

Wdrożenie compliance w 6 krokach

**PRAKTYCZNE ASPEKTY
WDROŻENIA**

Wojciech Piszewski

GRC LEGAL



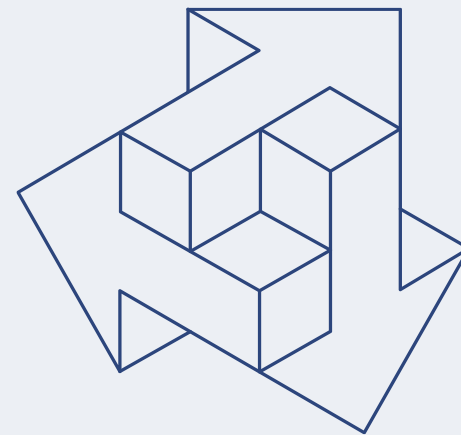


Compliance i system compliance – wprowadzenie

Czym jest compliance?

**„Jeśli nikt mnie o to nie pyta, wiem.
Jeśli pytającemu usiłuję wytłumaczyć, nie wiem”.**

– św. Augustyn



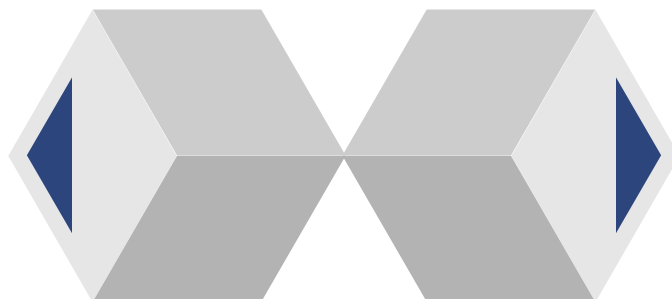
Standardowe (typowe) obszary compliance

Zgodność z prawem /
wymogami sektorowymi



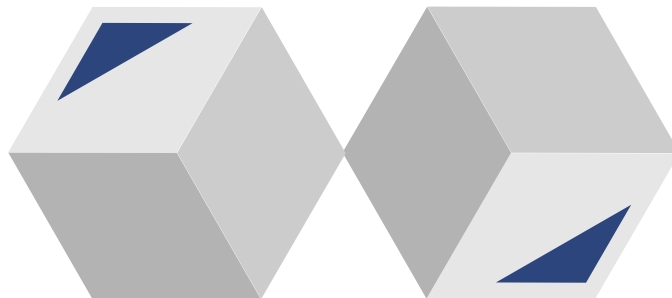
Bezpieczeństwo
łańcucha dostaw

Przeciwdziałanie korupcji
i konfliktom interesów



HR Compliance

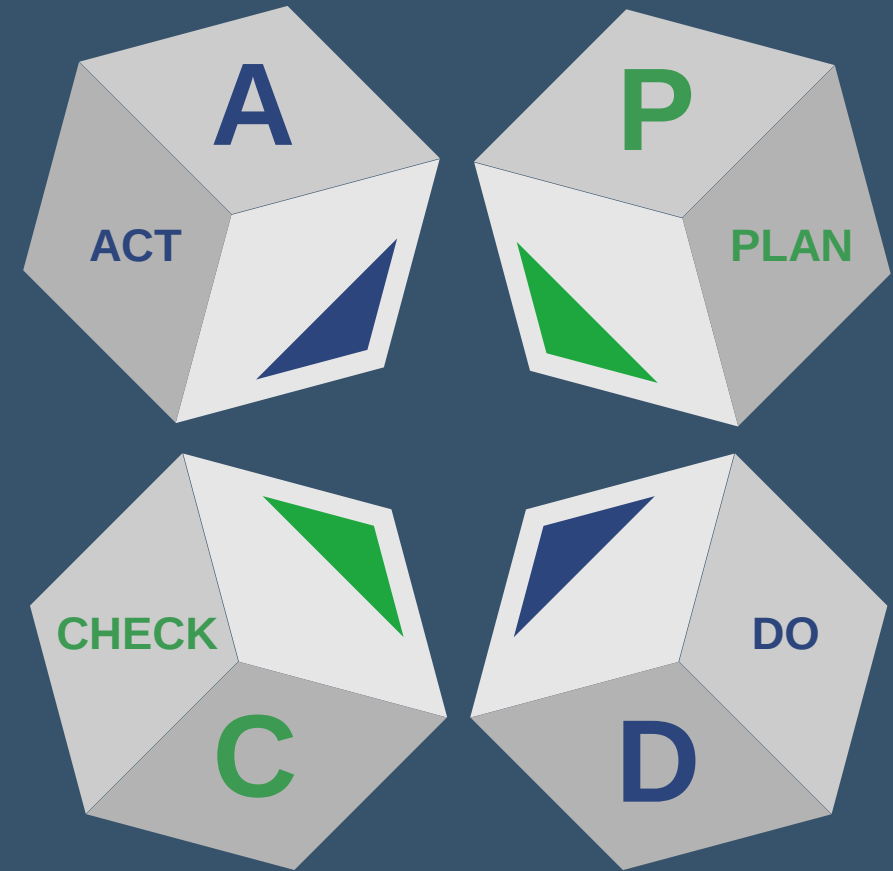
Zarządzanie informacjami
(RODO, bezpieczeństwo informacji,
tajemnica przedsiębiorstwa)



Ochrona
sygnalistów

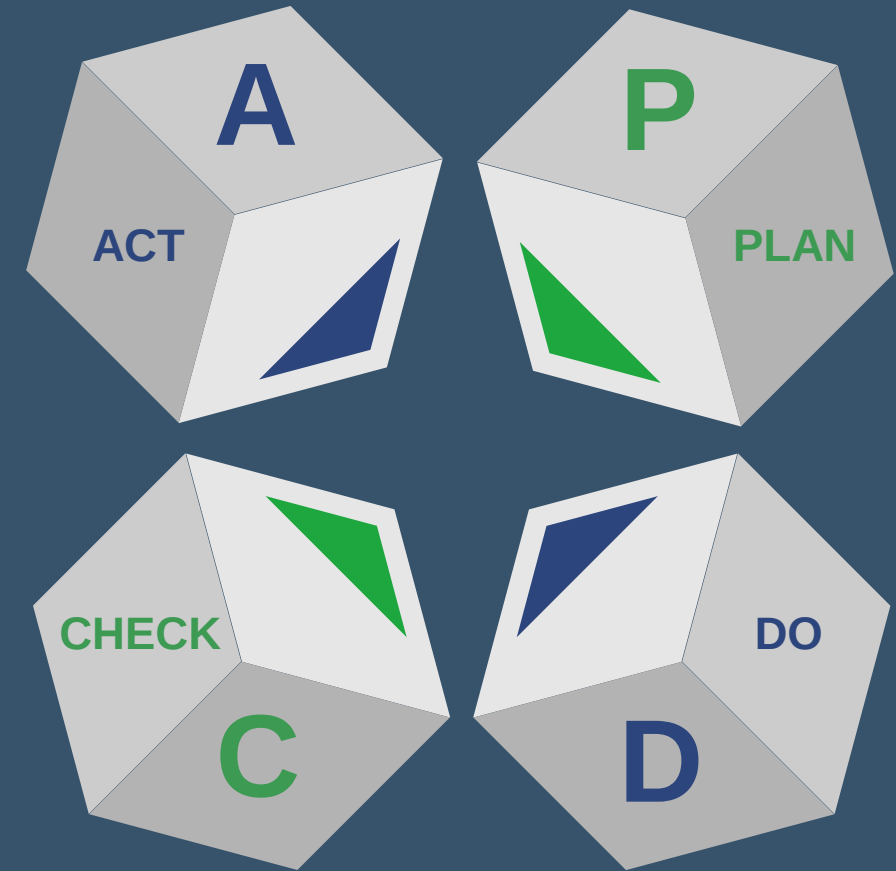
System Compliance I

- Osoby odpowiedzialne
- Miejsce w strukturze firmy**
- Zasoby i sposoby działania
- Procedury i polityki



System Compliance II

- ❏ Kontekst organizacji
- ❏ **Analiza ryzyka**
- ❏ Plan działania
- ❏ Wdrożenie
- ❏ Utrzymanie zgodności



