

KOMPLEKSOWE PODEJŚCIE DO ZARZĄDZANIA RYZYKIEM W UJĘCIU PROCESOWYM

30 września 2026



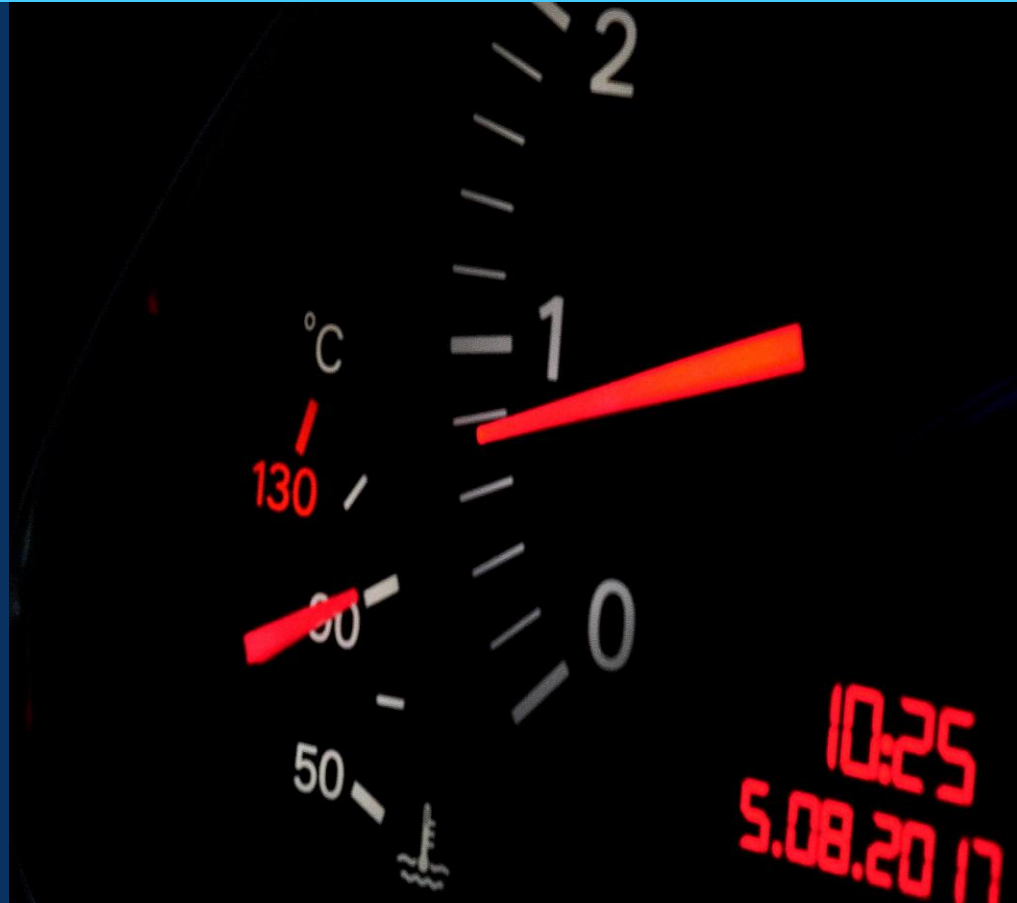
Robert Gołdecki



RYZYZKO

**„To co jest mierzone,
jest zarządzane.”**

Peter Drucker



Instytut Audytorów
Wewnętrznych IIA Polska

Problem polega na tym, że jeśli nie podejmiesz żadnego ryzyka, ryzykujesz jeszcze bardziej

/Erica Jong/

Ryzyko to możliwość zaistnienia zdarzenia, działania lub **braku działania**, które będzie miało wpływ na realizację celów organizacji.

Ryzyko może mieć charakter **zagrożenia** (negatywny) lub też **szansy** (pozytywny).



Instytut Audytorów
Wewnętrznych IIA Polska

ZARZĄDZANIE RYZYKIEM

Należy pamiętać , że zarządzanie ryzykiem:

- **NIE** sprowadza się do prowadzenia dokumentacji
- **NIE** jest jednorazowym działaniem
- **NIE** dotyczy tylko określonych pracowników
- **NIE** dotyczy tylko kwestii finansowych
- **NIE** ogranicza się do celów określonych w planie działalności
- **NIE** ogranicza się do ryzyka objętego możliwością ubezpieczenia



EFEKTYWNOŚĆ ZARZĄDZANIA RYZYKIEM

- Powinno być ściśle powiązane z realizacją celów organizacji;
- Powinno być integralną częścią procesu zarządzania;
- Powinno być skorelowane z oceną mechanizmów kontrolnych pod kątem:
 - adekwatności
 - skuteczności
 - efektywności



RYZYO

CELE z PLANU DZIAŁALNOŚCI

≠

=

?

CELE ORGANIZACJI



Instytut Audytorów
Wewnętrznych IIA Polska

PRZEGLĄD RYZYKA

Częstotliwość przeglądów – czyli im mniej wiesz, tym żyjesz dłużej i szczęśliwiej??

Reakcja na dynamikę zmian w otoczeniu.

Przegląd ryzyka, przegląd podatności, a co z przeglądem mechanizmów kontrolnych?



MECHANIZMY KONTROLNE

Ocena mechanizmów kontrolnych bez odniesienia do procesu ma sens?

Jaką wartość ma ocena pojedynczych mechanizmów kontrolnych?

Weryfikacja adekwatności, skuteczności i efektywności mechanizmów kontrolnych łącznie, z uwzględnieniem ich wzajemnych powiązań, zależności, interakcji itp.



ZARZĄDZANIE RYZYKIEM – ISTOTA PROBLEMU

**Bezpieczeństwo
Informacji
(SZBI)**

**Ochrona
Danych
Osobowych
(RODO)**

**Kontrola
Zarządcza
(Kompleksowy System
Zarządzania
Jednostką)**

**Ciągłość
działania
(BCMS)**

**Sztuczna
Inteligencja
(AI)**

Źródło: opracowanie własne



Instytut Audytorów
Wewnętrznych IIA Polska

ZARZĄDZANIE RYZYKIEM – ISTOTA PROBLEMU

Bezpieczeńst wo Informacji

- UKSC
- NIS 2
- AI Act
- ISO 27001
- ISO 27005
- polityki
- procedury
- instrukcje
- umowy

Ochrona Danych Osobowych

- RODO
- UODO
- polityka
- procedury
- instrukcje
- klauzule
- umowy

Kontrola Zarządcza

- UoFin.Publ.
- Komunikaty MF
- COSO II
- polityka KZ
- rejestry
- pozostała dokumentacja KZ

Ciągłość działania

- ISO 22301
- ISO 31000
- UKSC
- NIS 2
- polityka
- procedury
- plany ciągłości działania

