2BEAWARE
SECURITY AWARENESS

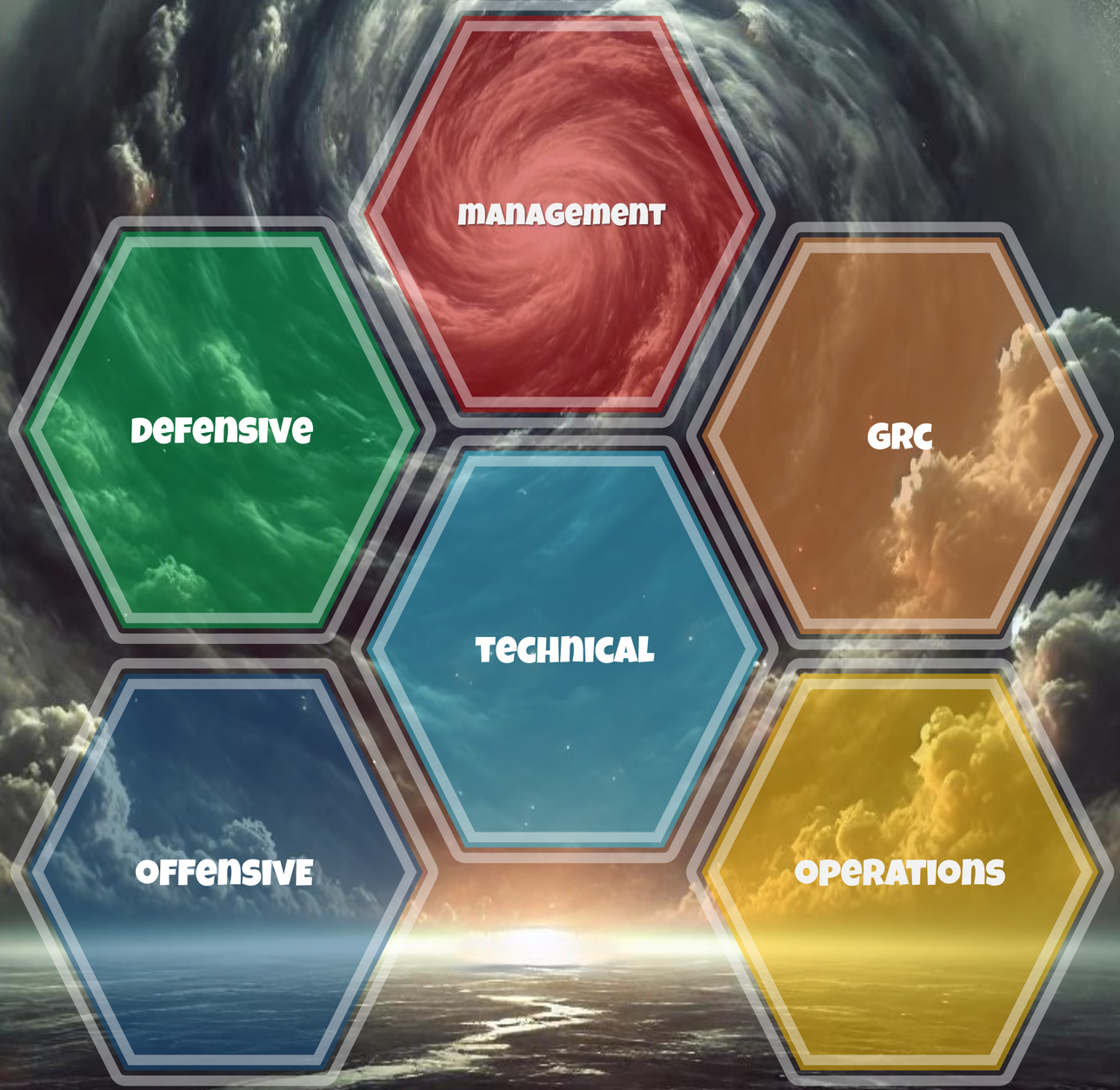
SECURITY DLA LIDERÓW

KTO JEST KIM W SECURITY ?