Rola dobrej analizy ryzyka

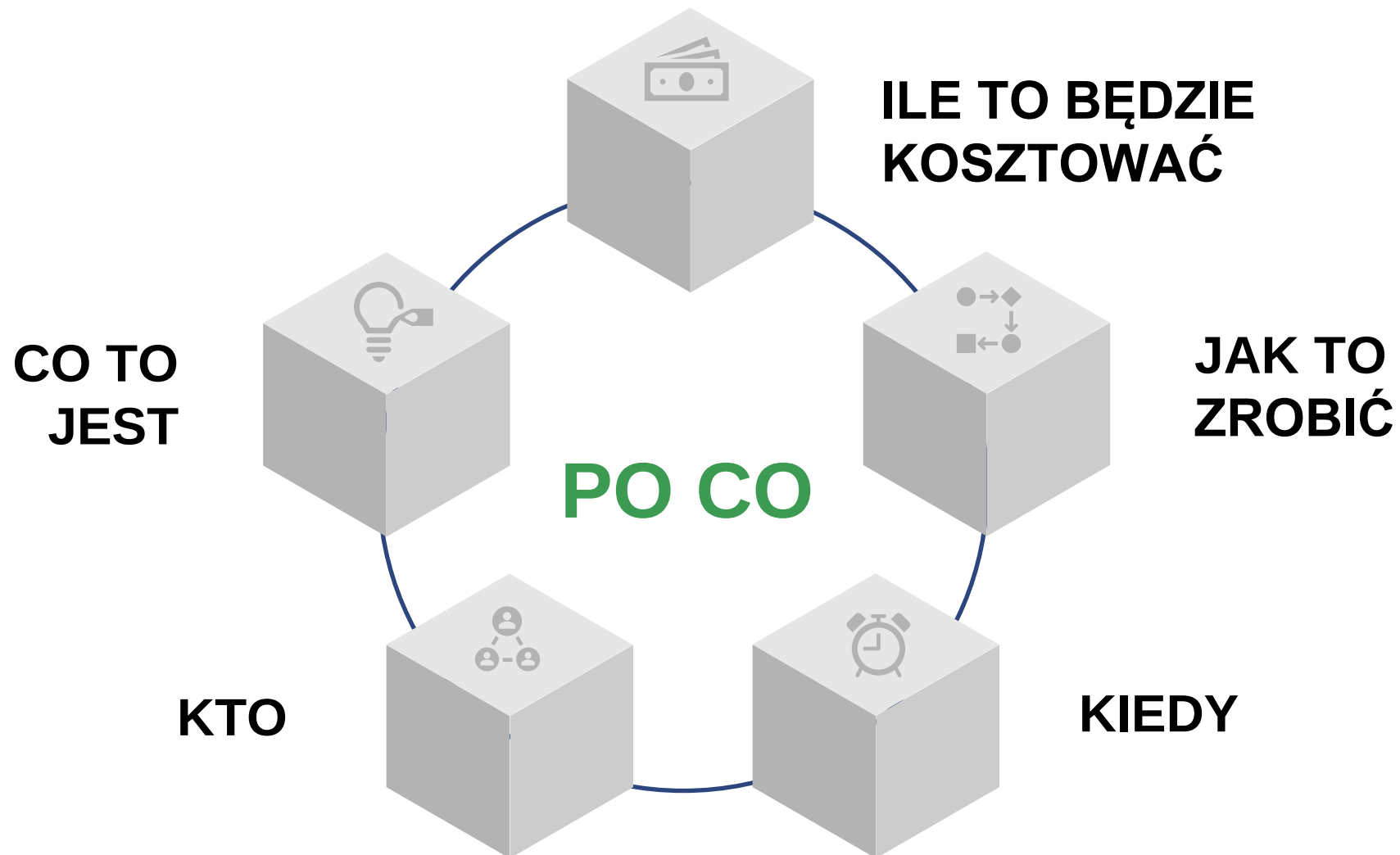
- ❏ **Priorytetyzacja działań**
- ❏ **Dobór środków do celu**
- ❏ Proces musi być „realizowalny” w praktyce – wskazanie praktycznych czynności do podjęcia
- ❏ Procedury to nie wszystko...





Zanim powiemy jak...

...kilka trudnych pytań



Czy chodzi tylko o uniknięcie kary?



KORZYŚCI WEWNĘTRZNE

- ❏ Strategiczne i przemysłane zarządzanie organizacją
- ❏ Ograniczenie ryzyka operacyjnego
- ❏ Zwiększenie bezpieczeństwa prawnego
- ❏ Zwiększenie atrakcyjności przedsiębiorstwa jako pracodawcy
- ❏ Polepszenie komunikacji i przepływu informacji
- ❏ Dostęp do informacji o przedsiębiorstwie „z pierwszej ręki”



KORZYŚCI ZEWNĘTRZNE

Czy chodzi tylko o uniknięcie kary?



KORZYŚCI WEWNĘTRZNE

- ❖ Strategiczne i przemysłane zarządzanie organizacją
- ❖ Ograniczenie ryzyka operacyjnego
- ❖ Zwiększenie bezpieczeństwa prawnego
- ❖ Zwiększenie atrakcyjności przedsiębiorstwa jako pracodawcy
- ❖ Polepszenie komunikacji i przepływu informacji
- ❖ Dostęp do informacji o przedsiębiorstwie „z pierwszej ręki”



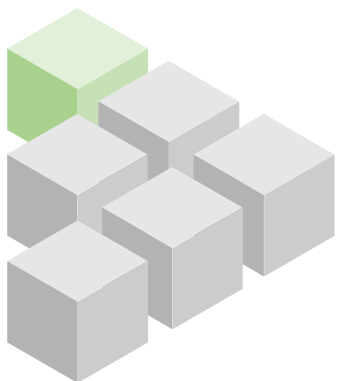
KORZYŚCI ZEWNĘTRZNE

- ❖ **Zwiększenie wiarygodności w oczach partnerów i klientów**
- ❖ **Przejrzystość i zaufanie w kontaktach biznesowych**
- ❖ **Polepszenie konkurencyjności firmy**
- ❖ **Zwiększenie wartości rynkowej**
- ❖ **Zmniejszenie kosztów transakcyjnych**



Wdrożenie CMS – aspekty praktyczne

Wdrożenie Compliance w 6 krokach



KROK 1

Określenie
kontekstu
organizacji



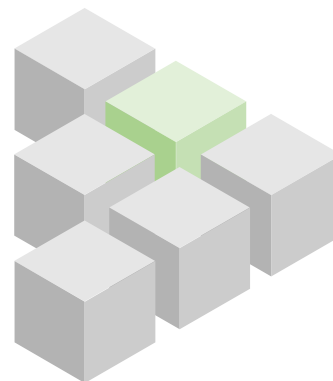
KROK 2

Analiza
ryzyka
i plan
wdrożenia



KROK 3

Ramy CMS
i polityka
compliance



KROK 4

Rozwiązania
organizacyjne
i proceduralne
w kolejnych
obszarach



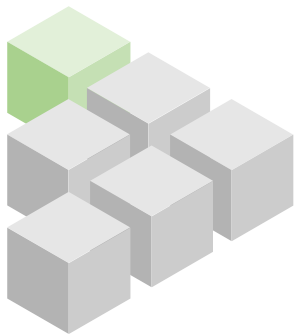
KROK 5

Szkolenia
i komunikacja



KROK 6

Utrzymanie
zgodności
(monitoring
compliance)