Sztuczna Inteligencja

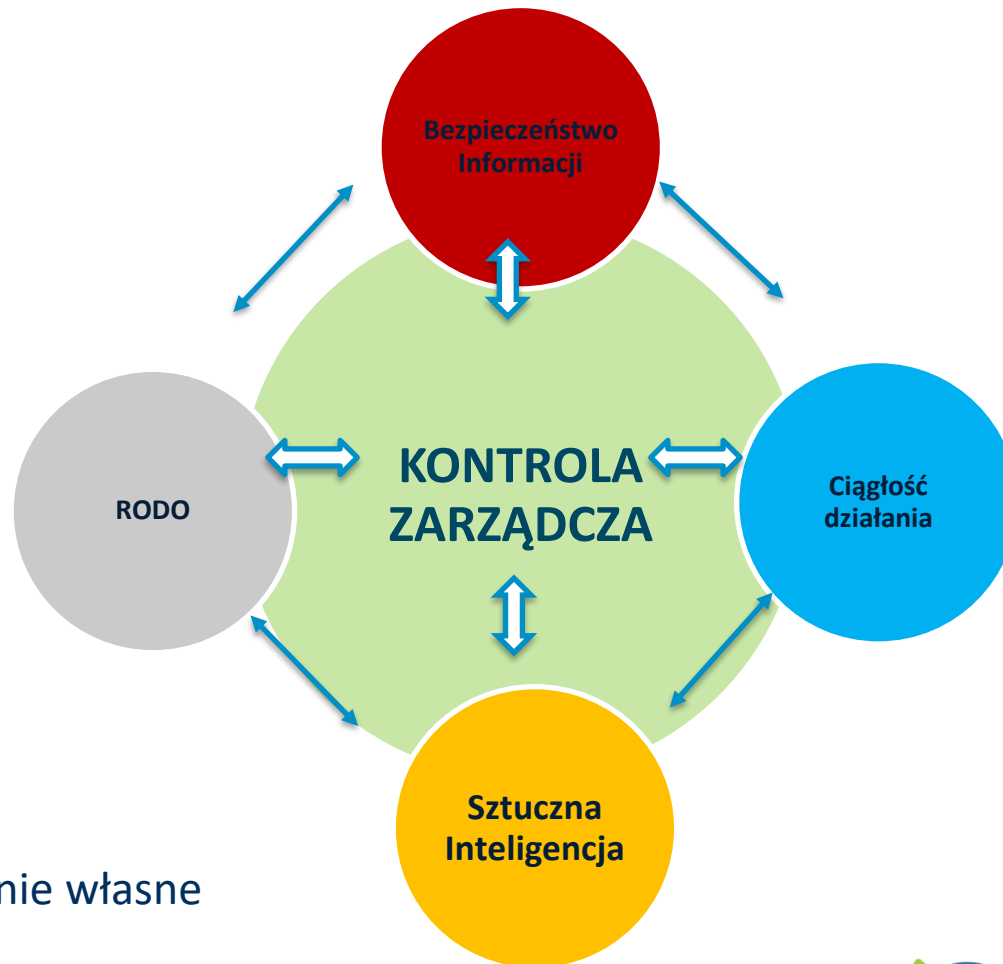
- AI Act
- ISO 42001
- polityka
- procedury
- wytyczne

Źródło: opracowanie własne



Instytut Audytorów
Wewnętrznych IIA Polska

ZARZĄDZANIE RYZYKIEM – MODEL DOCELOWY



Źródło: opracowanie własne



Instytut Audytorów
Wewnętrznych IIA Polska

PROCES

„Jeśli nie potrafisz opisać tego
co robisz jako proces,
nie wiesz co robisz”

W.E. Deming



Instytut Audytorów
Wewnętrznych IIA Polska

PROCES

Proces? Jaki proces, ja mam zadania ...

Mnie proces nie dotyczy, mam do realizacji cele ...

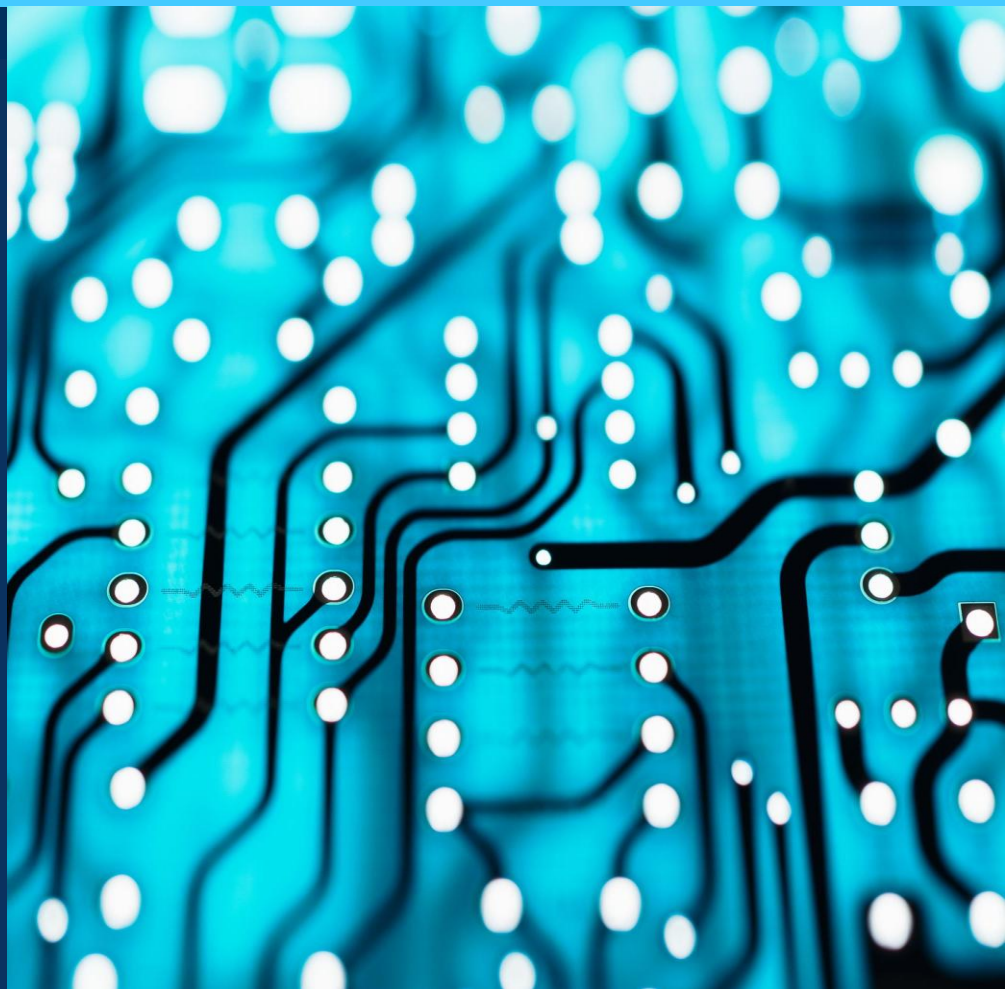
Zadanie to proces??