KRZYSZTOF
BRYŁA

CZĘŚĆ 4

OBSZARY SECURITY



2BEAWARE
SECURITY AWARENESS

Governance Compliance Risk

GRC: ŁAD, ZGODNOŚĆ, RYZYKO

- ZAPEWNIENIE ODPOWIEDNIEGO ZARZĄDZANIA, NADZORU I KIEROWANIA ORGANIZACJĄ, ZAPEWNIAJĄCEGO OSIĄGANIE STRATEGICZNYCH CELÓW
- ZAPEWNIENIE, ŻE FIRMA DZIAŁA ZGODNIE Z OBOWIĄZUJĄCYMI PRZEPISAMI PRAWNYMI, STANDARDAMI BRANŻOWYMI ORAZ WEWNĘTRZNYMI POLITYKAMI
- IDENTYFIKACJA, ANALIZA I MITYGACJA RYZYK, KTÓRE MOGĄ WPŁYNĄĆ NA OSIĄGNIĘCIE CELÓW ORGANIZACJI
- TWORZENIE I AKTUALIZACJA WEWNĘTRZNYCH POLITYK I PROCEDUR
- PROWADZENIE PROGRAMÓW SZKOLENIOWYCH I EDUKACYJNYCH DLA PRACOWNIKÓW

Zespoły GRC, bardzo często tworzą tzw. drugą linię obrony

Business, Operations, Zarząd, Security Operations

Działanie, Operacje, Procesy

1stLofD (Pierwsza Linia Obrony)

Zespoły GRC, bardzo często tworzą tzw. drugą linię obrony

Business, Operations, Zarząd, Security Operations

Działanie, Operacje, Procesy — 1stLofD (Pierwsza Linia Obrony)

Governance, Compliance, Risk, Legal, DPO

Superwizja, Kontrola, Wsparcie - dla 1stLofD — 2ndLofD (Druga Linia Obrony)

Zespoły GRC, bardzo często tworzą tzw. drugą linię obrony

Business, Operations, Zarząd, Security Operations

Działanie, operacje, procesy — 1stLofD (Pierwsza Linia Obrony)