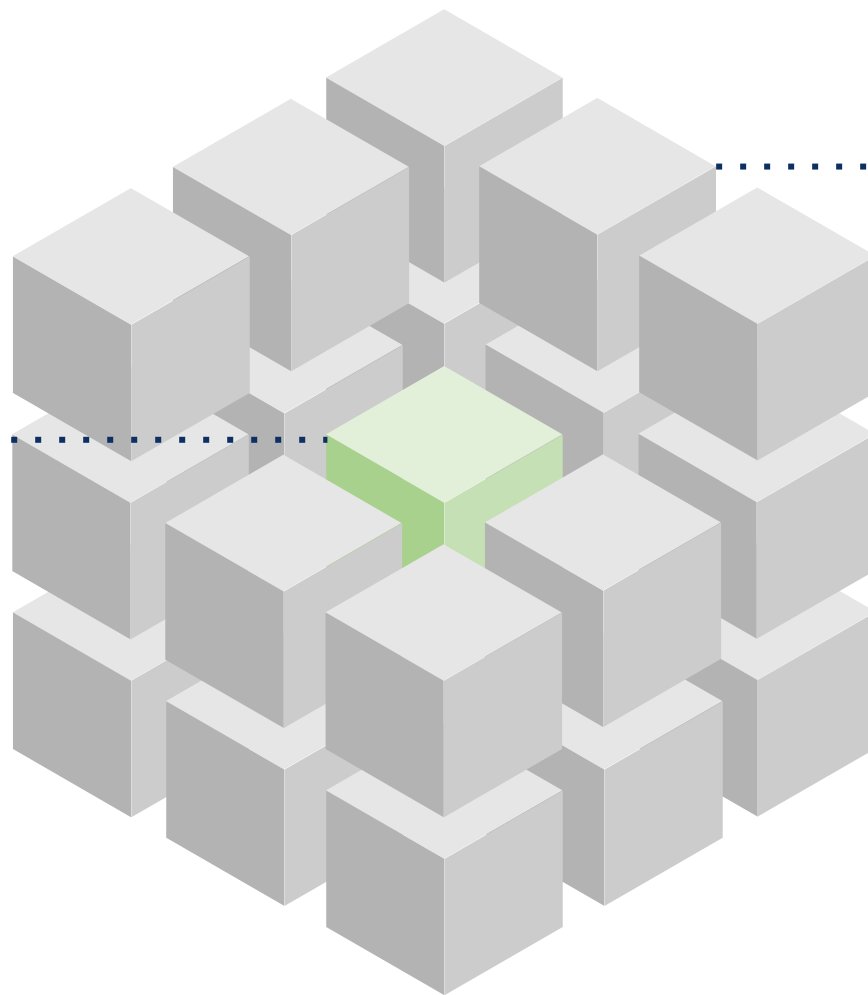
KROK 1

Określenie kontekstu organizacji



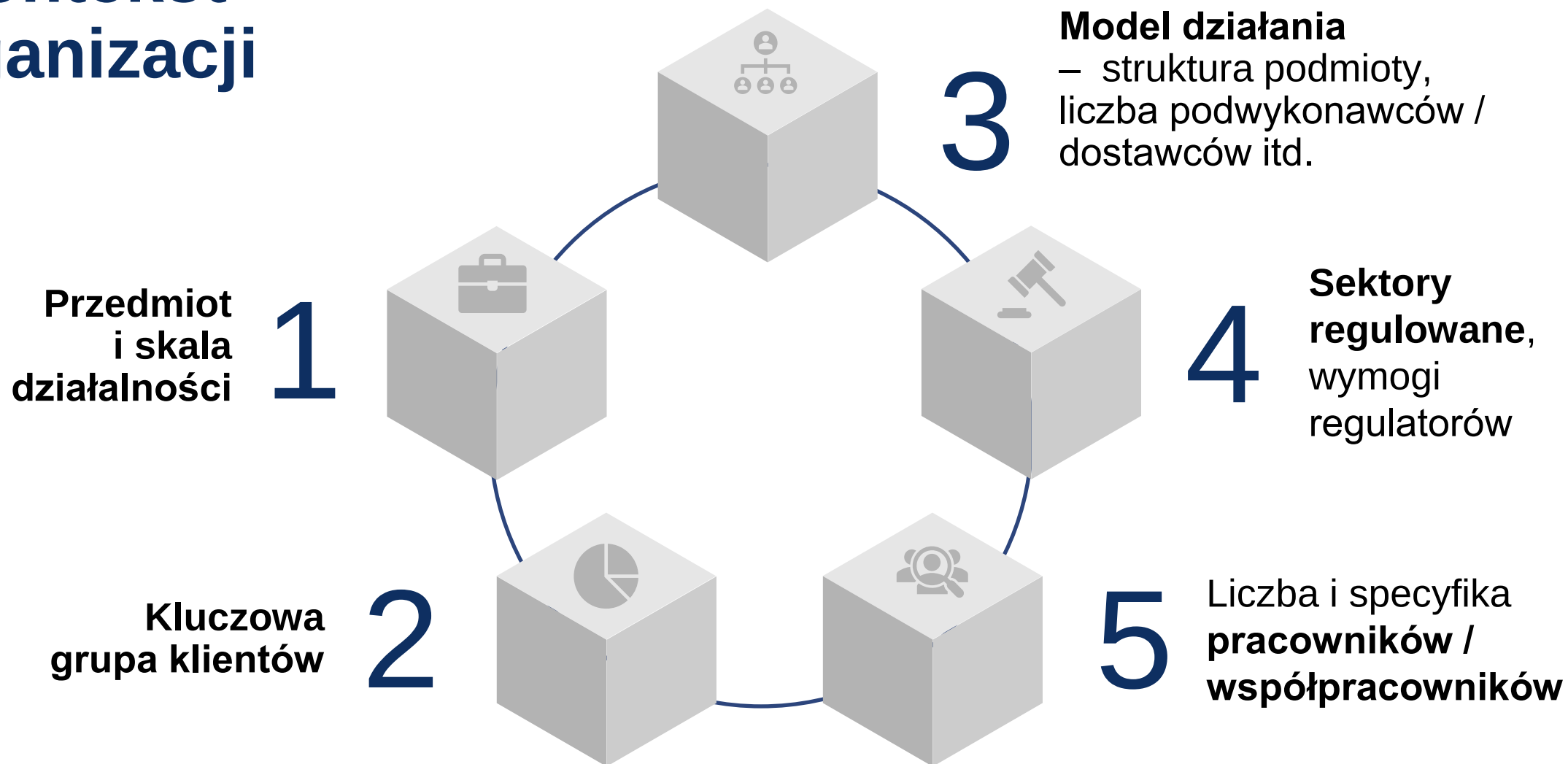
Compliance – wypełnianie wszystkich obowiązków organizacji

WYMOGI PRAWA

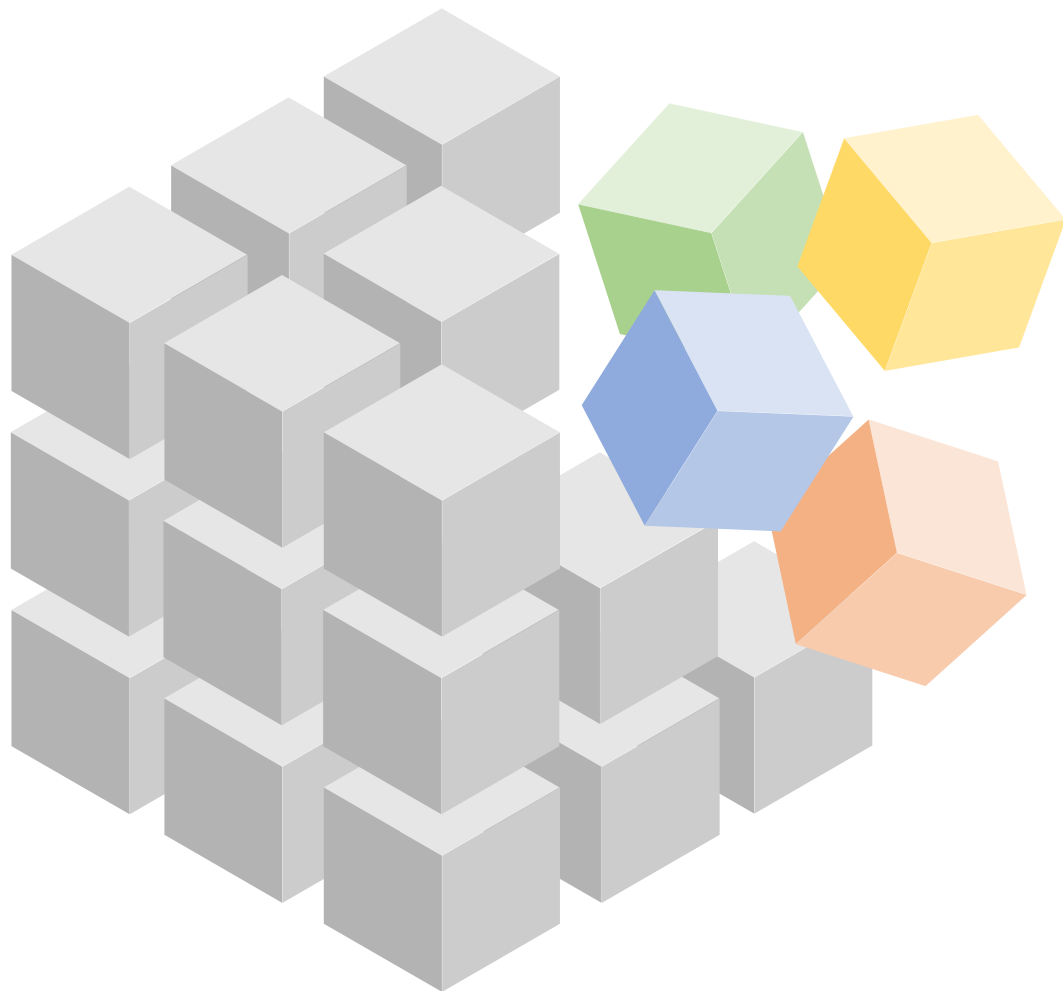


- Wymogi sektorowe / wymogi regulatora
- Normy i standardy
- Wewnętrzne procedury i polityki
- Regulacje grupy kapitałowej

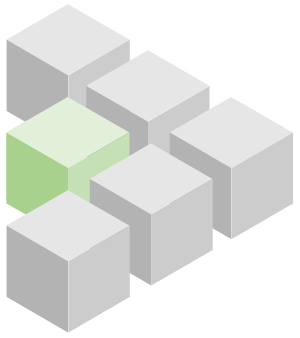
„Kontekst” organizacji



Wybrane obszary compliance



- ❏ Ochrona danych osobowych
- ❏ Przeciwdziałanie konfliktom interesów
- ❏ Cyber compliance
- ❏ Bezpieczeństwo łańcucha dostaw
- ❏ HR Compliance
- ❏ Ochrona signalistów