PROCES

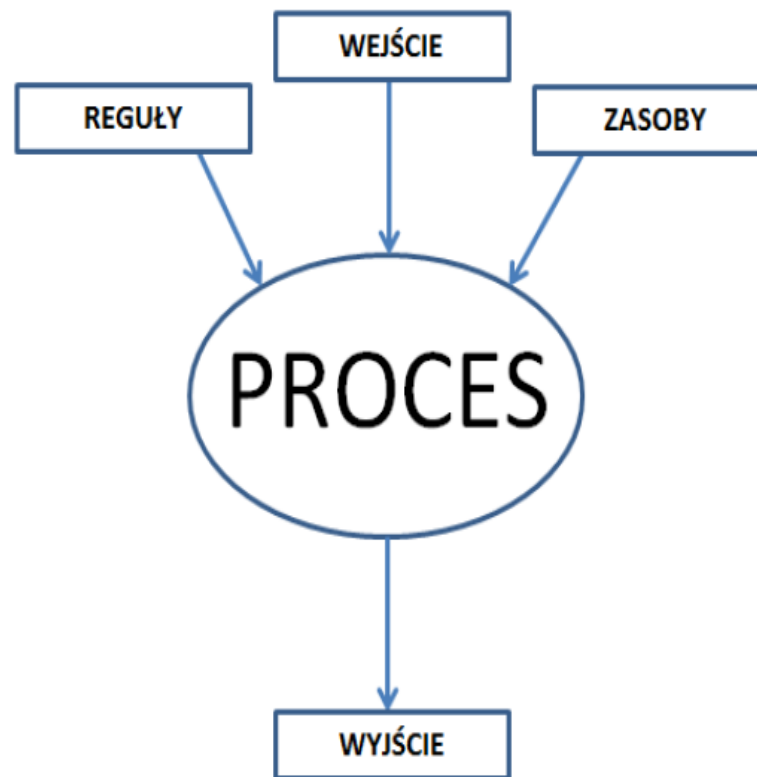
Proces - to logiczny ciąg czynności, wzajemnie ze sobą powiązanych, których realizacja jest niezbędna dla uzyskania określonego rezultatu.

Zasoby użyte do realizacji procesu przekształcają stan wejściowy w wyjściowy

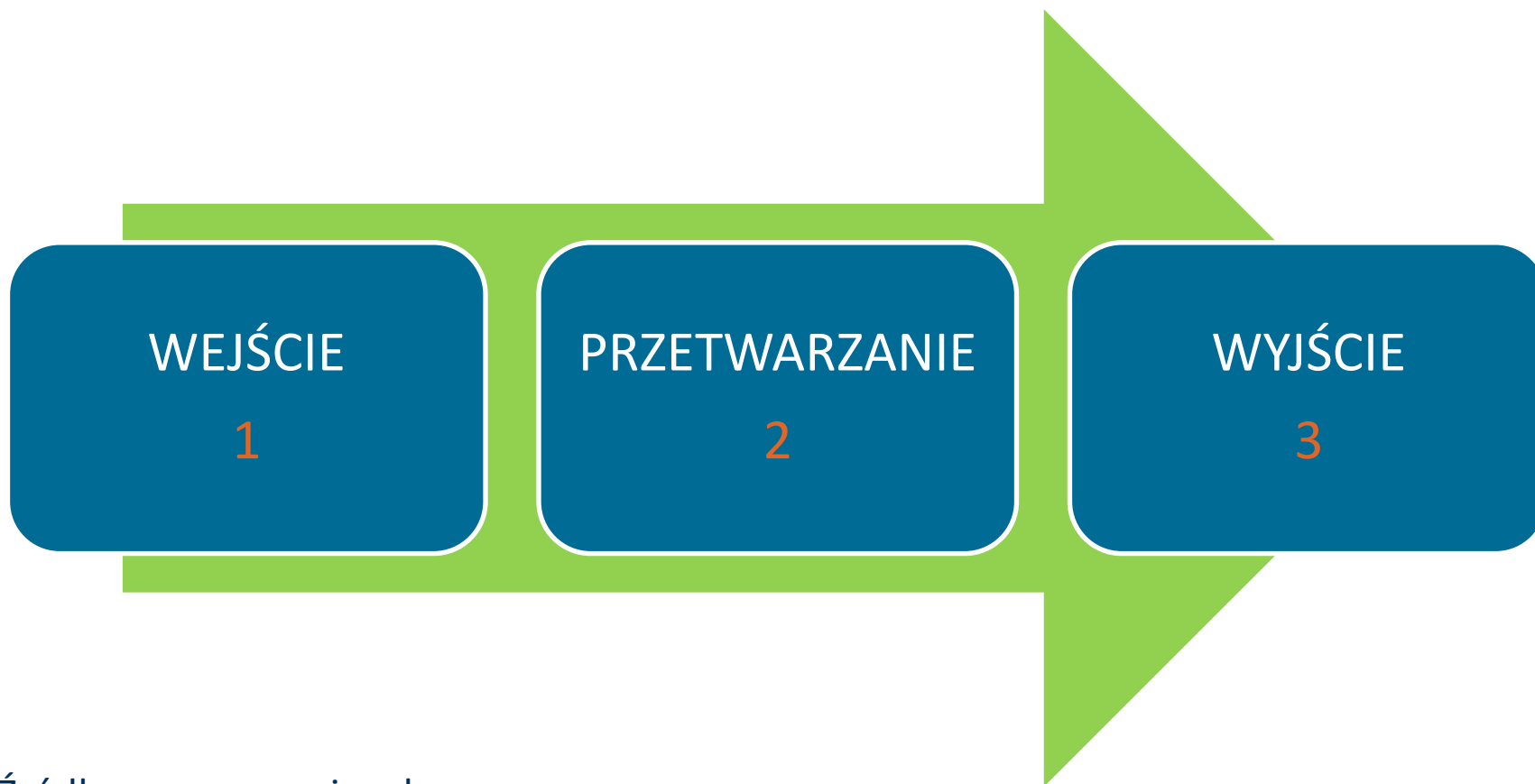


PROCES

- Każdy proces ma początek i koniec;
- Każdy proces ma **właściciela, który za niego odpowiada** (właściciel biznesowy);
- Każdy proces posiada uczestników oraz potrzebuje i wykorzystuje zasoby;
- Każdy proces wymaga narzędzi, pomiarów i kryteriów oceny;
- Każdy proces wymaga dokumentowania;
- Każdy proces wymaga doskonalenia.



PROCES



Źródło: opracowanie własne



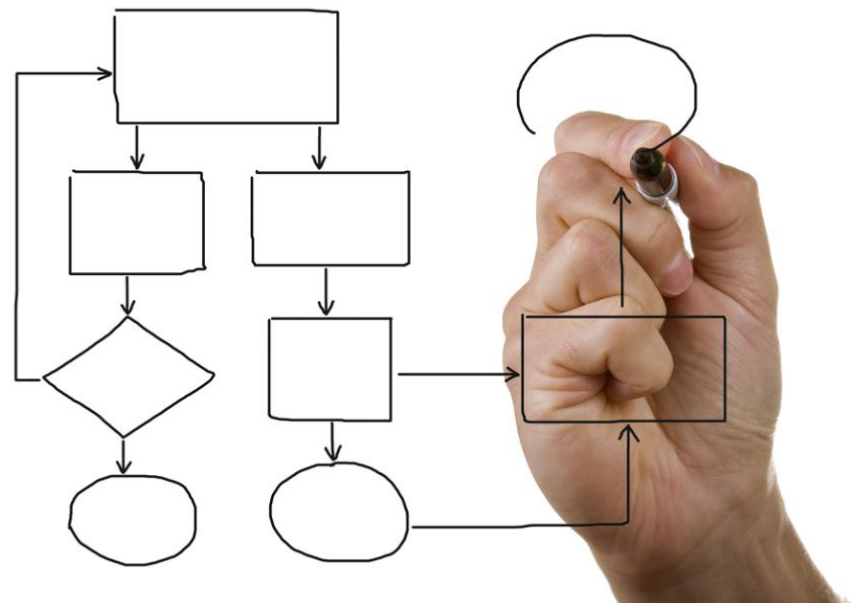
Instytut Audytorów
Wewnętrznych IIA Polska

PROCES

Mapowanie procesów

Mapa procesu – to graficzne przedstawienie procesu lub zespołu procesów i podprocesów, wraz z ich wzajemnymi powiązaniami.