Governance, Compliance, Risk, Legal, DPO

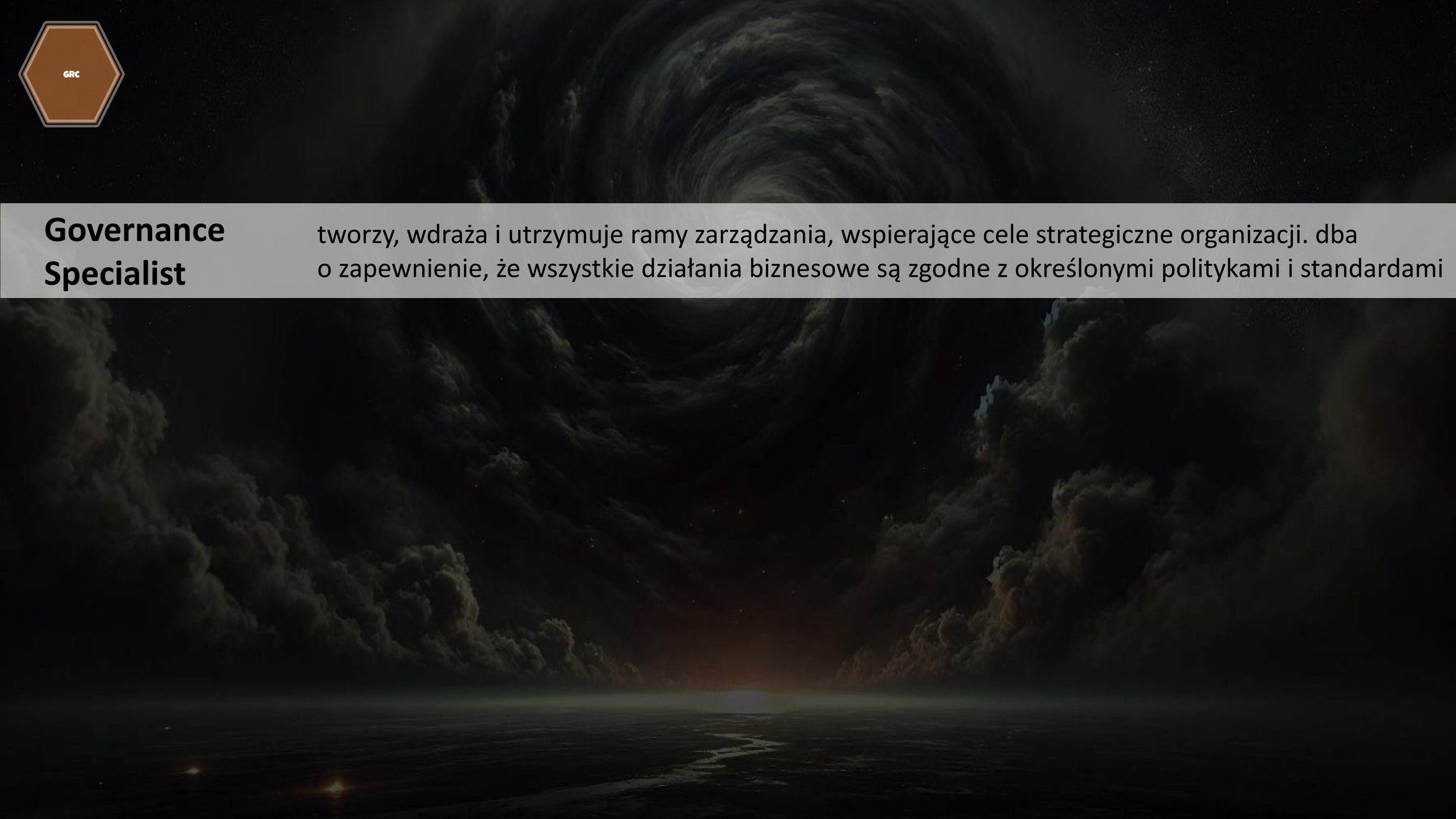
Superwizja, kontrola, wsparcie - dla 1stLofD — 2ndLofD (Druga Linia Obrony)

Audit

Kontrola, audyt — 3rdLofD (Trzecia Linia Obrony)

GRC

- Zapewnienie odpowiedniego zarządzania, nadzoru i kierowania organizacją, zapewniającego osiąganie strategicznych celów
- Zapewnienie, że firma działa zgodnie z obowiązującymi przepisami prawnymi, standardami branżowymi oraz wewnętrznymi politykami
- Identyfikacja, analiza i mitygacja ryzyka, które może wpłynąć na osiągnięcie celów organizacji
- Tworzenie i aktualizacja wewnętrznych polityk i procedur
- Prowadzenie programów szkoleniowych i edukacyjnych dla pracowników



Governance Specialist

tworzy, wdraża i utrzymuje ramy zarządzania, wspierające cele strategiczne organizacji. dba o zapewnienie, że wszystkie działania biznesowe są zgodne z określonymi politykami i standardami

Governance Specialist	tworzy, wdraża i utrzymuje ramy zarządzania, wspierające cele strategiczne organizacji. dba o zapewnienie, że wszystkie działania biznesowe są zgodne z określonymi politykami i standardami
Risk Manager	tworzy ramy zarządzania ryzykiem dla organizacji, identyfikuje, analizuje i raportuje ryzyko w organizacji. podnosi świadomość w obszarze zarządzania ryzykiem

GRC

Governance Specialist	tworzy, wdraża i utrzymuje ramy zarządzania, wspierające cele strategiczne organizacji. dba o zapewnienie, że wszystkie działania biznesowe są zgodne z określonymi politykami i standardami
Risk Manager	tworzy ramy zarządzania ryzykiem dla organizacji, identyfikuje, analizuje i raportuje ryzyko w organizacji. podnosi świadomość w obszarze zarządzania ryzykiem
Compliance Officer	monitoruje i raportuje zgodność organizacji z przepisami prawnymi i wewnętrznymi regulacjami