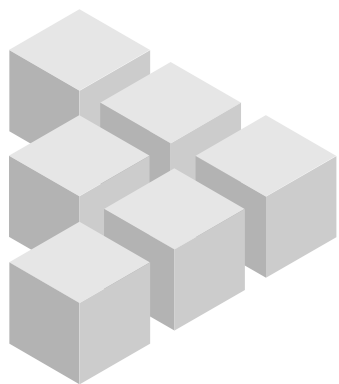


KROK 2

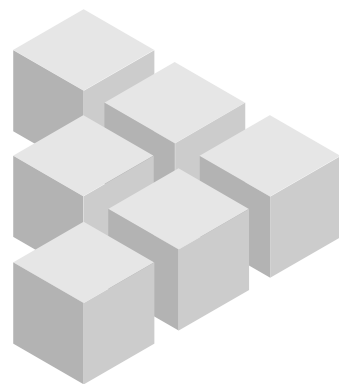
Analiza ryzyka i plan wdrożenia



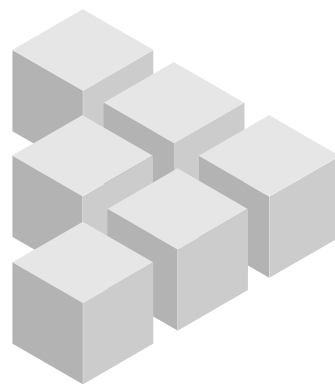
Od czego zacząć



**Określenie
istotności ryzyka**



**Określenie
prawdopodobieństwa
(poziomu dojrzałości
organizacji)**



**Plan mitygacji
ryzyka**



**Plan utrzymania
zgodności**

Ocena istotności ryzyka

ISTOTNOŚĆ

- 📦 Prawna
- 📦 Finansowa
- 📦 Biznesowa
- 📦 Reputacyjna

OCENA RYZYKA BRAKU ZGODNOŚCI							
NAZWA SPÓŁKI							
OSOBA ODPOWIEDZIALNA							
DATA OCENY							
IDENTYFIKACJA RYZYKA			ISTOTNOŚĆ RYZYKA				
LP.	OBSZAR RYZYKA	KONSEKWENCJE BRAKU ZGODNOŚCI	PRAWNA	FINANSOWA	BIZNESOWA	REPUTACYJNA	ŚREDNIA
2	Przeciwdziałanie korupcji oraz konfliktom interesów	1) Odpowiedzialność karna (kara ograniczenia albo pozbawienia wolności, grzywna) 2) Odpowiedzialność karna Spółki jako podmiotu zbiorowego 3) Znaczna utrata zaufania klientów i kontrahentów (ryzyko reputacyjne)	4	4	4	4	4
5	Whistleblowing	1) Ryzyko reputacyjne (wewnętrzne i zewnętrzne), 2) Istotny wpływ na skuteczność działań podejmowanych w pozostałych obszarach ryzyka	2	1	4	4	3

Ocena „dojrzałości”

MUST-HAVE

- ❏ Właściwa procedura / polityka
- ❏ Szkolenie i komunikacja
- ❏ Role i odpowiedzialności
- ❏ Rozliczalność
- ❏ Ewaluacja i kontrola

OBSZAR	CHECKLISTA WYMAGAŃ		
	LP.	PYTANIA KONTROLNE	WAGA
Korupcja i konflikt interesów	1	Czy określono zasady przeciwdziałania korupcji w odpowiedniej polityce / procedurze zgodności?	3
Korupcja i konflikt interesów	2	Czy polityka / procedura ta spełnia wszystkie merytoryczne wymagania?	3
Korupcja i konflikt interesów	3	Czy zaznajomiono pracowników z zasadami przeciwdziałania korupcji obowiązującymi w Spółce (udostępnienie polityki / procedury, szkolenia, instrukcje, komunikacja)?	3
Korupcja i konflikt interesów	4	Czy określono role i odpowiedzialności w zakresie zapobiegania i przeciwdziałania korupcji?	2
Korupcja i konflikt interesów	5	Czy opracowano zasady dokumentowania przypadków korupcji i podejmowania działań naprawczych?	2
Korupcja i konflikt interesów	6	Czy ryzyko zaistnienia korupcji jest analizowane, mitygowane i monitorowane?	2
Korupcja i konflikt interesów	7	Czy prowadzone są audyty stosowania zasad przeciwdziałania korupcji przez pracowników?	2
Korupcja i konflikt interesów	8	Czy z audytów wynika, że zasady te są stosowane we wszystkich obszarach działalności Spółki?	1

Plan implementacji

PLAN MITYGACJI RYZYKA			
STRATEGIA POSTĘPOWANIA	REKOMENDOWANE DZIAŁANIA	TERMIN	WŁAŚCICIEL RYZYKA
REDUKCJA	Należy wdrożyć rekomendacje opisane w checkliście wymagań, w tym: * doprecyzować informacje dot. osób odpowiedzialnych i określić konkretne obowiązki zespołu compliance, kadry zarządzającej i pracowników w tym obszarze; * opracować nowy Kodeks Dostawcy; * zaplanować i zrealizować szkolenia oraz komunikację dla pracowników, * zaplanować i przeprowadzić audyty w poszczególnych jednostkach biz., * uwzględnić wyniki audytów w kolejnej analizie ryzyka	Q3-Q4 2022	Compliance Manager

STRATEGIE ZARZĄDZANIA RYZYKIEM

- Unikanie
- Przeniesienie
- Redukcja
- Akceptacja



Plan utrzymania zgodności

❏ Priorytety

❏ Terminy

❏ Czas wdrożenia

PLAN UTRZYMANIA ZGODNOŚCI																			
		lip 22	sie 22	wrz 22	paź 22	lis 22	gru 22	sty 23	lut 23	mar 23	kwi 23	maj 23	cze 23	lip 23	sie 23	wrz 23	paź 23	lis 23	gru 23
ZADANIA STAŁE: Realizacja bieżących obowiązków Compliance Managera																			
1.	Analiza ryzyka i nadzór nad wdrożeniem rekomendacji	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2.	Przegląd polityk i procedur zgodności	4	4	4	4	4	4	2	2	2	2	2	2	2	2	2	2	2	2
3.	Prowadzenie audytów	3	3	3	3	3	3	5	5	5	5	5	5	5	5	5	5	5	5
4.	Szkolenia (onboarding i dedykowane) i komunikacja	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
5.	Przyjmowanie zgłoszeń sygnalistów	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
6.	Opiniowanie polityk, procedur i innych dokumentów przypisanych do innych jednostek biz.	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5
7.	Raportowanie	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
8.	Monitoring zmian prawnych	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
MIESIĘCZNA CZASOCHŁONNOŚĆ (LICZBA MD)		14	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
ZADANIA CYKLICZNE																			
PRZEGŁĄD POLITYKI I PROCEDUR ZGODNOŚCI: 1. Wdrożenie rekomendacji wynikających z analizy ryzyka, 2. Przegląd i aktualizacja polityki / procedury, 3. Podział odpowiedzialności, wdrożenie zmian, 4. S																			
1.	[Polityka klasyfikacji informacji]	x	x									x	x	x					
2.	Instrukcja zgłaszania nieprawidłowości		x	x										x	x	x			
3.	Polityka Antymobbingowa			x	x											x	x	x	
4.	[Kodeks Dostawcy]				x	x												x	x
5.	[Polityka compliance]					x	x												
6.	Kodeks Antykorupcyjny i Polityka Upominkowa							x	x	x									
7.	Kodeks Etyki									x	x	x							
AUDYTY ZGODNOŚCI W POSZCZEGÓLNYCH JEDNOSTKACH ORGANIZACYJNYCH																			
1.	Dział Prawny	x	x	x													x	x	
2.	Dział Bezpieczeństwa Informacji		x	x	x													x	x
3.	Dział Sprzedaży i Marketingu				x	x	x												x
4.	Dział HR							x	x										

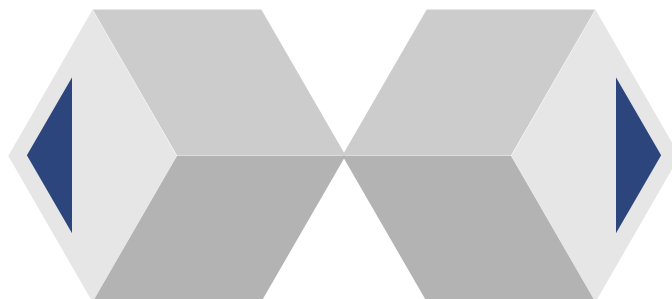
Kryteria kolejnych analiz

Wymagania prawne
(zmiany w prawie)