Procedura – to opis procesu, ustalony sposób prowadzenia lub działania procesu.



SYMBOLE GRAFICZNE

- Dana, informacja, materiał wejściowy lub wyjściowy
- Proces, operacja, działanie
- Decyzja, test, inspekcja
- Operacja ręczna
- Dokument, zapis
- Konektor (pomiędzy poszczególnymi stronami mapy procesu)
- Terminator (początek lub koniec mapy)



PROCES

W działalności organizacji wyróżnia się następujące procesy:

- **Główne**
(Biznesowe)
- **Zarządcze**
- **Wspierające**
(Pomocnicze)



KONTEKST ORGANIZACJI

„Kultura organizacyjna
zjada strategię na
śniadanie”

Peter Drucker



Instytut Audytorów
Wewnętrznych IIA Polska

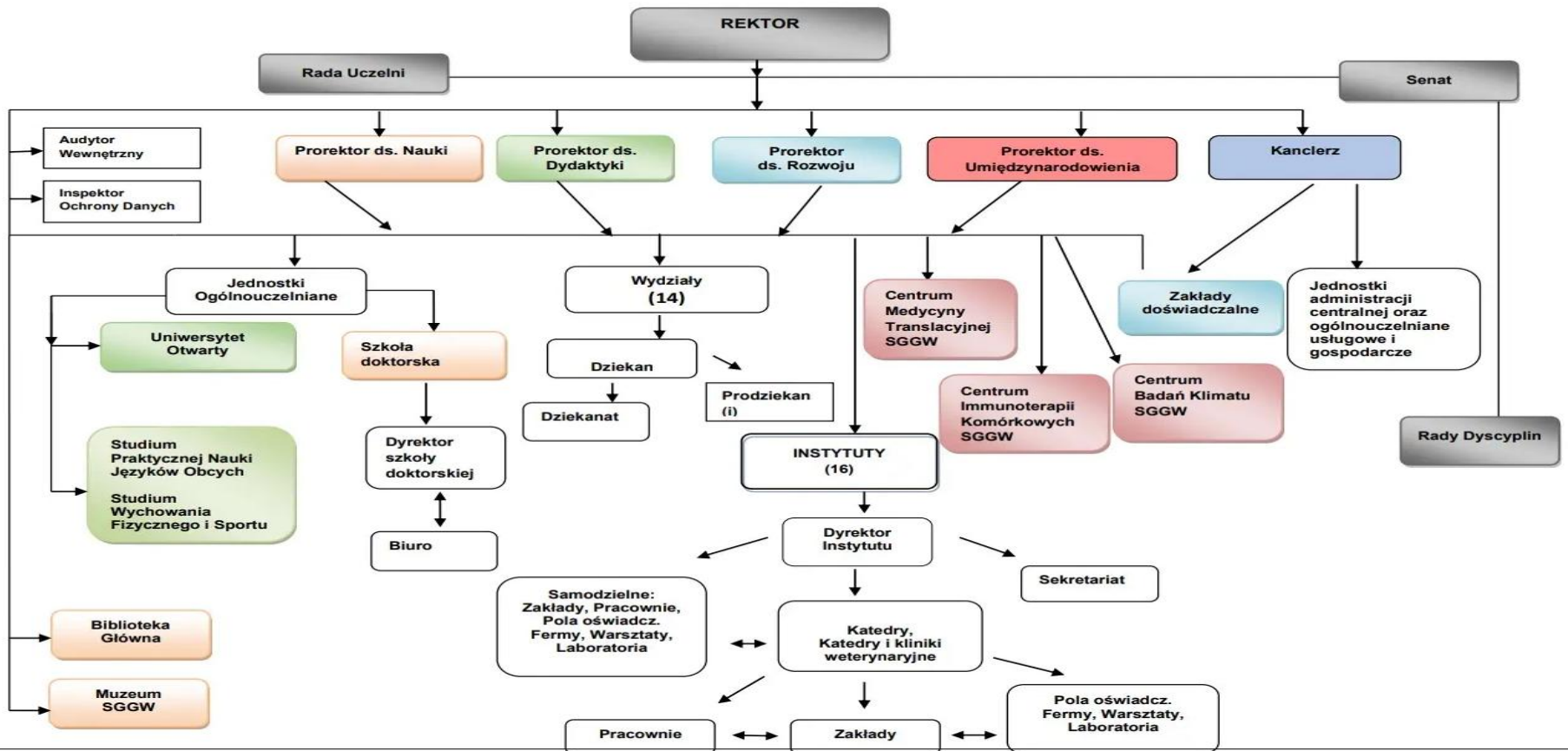
KONTEKST ORGANIZACJI

Wewnętrzny kontekst organizacji:

- **Kultura organizacyjna:** normy, wartości, zwyczaje i zachowania w organizacji;
- **Zasoby ludzkie:** umiejętności, wiedza, doświadczenie (kompetencje twarde i miękkie), wpływ na realizację celów organizacji, wpływ na realizację procesów;
- **Procesy wewnętrzne:** przebieg procesów, kryteria i wskaźniki, zasoby, odpowiedzialności;
- **Infrastruktura:** budynki, urządzenia, infrastruktura IT;
- **Strategia i cele:** kierunek działania i priorytety organizacji;
- **Zasoby finansowe:** kapitał dostępny na inwestycje, operacje i rozwój;
- **Struktura organizacyjna:** wewnętrzna organizacja pracy, hierarchia, relacje;



STRUKTURA ORGANIZACYJNA



Załącznik Nr 2 do Zarządzenia Nr 140 Rektora SGGW z dnia 31 grudnia 2025 r. zmieniającego Zarządzenie Nr 46 Rektora Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie z dnia 1 października 2019 r. w sprawie wprowadzenia

Regulaminu organizacyjnego Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie
Załącznik Nr 2 „Struktura organizacyjna Uczelni” do Regulaminu organizacyjnego SGGW

