Taktyka walki lepsza niż oczekiwano **(5 to 1)**
- Niesamowita wydajność

W pierwszej misji Dywizjonu 303 zestrzelono sześć myśliwców wroga. W 15 minut.

STUDIUM PRZYPADKU – OCENA RYZYKA DOSTAWCY

KROKI 7 I 8

NIE JEST TO WYMAGANE, POZWÓLMY IM LATAĆ

STUDIUM PRZYPADKU – OCENA RYZYKA DOSTAWCY

DZIĘKUJEMY!

Dziękujemy za uwagę

MODEL KOMPETENCYJNY
WIEDZA UMIEJĘTNOŚCI POSTAWY

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

AUDYT WEWNĘTRZNY

BW advisory
Przez naszą wiedzę do Twojej wartości.

C&F

Ministerstwo
Finansów

06 Pytania

Pytania od uczestników

Dziękujemy! Zapraszamy do kontaktu (Linkedin, email)

Jan Anisimowicz
C&F SA
Warsaw ISACA Chapter
IIA Polska
Jan.Anisimowicz@candf.com

www.adaptivegrc.com
www.candf.com

Sebastian Burgemeister
BW Advisory Sp. z o.o.
IIA UAE (Dubai)
Former President of IIA Polska
s.burgemejster@itgrc.pl

www.itgrc.pl
www.akademiaitgrc.pl