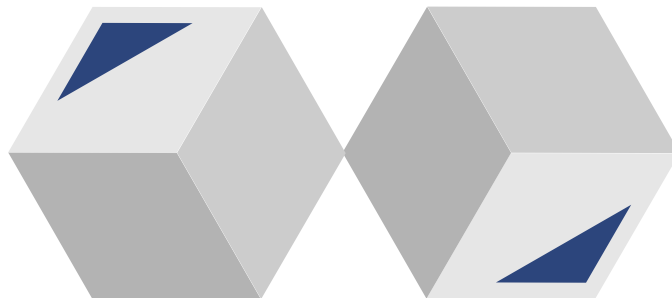
Analiza zgłoszonych
nieprawidłowości

**Wymagania partnerów
biznesowych**

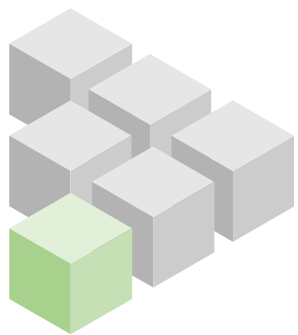


Wyniki audytów
w poszczególnych
obszarach

Poziom dojrzałości
(zaawansowanie
i efektywność wdrożenia)



Inne zidentyfikowane
podatności i problemy



KROK 3

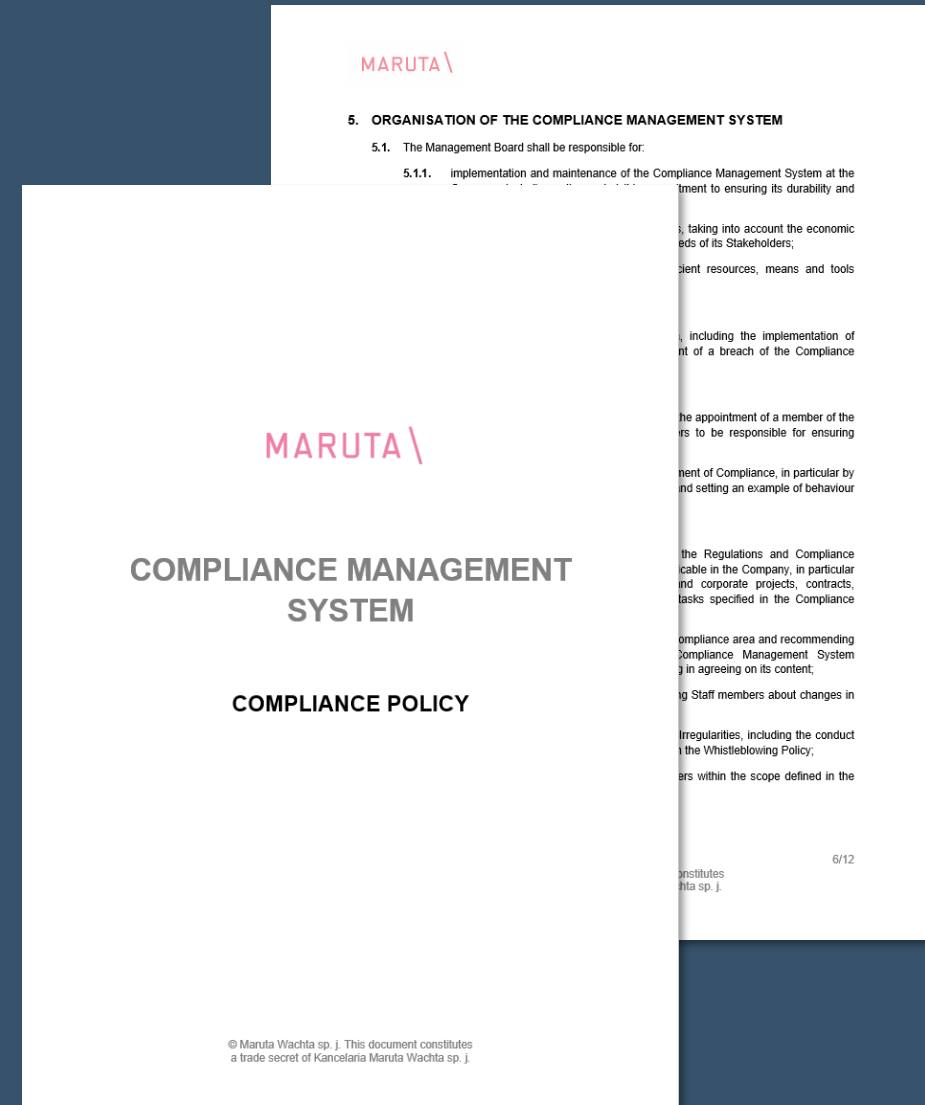
Ramy CMS i polityka compliance



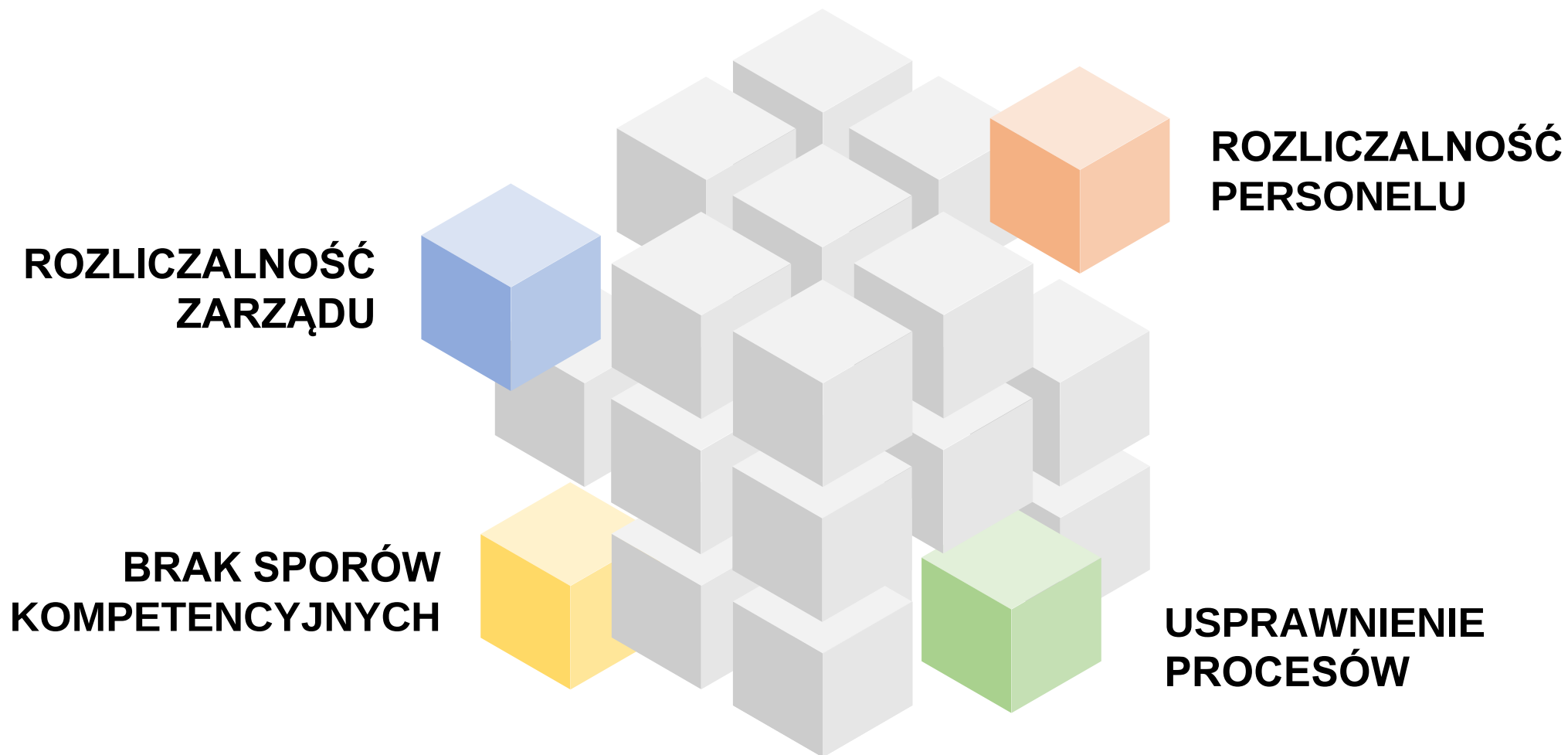
Ramy CMS

STRUKTURA ORGANIZACYJNA I SPOSÓB DZIAŁANIA

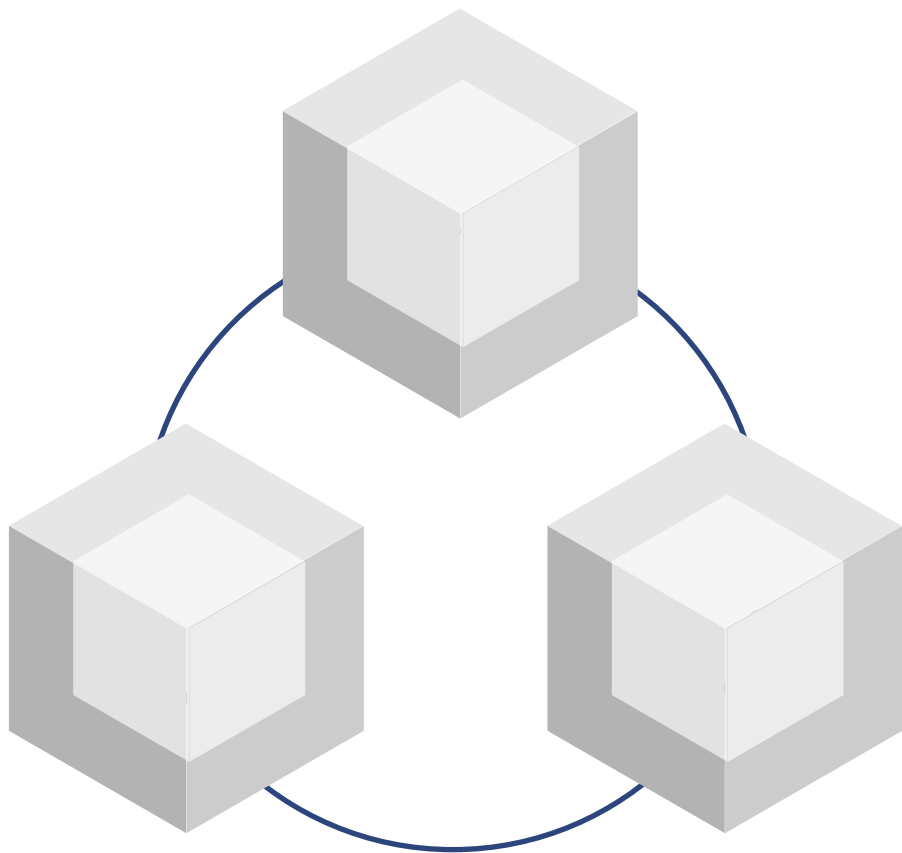
- ❏ Role i odpowiedzialności
- ❏ Miejsce w strukturze
- ❏ Sposoby działania
- ❏ Raportowanie i zasady eskalacji
- ❏ Monitorowanie aktualności w zakresie zgodności



Role i odpowiedzialności – perspektywa kadry kierowniczej



Role i odpowiedzialności – perspektywa pracownika



1

Jednoznacznie
przypisane zadania

2

Jasny model
raportowania

3

Brak dublowania
działań

Who's who w systemie zarządzania zgodnością