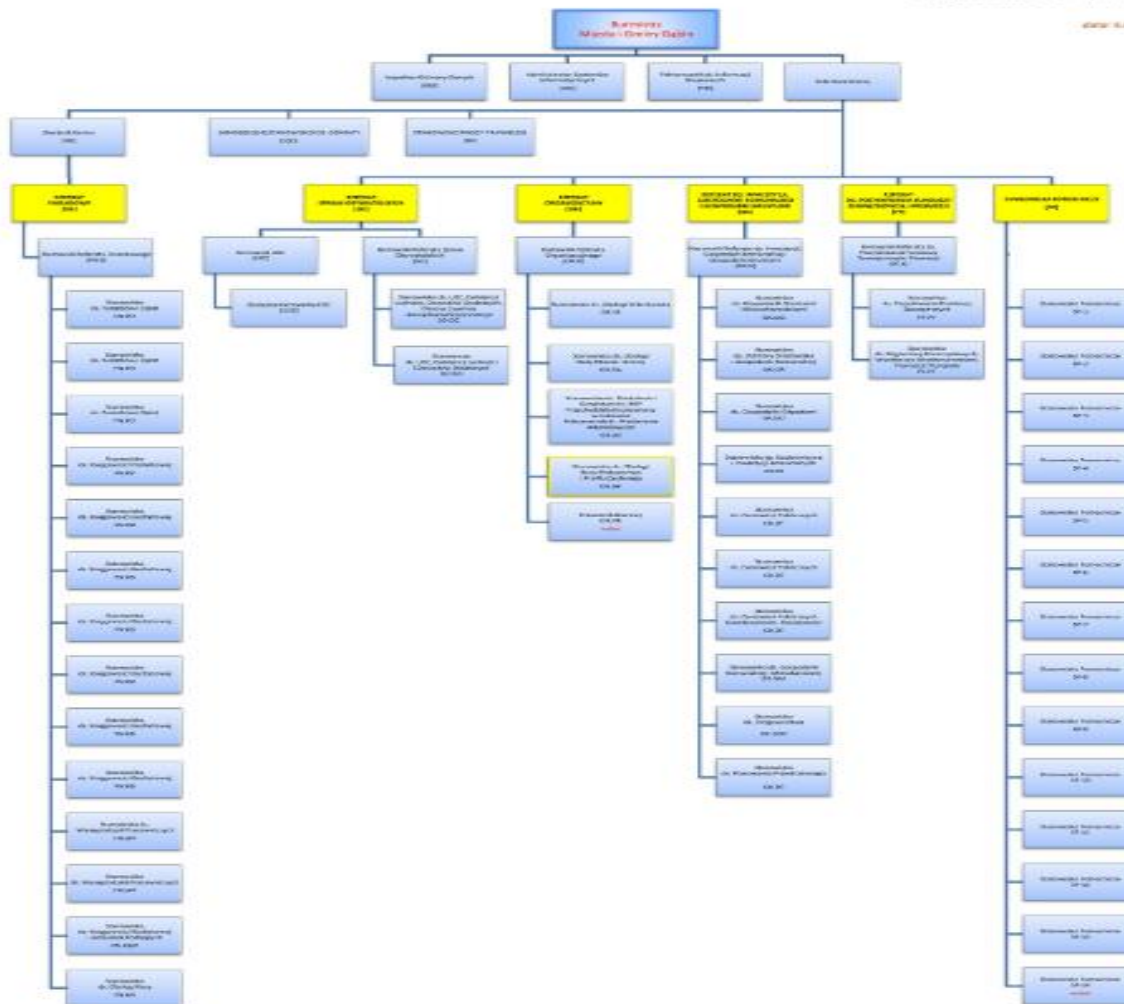


Instytut Auditorów
Wewnętrznych IIA Polska

STRUKTURA ORGANIZACYJNA

Załącznik nr 1
do Regulaminu Organizacyjnego
Urzędu Miasta i Gminy w Gąbinie

© 2007 Blackwell Publishing Ltd



KONTEKST ORGANIZACJI

Zewnętrzny kontekst organizacji:

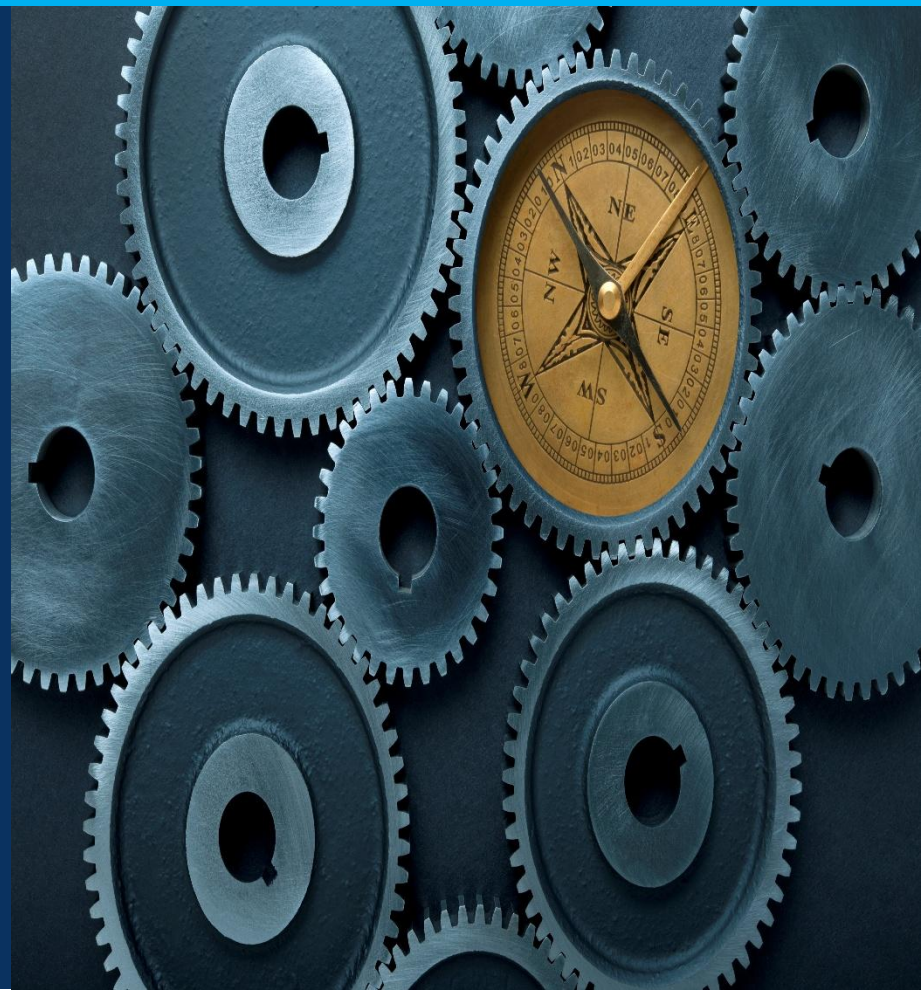
- **Otoczenie organizacyjne:** jednostki/instytucje sektora publicznego i ich zadania, podmioty prywatne, obszary działalności itp;
- **Otoczenie rynkowe:** konkurencja, klienci, dostawcy;
- **Otoczenie prawne:** przepisy, regulacje, standardy;
- **Otoczenie techniczne:** postęp technologiczny, dostęp do nowych rozwiązań;
- **Otoczenie społeczno-ekonomiczne:** wpływ czynników społecznych, demograficznych i ekonomicznych;
- **Otoczenie kulturowe:** kultura regionu, wartości społeczne i etyczne;
- **Interesariusze:** rezultaty, potrzeby i oczekiwania;