Governance Specialist	tworzy, wdraża i utrzymuje ramy zarządzania, wspierające cele strategiczne organizacji. dba o zapewnienie, że wszystkie działania biznesowe są zgodne z określonymi politykami i standardami
Risk Manager	tworzy ramy zarządzania ryzykiem dla organizacji, identyfikuje, analizuje i raportuje ryzyko w organizacji. podnosi świadomość w obszarze zarządzania ryzykiem
Compliance Officer	monitoruje i raportuje zgodność organizacji z przepisami prawnymi i wewnętrznymi regulacjami
ISO	rozwija, wdraża i utrzymuje polityki bezpieczeństwa informacji. przeprowadza analizy ryzyka, aby zidentyfikować potencjalne zagrożenia dla bezpieczeństwa informacji. podnosi świadomości w temacie zagrożeń cybernetycznych i najlepszych praktyk w zakresie bezpieczeństwa informacji

Governance Specialist	tworzy, wdraża i utrzymuje ramy zarządzania, wspierające cele strategiczne organizacji. dba o zapewnienie, że wszystkie działania biznesowe są zgodne z określonymi politykami i standardami
Risk Manager	tworzy ramy zarządzania ryzykiem dla organizacji, identyfikuje, analizuje i raportuje ryzyko w organizacji. podnosi świadomość w obszarze zarządzania ryzykiem
Compliance Officer	monitoruje i raportuje zgodność organizacji z przepisami prawnymi i wewnętrznymi regulacjami
ISO	rozwija, wdraża i utrzymuje polityki bezpieczeństwa informacji. przeprowadza analizy ryzyka, aby zidentyfikować potencjalne zagrożenia dla bezpieczeństwa informacji. podnosi świadomości w temacie zagrożeń cybernetycznych i najlepszych praktyk w zakresie bezpieczeństwa informacji
BCM	rozwija i utrzymuje procesy, zapewniające ciągłość operacji biznesowych w przypadku wystąpienia nieprzewidzianych zdarzeń. opracowuje i testuje plany kontynuacji działalności oraz odzyskiwania po awarii