RADA NADZORCZA

ZARZĄD

KADRA
KIEROWNICZA

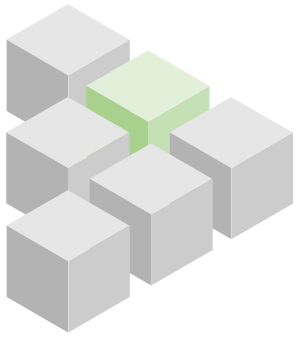
AUDYT
WEWNĘTRZNY

DZIAŁ
PRAWNY

COMPLIANCE
OFFICER

ZESPÓŁ
COMPLIANCE
OFFICERA

CZŁONKOWIE ZESPOŁÓW MERYTORYCZNYCH



KROK 4

Wdrożenie operacyjne – podejście „modułowe”



Priorytety

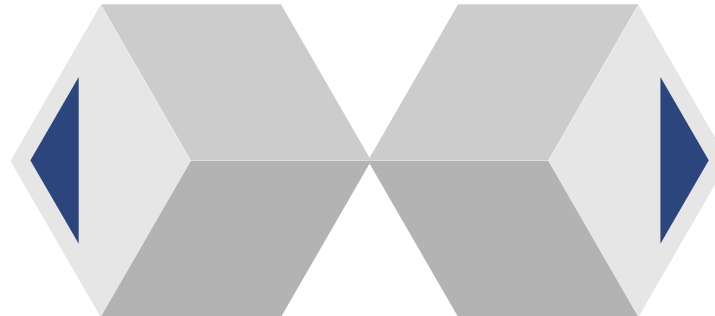
(1) IT Compliance



**Przeciwdziałanie
dyskryminacji
i mobbingowi**

(?)

(3) Przeciwdziałanie
korupcji oraz
konfliktom interesów



**Weryfikacja
kontrahentów /
dostawców**

(?)

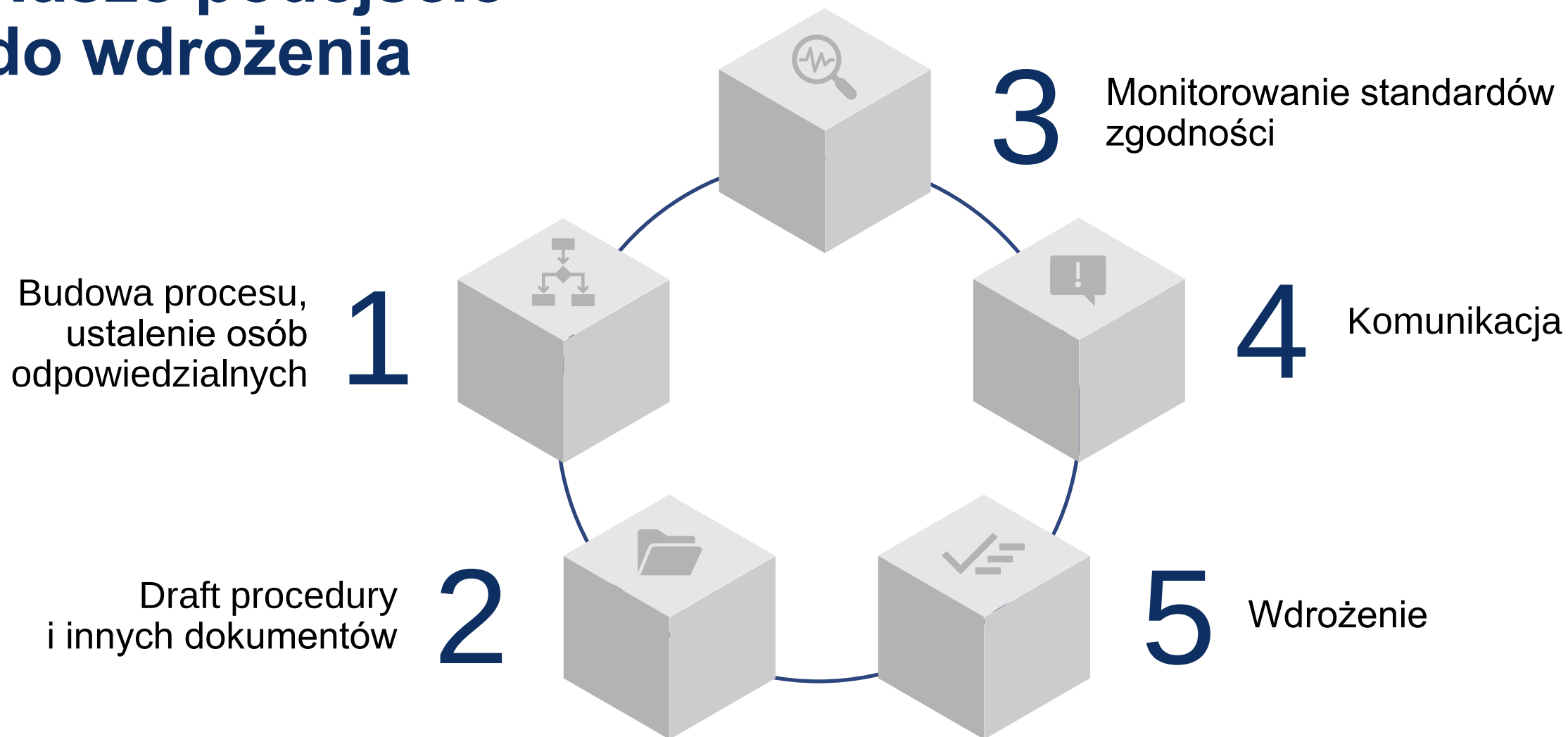
(4) Zgłaszanie
nieprawidłowości
(whistleblowing)



**Kontakty z organami
nadzorczymi
i obsługa naruszeń**

(2)

Nasze podejście do wdrożenia



Procedure Compliance



POLITYKA COMPLIANCE

- ❏ Polityka przeciwdziałania mobbingowi i dyskryminacji
- ❏ Polityka antykorupcyjna
- ❏ Polityka zarządzania konfliktami interesów
- ❏ Procedura zgłaszania naruszeń
- ❏ Procedura weryfikacji Partnerów