KONTROLA ZARZĄDCZA

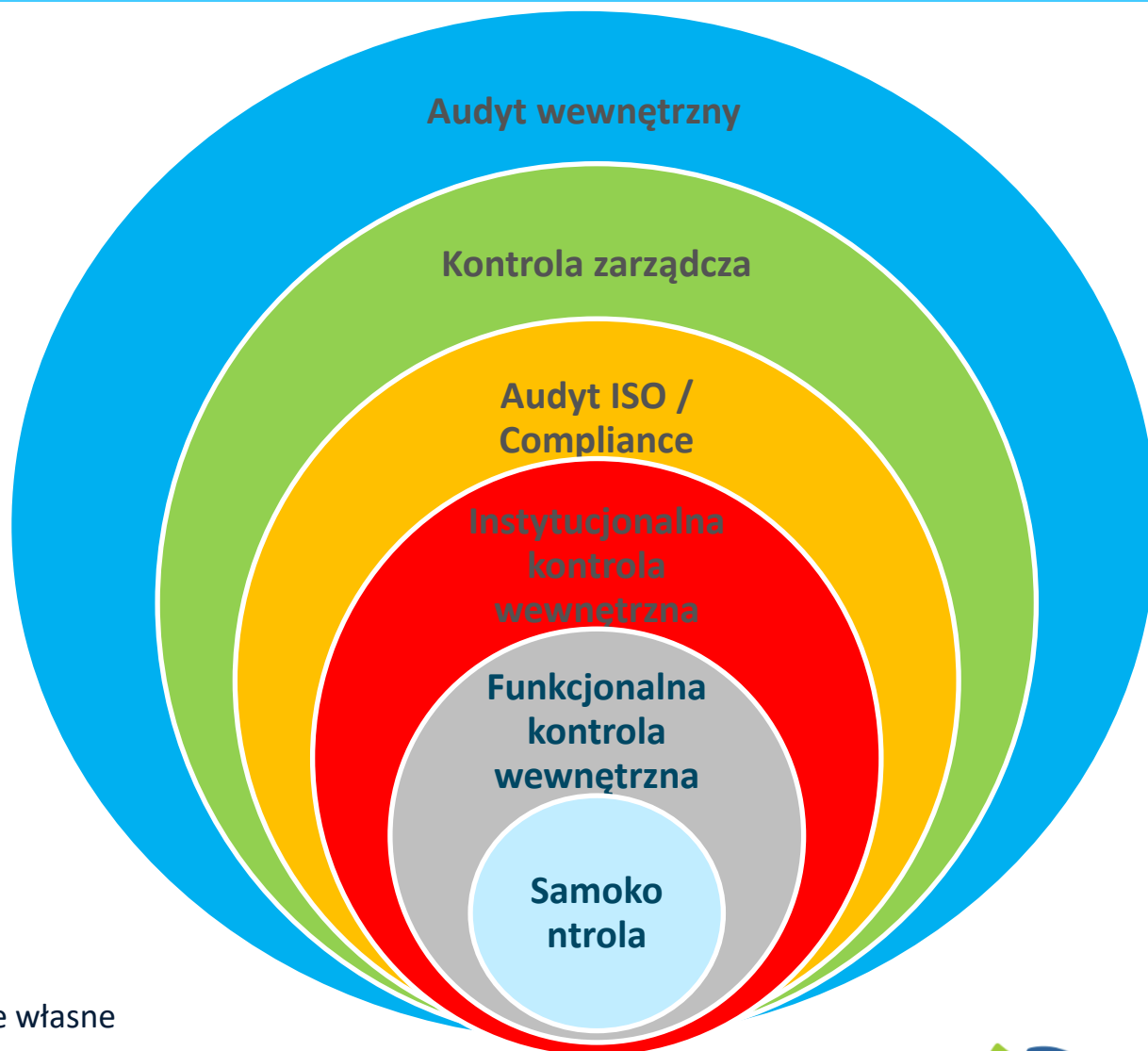
„Chodzi o to, że zdolność do wykazania się 'należyłą starannością' nie polega na posiadaniu czegoś (polityki, systemu lub sterty procedur i list kontrolnych), ale na wykonywaniu czegoś”

Max Geyer



Instytut Audytorów
Wewnętrznych IIA Polska

STRUKTURA SYSTEMU ZARZĄDZANIA ORGANIZACJĄ



Źródło: opracowanie własne



Instytut Audytorów
Wewnętrznych IIA Polska

KONTROLA ZARZĄDCZA

Kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób **zgodny z prawem, efektywny, oszczędny i terminowy**.

/źródło: art. 68 ust. 1 ustawy z 27 sierpnia 2009 r. o finansach publicznych /

Kontrola zarządcza dotyczy wszystkich obszarów działalności jednostki sektora finansów publicznych, całego kierownictwa oraz wszystkich pracowników tej jednostki. Bez wyjątku.



KONTROLA ZARZĄDCZA

Kontrola zarządcza jest plastyczna i modyfikowalna, dzięki czemu można ją doskonale dopasować do bieżących potrzeb organizacji, w pięciu podstawowych obszarach:

- A. Środowisko wewnętrzne**
- B. Zarządzanie ryzykiem**
- C. Mechanizmy kontroli**
- D. Informacja i komunikacja**
- E. Monitorowanie i ocena**

Źródło: komunikat Nr 23 Ministra Finansów z 16 grudnia 2009 r w sprawie standardów kontroli zarządczej dla sektora finansów publicznych



A. ŚRODOWISKO WEWNĘTRZNE

1. Przestrzeganie wartości etycznych.
2. Kompetencje zawodowe.
3. Struktura organizacyjna.
4. Delegowanie uprawnień.



B. CELE I ZARZĄDZANIE RYZYKIEM

1. Misja.
2. Określenie celów i zadań, monitorowanie i ocena ich realizacji.
3. Identyfikacja ryzyka.
4. Analiza ryzyka.
5. Reakcja na ryzyko.



C. MECHANIZMY KONTROLI

1. Dokumentowanie systemu kontroli zarządczej.
2. Nadzór.
3. Ciągłość działalności.
4. Ochrona zasobów.
5. Szczegółowe mechanizmy kontroli dotyczące operacji finansowych i gospodarczych.
6. Mechanizmy kontroli dotyczące systemów informatycznych.



D. INFORMACJA I KOMUNIKACJA

1. Bieżąca informacja.
2. Komunikacja wewnętrzna.
3. Komunikacja zewnętrzna.



E. MONITOROWANIE I OCENA

1. Monitorowanie systemu kontroli zarządczej.
2. Samoocena.
3. Audyt wewnętrzny.
4. Uzyskanie zapewnienia o stanie kontroli zarządczej.



Największe zagrożenia dla przetwarzanych danych i zasobów informacyjnych pochodzą z wewnątrz organizacji.

/własne/



ISTOTNE RYZYKA

- Nieuprawniony (nieautoryzowany) dostęp do danych;
- Nieuprawnione przetwarzanie danych:
 - przeglądanie,
 - kopiowanie,
 - fałszowanie,
 - usuwanie;
- Utrata danych / utrata ważnych zasobów informacyjnych;
- Utrata fizycznych nośników danych;
- Awarie sprzętowe;



ISTOTNE RYZYKA

- Niezgłaszanie incydentów;
- Komunikaty false-positive;
- Nieuprawnione zarządzanie incydentami;
- Atak na systemy teleinformatyczne;
- Utrata dostępu do danych (czasowa lub trwała);
- Nieautoryzowane działania pracowników;
- Nieautoryzowany dostęp do infrastruktury IT po stronie dostawcy;
- Awaria po stronie dostawcy;



