



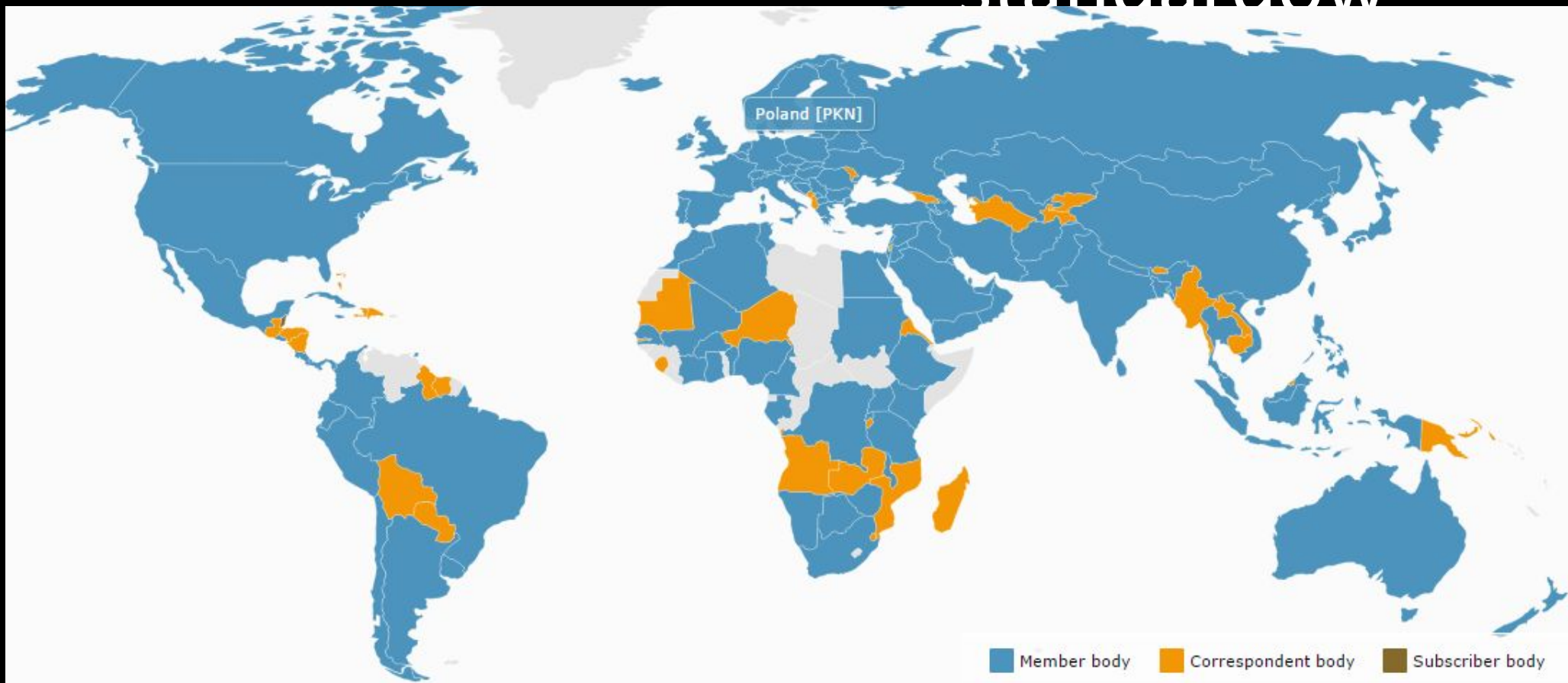
Uniwersytet  
Wrocławski

# ISO normy w IT



International  
Organization for  
Standardization

1946r. London  
Swissland  
16,5 tys.  
standardów





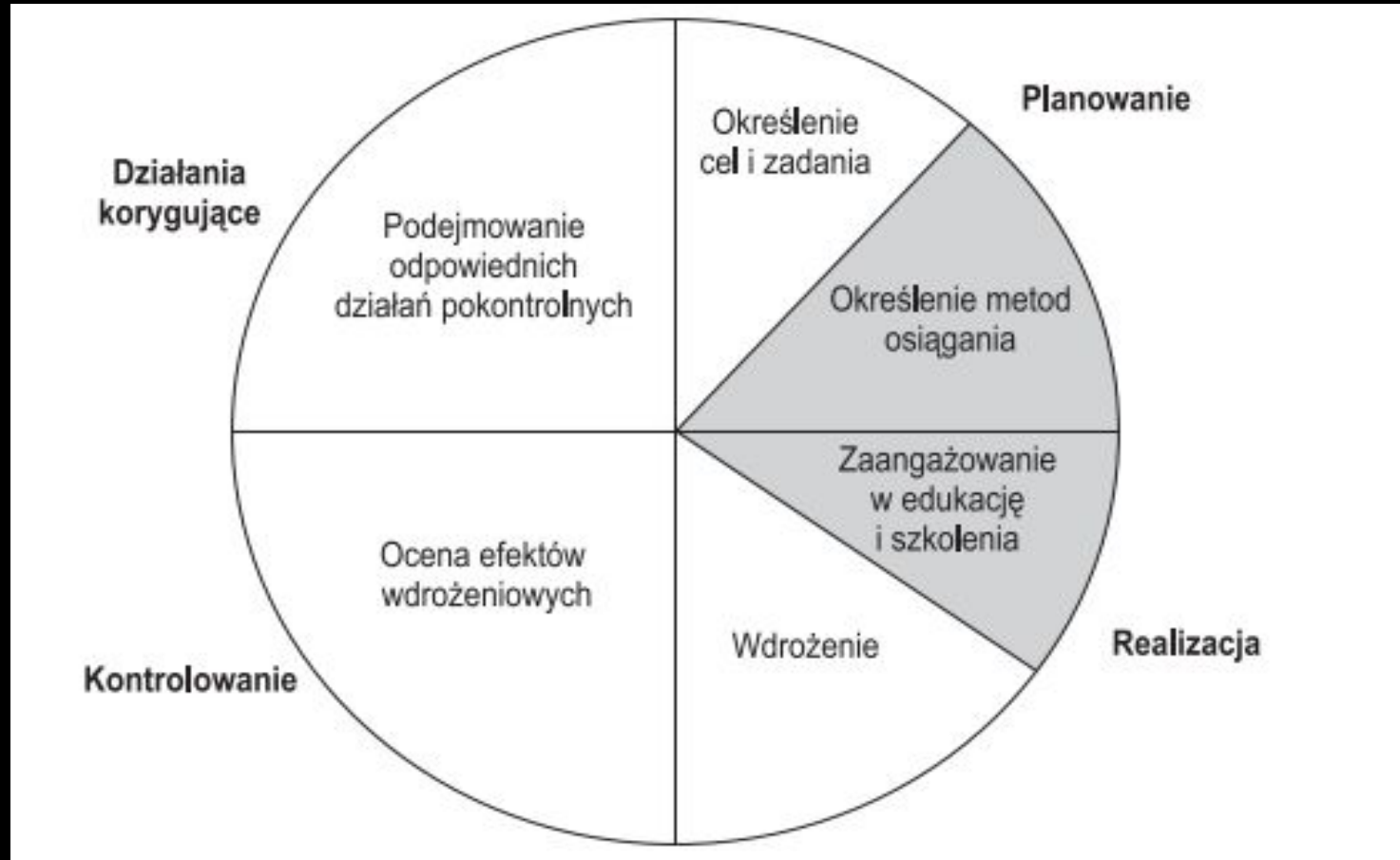
## Certyfikacja dobrowolna



dobrowolny certyfikat zgodności.

## Certyfikacja obowiązkowa

# PLAN->DO->CHECK->ACT



cztery etapy koła Deminga

# Po co się męczyć?



- Wymogi zamawiających ( międzynarodowych inwestorzy)
- Obowiązkowe umowy dla przetargów
- Konieczność zwiększenia ryzyko dla bezpieczeństwa
- Zmniejszenie liczby i kosztów wypadków
- Kreowanie pozytywnego wizerunku firmy, bezpiecznego i nowoczesnego