KODEKS ETYKI

- ❏ Procedury w obszarze ochrony danych osobowych
- ❏ Ochrona konkurencji i konsumentów
- ❏ Przeciwdziałanie praniu pieniędzy

Niezbędne elementy procedury

CEL

Cel przyjęcia procedury wraz z jej zakresem podmiotowym i przedmiotowym

ROLE

Podział odpowiedzialności, wskazanie osób decyzyjnych i zasady eskalacji

PROCES

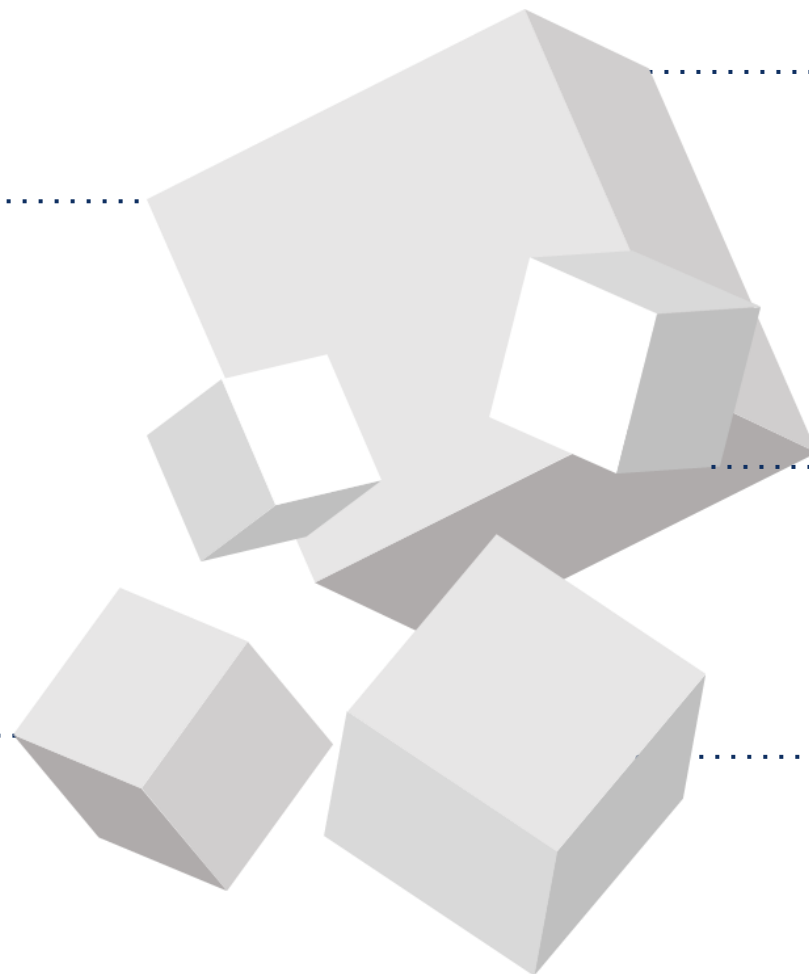
Przebieg procesu z opisem poszczególnych kroków i sposobu ich realizacji

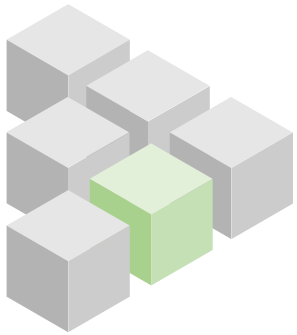
ROZLICZALNOŚĆ

Wymagana dokumentacja, reguły jej przechowywania i zasady retencji

MONITORING

Sygnały ostrzegawcze i mechanizmy kontrolne, zasady weryfikacji i raportowania



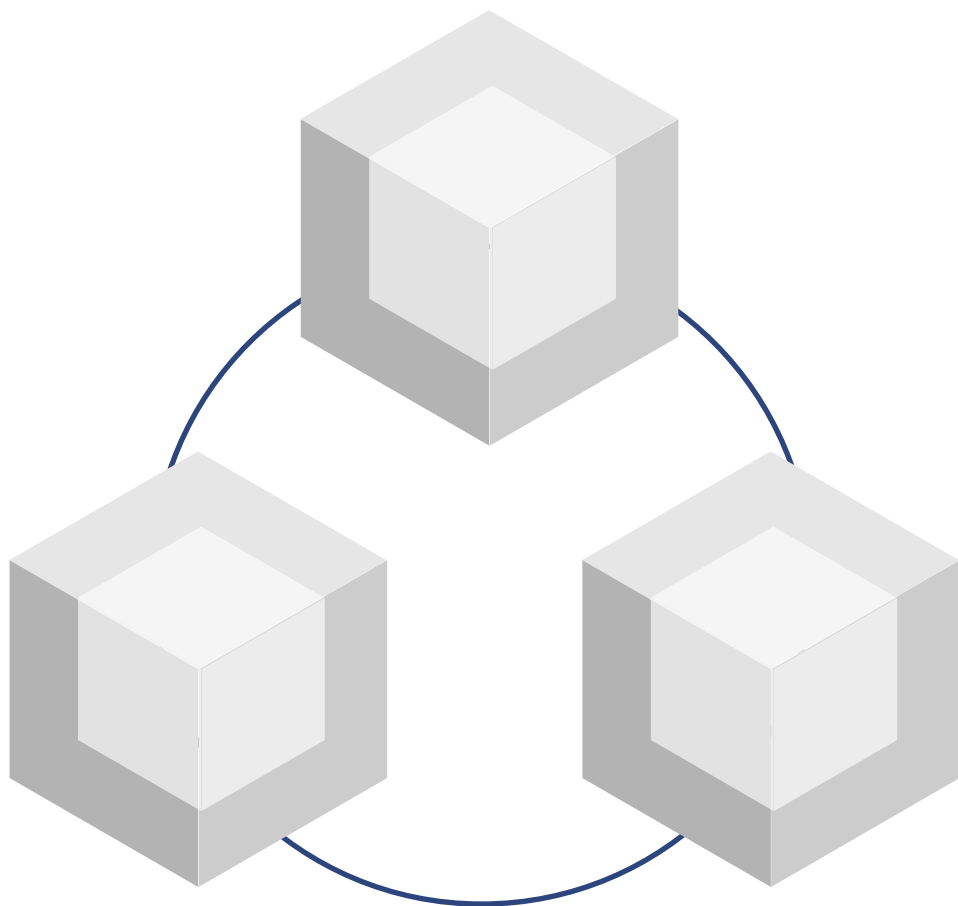


KROK 5

Szkolenia i komunikacja



Sama procedura nie wystarczy



1

PROCEDURA

- Role, odpowiedzialności i zadania
- Ogólne zasady postępowania

2

ROZWIĄZANIA ORGANIZACYJNE

- Oświadczenia i formularze
- Wzory rejestrów, szablony raportów
- Systemy IT i inne narzędzia

3

SZKOLENIA I KOMUNIKACJA

- Dedykowane szkolenia dla osób odpowiedzialnych
- Materiały onboardingowe
- Instrukcje i schematy

Co należy komunikować?

- ❏ **Procedury i polityki**
– oczekiwania względem personelu
- ❏ **Role i odpowiedzialności**
– podział kompetencji
- ❏ **Zasady zgłaszania naruszeń**
- ❏ **Zobowiązanie** (*commitment*) kierownictwa do przestrzegania procedur
- ❏ Powołanie **osób odpowiedzialnych**