ISTOTNE RYZYKA

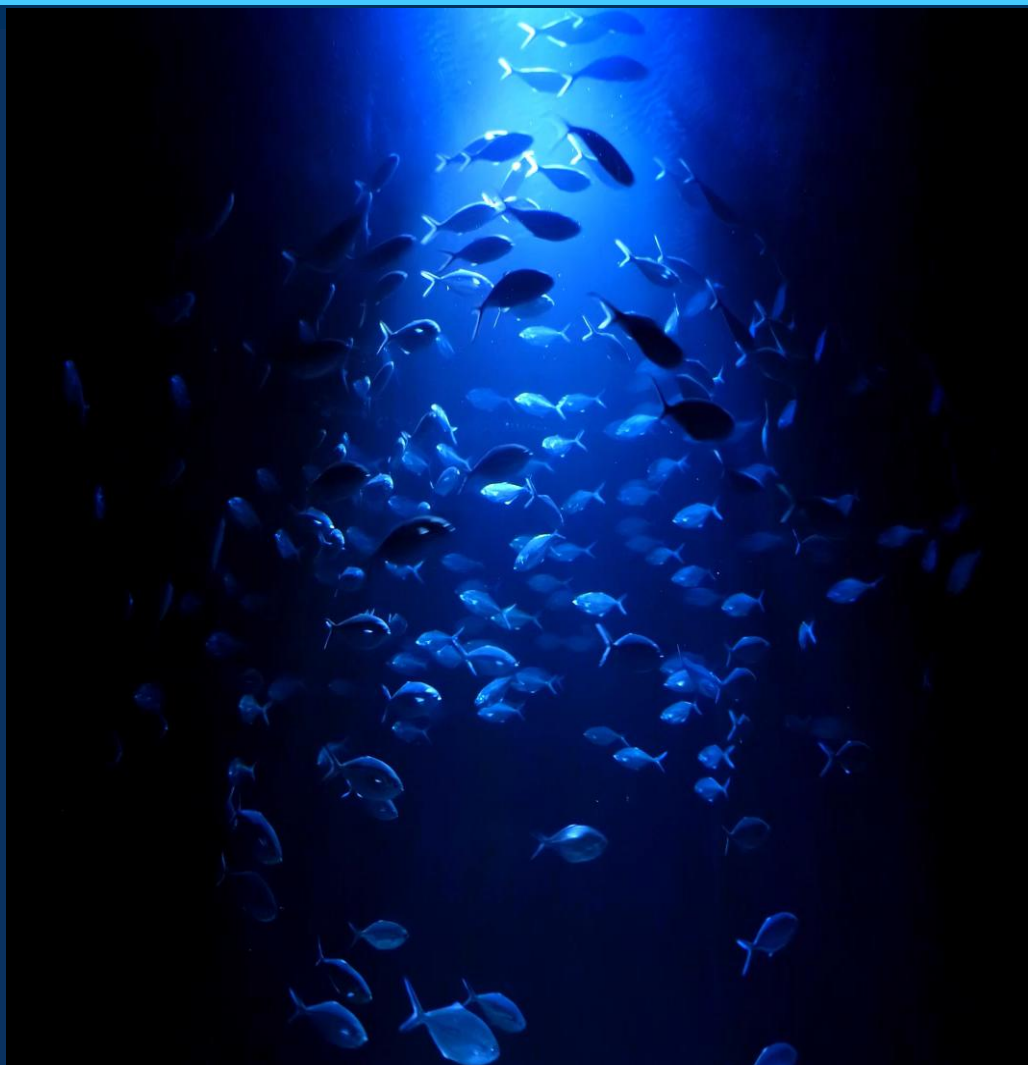
- Konflikt interesów;
- Zachowania korupcyjne;
- Nieautoryzowany dostęp do stref przetwarzania danych.



RYZYKA KRYTYCZNE - SOCJOTECHNIKA

Spoofing:

- **Phishing e-mail** (w tym Spearphishing, Whaling, Business Email Compromise)
- **Vishing**
- **Smishing**
- **Quishing**
- **Fałszywe domeny**
- **Tailgating**



AI – NOWE ZAGROŻENIE DLA BEZPIECZEŃSTWA

W wielu organizacjach AI wdrożona jest bez strategii, bez zabezpieczeń, bez świadomości ryzyka.

- **Shadow AI** – nieautoryzowane użycie narzędzi AI przez pracowników
- **Agent AI** – automatyzacja działań w imieniu użytkowników (np. obsługa poczty e-mail, uruchamianie kodu)

Czy na pewno wiemy kto w organizacji, jak i kiedy używa narzędzi AI?



PODATNOŚCI

Podatności - to słabości, luki w zabezpieczeniach lub braki odporności, które mogą zostać wykorzystane przez zagrożenie (składowe ryzyka).

Podatności wykorzystywane są między innymi do kradzieży danych, kradzieży środków finansowych, przejęcia kontroli nad kontem, systemami, zakłócenia działania usług, naruszenia prywatności, strat finansowych.



Ryzyko: ATAK NA SYSTEMY INFORMATYCZNE

Kategoria ryzyka: bezpieczeństwo informacji

Podatności:

- nieprawidłowe zabezpieczenia lub ich brak (np. brak ochrony antywirusowej;
- nieaktualne oprogramowanie antywirusowe na stacjach roboczych i urządzeniach mobilnych);
- brak aplikacji typu VPN, ZTNA chroniących zdalną komunikację z urządzeniami sieciowymi, na których przetwarzane są dane, lub niewłaściwa konfiguracja tych aplikacji;
- brak inwentaryzacji zasobów informatycznych pozwalających na pracę w sieci obcych stacji roboczych i obcych urządzeń mobilnych;



PODATNOŚCI

- brak systematycznego nadzoru nad stacjami roboczymi użytkowników;
- nieświadomość pracowników;
- brak adekwatnych procedur;
- nieprzestrzeganie zapisów procedur/polityk bezpieczeństwa;
- brak rozwiązań mitygujących lawinowe przyrosty zapytań skutkujące odmową świadczenia usług;
- rozwój AI stwarzający możliwości generowania nowych rodzajów ataków, ułatwiający ataki osobom bez umiejętności technicznych.



Ryzyko: ATAK NA SYSTEMY INFORMATYCZNE

- **Kategoria ryzyka:** bezpieczeństwo informacji

Objaśnienia

- **VPN** - (Virtual Private Network) to wirtualna sieć prywatna, która chroni połączenie internetowe i tożsamość online. VPN szyfruje dane i ukrywa adres IP użytkownika. Tworzy zaszyfrowany tunel między komputerem użytkownika i serwerem.
- **ZTNA** - (Zero Trust Network Access) to nowoczesne podejście do bezpieczeństwa sieci, które zakłada brak zaufania do żadnego użytkownika ani urządzenia, dopóki nie zostaną zweryfikowane. Zamiast otwartego dostępu do całej sieci, ZTNA zapewnia bezpieczny dostęp do konkretnych zasobów tylko po zweryfikowaniu tożsamości i uprawnień użytkownika.



Ryzyko: NIEEFEKTYWNY PRZEPŁYW INFORMACJI MIĘDZY KOMÓRKAMI ORGANIZACYJNYMI

Kategoria ryzyka: organizacyjne

Podatności:

- problemy w przekazywaniu dokumentów;
- błędne przekazywanie;
- przetrzymywanie;
- nieprzykazywanie;
- wydłużony czas przekazywania;
- przekazanie do niewłaściwej komórki organizacyjnej;
- spory kompetencyjne między komórkami organizacyjnymi;

PODATNOŚCI

- problemy komunikacyjne w pracy zdalnej;
- niewłaściwa obsługa EZD, poczty elektronicznej;
- brak kierunkowych wytycznych, brak lub niesprawność stosowanych kanałów informacyjnych;
- niejednolite wykonywanie zadań;
- brak wymiany obserwacji i spostrzeżeń wynikających z bieżącej realizacji zadań;
- niejasne komunikaty, brak informacji zwrotnej od przełożonych.