2BEAWARE
SECURITY AWARENESS

*

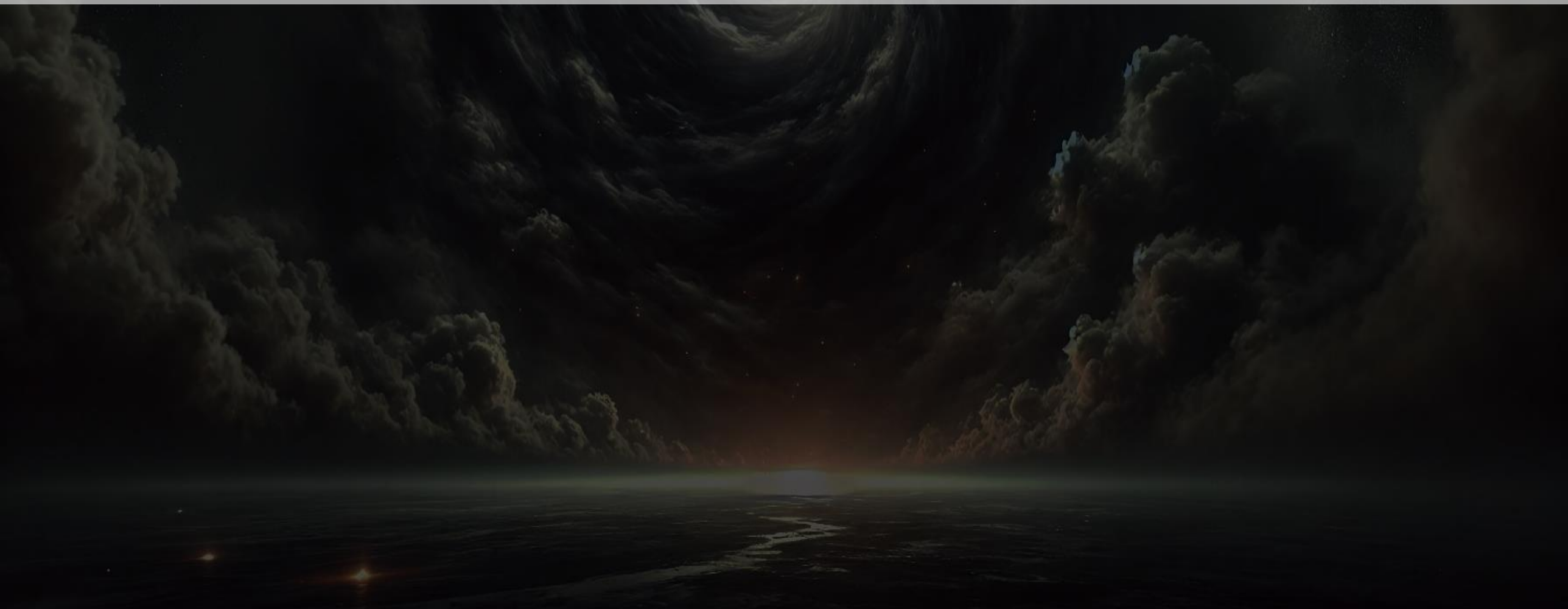
Funkcje wspierające

Funkcje wspierające

- Nadzór nad procesami przyznawania, monitorowania i cofania dostępu do systemów i danych firmowych, nadzór na procesami on/off boardingu
- Organizowanie i zapewnianie regularnych szkoleń z zakresu bezpieczeństwa informacji
- Nadzorowanie przestrzegania przepisów dotyczących ochrony danych osobowych
- Koordynowanie reakcji na naruszenia ochrony danych osobowych i komunikacja z organami nadzorczymi
- Doradztwo w przypadku naruszeń bezpieczeństwa i potencjalnych konsekwencji prawnych
- Zapewnienie działania firmy zgodnego z lokalnymi, krajowymi i międzynarodowymi przepisami dotyczącymi bezpieczeństwa i ochrony danych osobowych

Funkcje wspierające

DPO	monitoruje zgodność organizacji z przepisami dotyczącymi ochrony danych osobowych. doradza organizacji w sprawach ochrony danych, przeprowadza audyty i szkolenia. jest punktem kontaktowym dla osób, których dane dotyczą oraz dla organów nadzorczych



Funkcje wspierające

DPO	monitoruje zgodność organizacji z przepisami dotyczącymi ochrony danych osobowych. doradza organizacji w sprawach ochrony danych, przeprowadza audyty i szkolenia. jest punktem kontaktowym dla osób, których dane dotyczą oraz dla organów nadzorczych
Legal	identyfikuje i minimalizuje ryzyka prawne związane z naruszeniami danych, w tym odpowiedzialność cywilną i karną firmy. sporządza umowy z podmiotami zewnętrznymi obejmujące klauzule dotyczące bezpieczeństwa informacji

Funkcje wspierające

DPO	monitoruje zgodność organizacji z przepisami dotyczącymi ochrony danych osobowych. doradza organizacji w sprawach ochrony danych, przeprowadza audyty i szkolenia. jest punktem kontaktowym dla osób, których dane dotyczą oraz dla organów nadzorczych
Legal	identyfikuje i minimalizuje ryzyka prawne związane z naruszeniami danych, w tym odpowiedzialność cywilną i karną firmy. sporządza umowy z podmiotami zewnętrznymi obejmujące klauzule dotyczące bezpieczeństwa informacji
HR	opracowuje i wdraża programy szkoleniowe skoncentrowane na świadomości i procedurach bezpieczeństwa. reaguje na przypadki naruszenia zasad bezpieczeństwa przez pracowników, zarządzając procesami dyscyplinarnymi

2BEAWARE
SECURITY AWARENESS

CDN ...

Pytanie dla uważnych:

Czy brak zespołu GRC czy nawet GRC* pozbawia organizację bezpieczeństwa ?

2BEAWARE
SECURITY AWARENESS

KRZYSZTOF BRYŁA

2beaware

2beaware_

office@2beaware.co

krzysztof-bryla