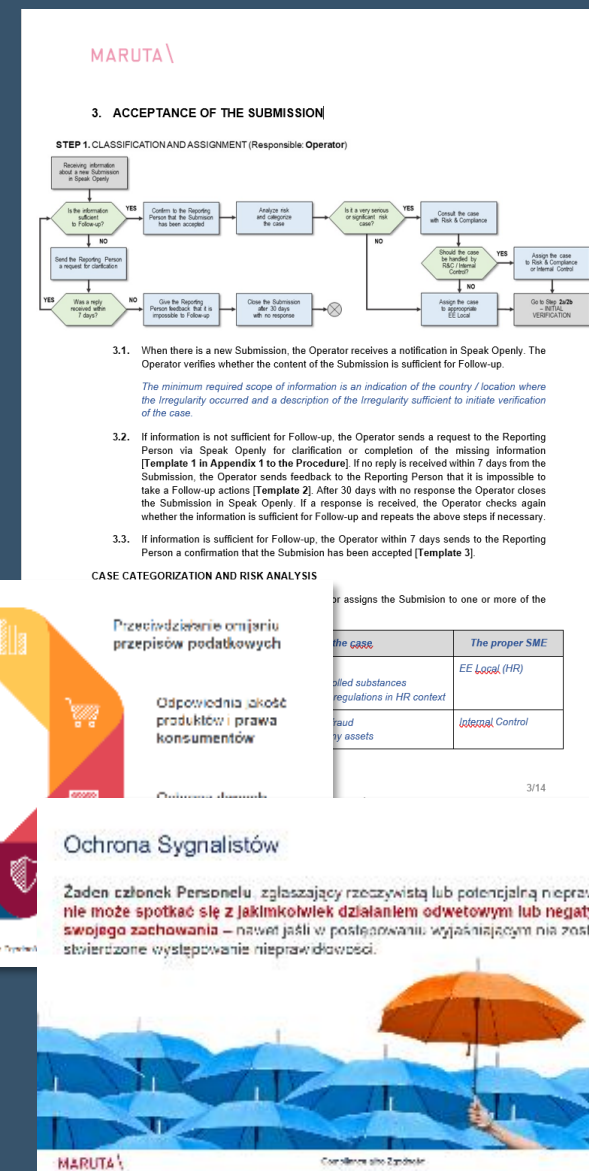
Skuteczność CMS

SZKOLENIA I KOMUNIKACJA

- 📦 Język korzyści
- 📦 Krótka, prosta i przyjazna komunikacja
- 📦 Tone from the top

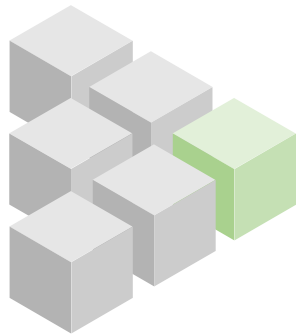
INSTRUKCJE I SCHEMATY

- 📦 Jasne zasady z przykładami
- 📦 Proste rozwiązania i ścieżka krok po kroku
- 📦 Konkretnie osoby odpowiedzialne i ich zadania



Legal design: zasady dobrej komunikacji





KROK 6

Utrzymanie zgodności



Plan Utrzymania Zgodności

- Rozliczalność
- Regularność
- Kompleksowość działań (pokrycie całej organizacji)

HARMONOGRAM UTRZYMANIA ZGODNOŚCI																														
	lip 19	sie 19	wrz 19	paź 19	lis 19	gru 19	sty 20	lut 20	mar 20	kwi 20	maj 20	cze 20	lip 20	sie 20	wrz 20	paź 20	lis 20	gru 20	sty 21	lut 21	mar 21	kwi 21	maj 21	cze 21	lip 21	sie 21	wrz 21	paź 21	lis 21	gru 21
ZADANIA STAŁE																														
1. Realizacja obowiązków określonych w Polityce przeciwdziałania Dyskryminacji i Mobbingowi	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
2. Realizacja obowiązków określonych w Polityce antykorupcyjnej	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
3. Realizacja obowiązków określonych w Polityce zarządzania Konfliktami interesów	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
4. Realizacja obowiązków określonych w Procedurze zgłaszania Nieprawidłowości i ochrony Sygnalistów	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
5. Realizacja obowiązków określonych w Procedurze zarządzania ryzykiem braku Zgodności	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
6. Realizacja obowiązków określonych w Procedurze nawiązywania współpracy z Partnerami	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
7. Realizacja obowiązków określonych w Procedurze wdrożenia Personelu i Planie szkoleń	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
8. Realizacja obowiązków określonych w Procedurze współpracy z Organami nadzorczymi	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
MIESIĘCZNA CZASOCHŁONNOŚĆ (LICZBA MH)	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42
ZADANIA CYKLICZNE																														
PRZEGLĄD PROCEDUR COMPLIANCE																														
1. Weryfikacja Polityki Compliance	8												8													8				
2. Weryfikacja Kodeksu Etyki	8												8													8				
3. Weryfikacja Polityki przeciwdziałania Dyskryminacji i Mobbingowi																														
4. Weryfikacja Polityki antykorupcyjnej																														
5. Weryfikacja Polityki zarządzania Konfliktami interesów																														
6. Weryfikacja Procedury zgłaszania Nieprawidłowości i ochrony Sygnalistów																														
7. Weryfikacja Procedury zarządzania ryzykiem braku Zgodności																														
8. Weryfikacja Procedury nawiązywania współpracy z Partnerami																														
9. Weryfikacja Procedury wdrożenia Personelu i Planu szkoleń																														
10. Weryfikacja Procedury współpracy z Organami nadzorczymi																														
11. Weryfikacja [...]																														
MIESIĘCZNA CZASOCHŁONNOŚĆ (LICZBA MH)																														
AUDYT																														
1. PROCESY HR - REKRUTACJA																														
2. PROCESY HR - OBSŁUGA ZATRUDNIENIA																														
3. PROCESY HR - ŚWIADCZENIA SOC.																														
4. PROCESY ZAKUPOWE																														
5. PROCESY SPRZEDAŻOWE																														
6. MARKETING																														
7. DZIAŁALNOŚĆ REGULOWANA [...]																														
MIESIĘCZNA CZASOCHŁONNOŚĆ (LICZBA MH)																														
CZASOCHŁONNOŚĆ ŁĄCZNE (LICZBA MH)																														

PRZEGLĄD PROCEDUR COMPLIANCE

Czynności, które należy wykonać w celu realizacji zadania:

1.

Wdrożenie zmian w przepisach prawa mających wpływ na daną Procedurę Compliance.

2.

Wdrożenie wydanych wytycznych organów nadzoru lub orzecznictwa mającego wpływ na daną Regulację Compliance.

3.

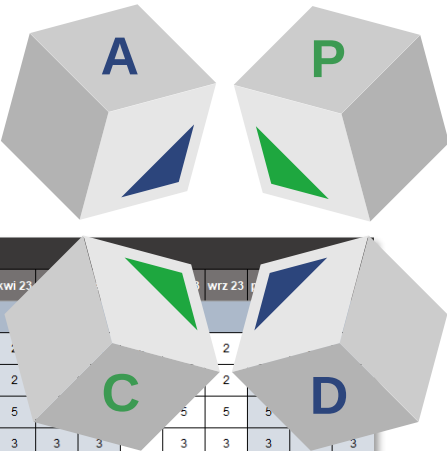
Zebranie informacji od osób odpowiedzialnych za stosowanie Procedury Compliance na temat możliwej optymalizacji jej stosowania.

4.

Weryfikacja aktualności i kompletności wzorów dokumentacji wytwarzanej w związku z realizacją Procedur Compliance.

Ewaluacja i kontrola

- ❏ Sprawdzenie poziomu świadomości pracowników (np. za pomocą testów online)
- ❏ Audyty w poszczególnych działach przeprowadzane zgodnie z Planem Utrzymania Zgodności
- ❏ Wnioski ze zgłaszanych nieprawidłowości
- ❏ Okresowe raporty dla Zarządu



COMPLIANCE PLAN		lip 22	sie 22	wrz 22	paź 22	lis 22	gru 22	sty 23	lut 23	mar 23	kwie 23	maj 23	cze 23	lip 23	sie 23	wrz 23	paź 23	lis 23	gru 23
ROUTINE TASKS: Fulfilling routine duties of the Compliance Coordinator																			
1. Risk analysis and monitoring the implementation of recommendations		2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2. Review of compliance policies and procedures		4	4	4	4	4	4	2	2	2	2	2	2	2	2	2	2	2	2
3. Conducting audits		3	3	3	3	3	3	5	5	5	5	5	5	5	5	5	5	5	5
4. Trainings (onboarding and dedicated trainings) and communication		1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
5. Receiving reports from whistleblowers		0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
6. Providing opinions on policies, procedures and other documents assigned to other organisational units		1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5
7. Reporting		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
8. Monitoring legal changes		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
AMOUNT OF TIME PER MONTH (MD)		14	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
CYCLICAL TASKS																			
REVIEW OF COMPLIANCE POLICIES AND PROCEDURES: 1. Implementation of recommendations resulting from a risk analysis, 2. Review and update of the policy / procedure, 3. Division of responsibilities,																			
1. Compliance Policy		x	x									x	x	x					
2. Procedure for Reporting Breaches of Law			x	x										x	x	x			
3. Anti-Mobbing Policy				x	x										x	x	x		
4. Supplier Code of Conduct					x	x											x	x	
5. Data Classification Policy						x	x												
6. Anti-Corruption Code and Gift Policy								x	x	x									
7. Ethics Code										x	x	x							
COMPLIANCE AUDITS IN INDIVIDUAL BUSINESS UNITS																			
1. Legal Department		x	x	x													x	x	
2. Information Security Department			x	x	x													x	x
3. Marketing Department					x	x	x												x
4. HR Department								x	x										
5. Purchase Department									x	x	x								
6. IT Department											x	x							



Wojciech Piszewski
+ 48 538 238 202
wojciech.piszewski@grclegal.pl