MECHANIZMY KONTROLNE

„ Brak planowania to
planowanie porażki”

Benjamin Franklin



Instytut Audytorów
Wewnętrznych IIA Polska

KRYTERIA OCENY MECHANIZMÓW KONTROLNYCH

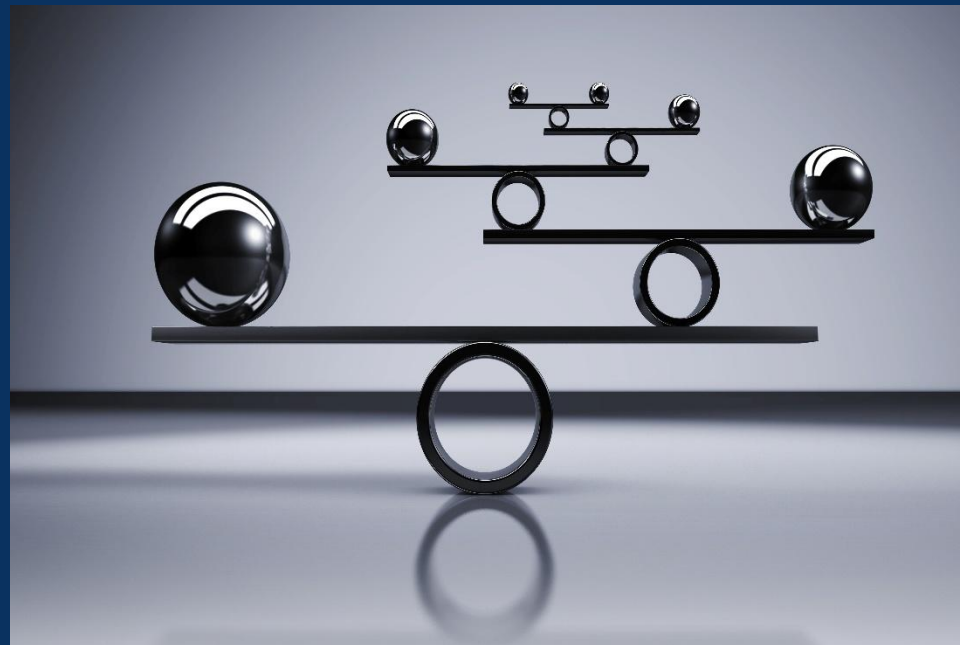


- **Adekwatność**
- **Skuteczność**
- **Efektywność**



MECHANIZMY KONTROLNE

- Wdrożenie strategii bezpieczeństwa
- Wdrożenie polityki bezpieczeństwa informacji
- Wdrożenie polityki bezpieczeństwa fizycznego i osobowego
- Wdrożenie instrukcji i procedur
- Polityka – Internet / Intranet
- Wdrożenie BCMS



MECHANIZMY KONTROLNE

- Zarządzanie kopiami zapasowymi – polityka backupu;
- Zarządzanie aktualizacjami oprogramowania – polityka informatyczna;
- Zarządzanie niszczeniem dysków HDD i SSD i pamięci RAM zawierających dane;
- Systemy wykrywania i prewencji (IDS/IPS);
- SOC (Security Operations Center) i NOC (Network Operations Center);
- Oprogramowanie klasy SIEM i platforma SPLUNK;
- Zarządzanie urządzeniami peryferyjnymi;



SIEM

Oprogramowanie SIEM (Security Information and Event Management) – to typ oprogramowania, które znacznie zwiększa cyberbezpieczeństwo.

W czasie rzeczywistym zbiera, analizuje i koreluje logi z różnych źródeł (serwery, routery, zapory, sieci) oraz przewiduje i ekspresowo alarmuje.

Pozwala na natychmiastowe wykrywanie zagrożeń, śledzenie incydentów oraz raportowanie zgodności zwiększając cyberodporność.

Źródło: <https://gdata.pl/przewodnik/co-to-siem>



Instytut Audytorów
Wewnętrznych IIA Polska

SPLUNK

Platforma SPLUNK – to zaawansowana platforma klasy Big Data do przeszukiwania, monitorowania i analizy bardzo dużych zbiorów danych maszynowych (logów) w czasie rzeczywistym.

Umożliwia zbieranie informacji z całej infrastruktury IT, wizualizację danych na dashboardach oraz wykrywanie zagrożeń (SIEM) i incydentów bezpieczeństwa. Działa w modelu lokalnym (Enterprise) lub w chmurze (Cloud Platform)

Źródło: <https://linuxpolska.com/pl/technologie/splunk/>



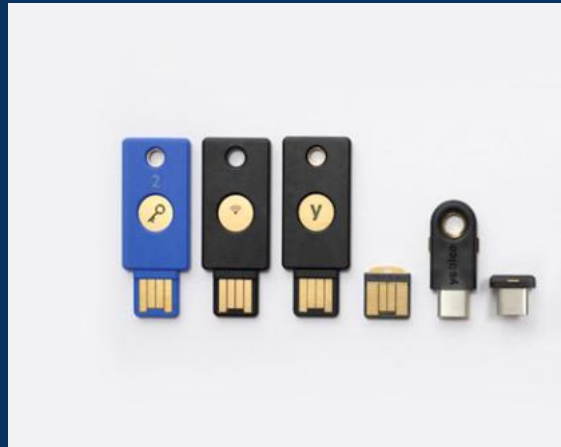
MECHANIZMY KONTROLNE

- Blokowanie portów – polityka użytkowania przenośnych pamięci zewnętrznych;
- Domena – adresy www i email;
- Poczta email służbowa – blokowanie dostępu do komercyjnych skrzynek poczty email;
- Monitorowanie aktywności użytkowników w sieci;
- Monitorowanie treści poczty email;
- Zasada „Zero Trust”;
- Uwierzytelnianie i autoryzacja;



MECHANIZMY KONTROLNE

- Definiowanie ról użytkowników;
- Uprawnienia dostępów zgodne z zakresami obowiązków;
- Hasła dostępu – min. 14 znaków (rekomendacja CERT Polska);
- Uwierzytelnianie **2FA** i **MFA** (Multi-Factor Authentication);
- Klucze U2F;



MECHANIZMY KONTROLNE

- Specjalistyczne stanowiska/zespoły do zarządzania incydentami;
- Obsługa incydentów:
 - wykrywanie,
 - rejestrowanie,
 - analizowanie,
 - klasyfikowanie,
 - priorytetyzacja,
 - podejmowanie działań naprawczych,
 - ograniczanie skutków incyduentu.



MECHANIZMY KONTROLNE

- Inwentaryzacja zasobów
/kto i skąd może połączyć się urządzeniami; jakie urządzenia pracują w naszej sieci; liczba punktów dostępowych i eliminacja zbędnych punktów/;
- Segmentacja sieci
/rozdzielenie systemów biurowych od biznesowych/;
- Plany awaryjne (what if?)
/przygotowanie scenariuszy na wypadek ataku, aby każdy pracownik wiedział jakie kroki podjąć/.



KLUCZOWE DZIAŁANIA W WYBRANYCH OBSZARACH

„Kto zna wroga i zna siebie, nie będzie zagrożony choćby i w stu starciach.

Kto nie zna wroga, ale zna siebie, czasem odniesie zwycięstwo, a innym razem zostanie pokonany.

Kto nie zna ani wroga, ani siebie, nieuchronnie ponosi klęskę w każdej walce.”

Sun Tzu



Instytut Audytorów
Wewnętrznych IIA Polska

Dziękuję za uwagę



Instytut Audytorów
Wewnętrznych IIA Polska

DANE KONTAKTOWE

Robert Gołdecki

LinkedIn: <https://www.linkedin.com/in/robertgoldecki/>



Instytut Audytorów
Wewnętrznych IIA Polska