orange™

## Różnica między standardami:

- **ISO 9001** Are your customers happy? Do you deliver what your contract requires?
- **ISO 20000** Think ITIL and running an IT Sustainment organization well, including things like help desk operations
- **ISO 27000** Think cyber security best practices/standards



Uniwersytet  
Wrocławski

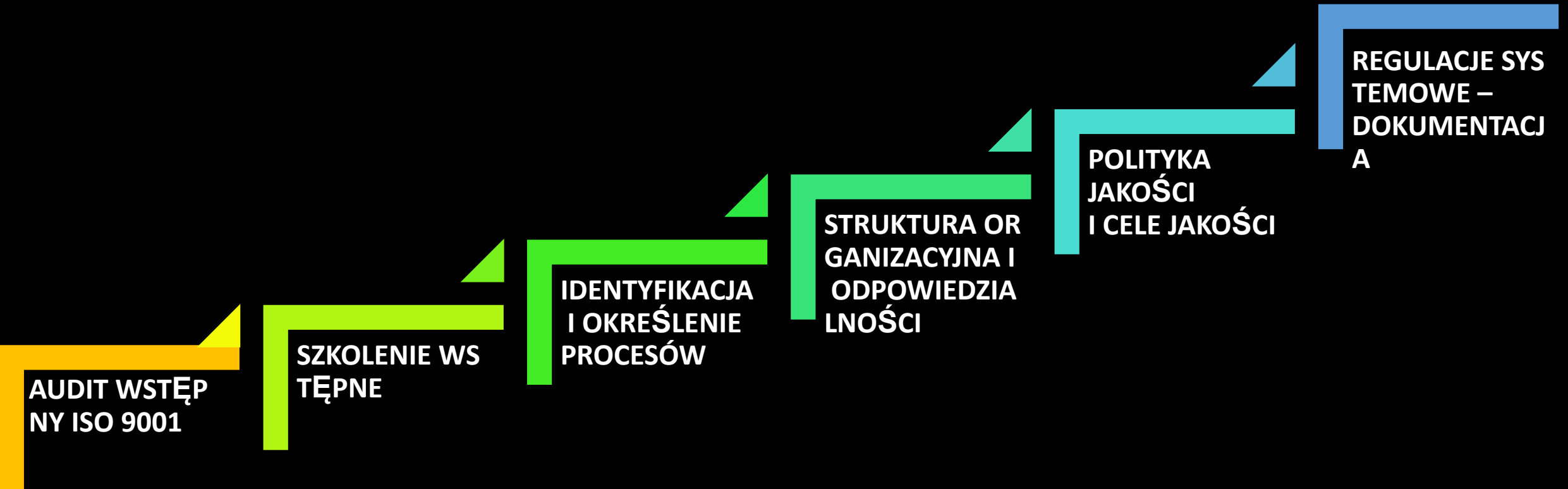
# ISO 9001

## 1. Odnobitowa certyfikacja

**Audyt**            1 rok

**Recertyfikacja**      3 lata

# Wdrożenie Systemu Zarządzania Jakością opisanego normą ISO 9001:2008





# Wdrożenie Systemu Zarządzania Jakością opisanego normą ISO 9001:2008

**KSIĘGA JAKOŚCI**

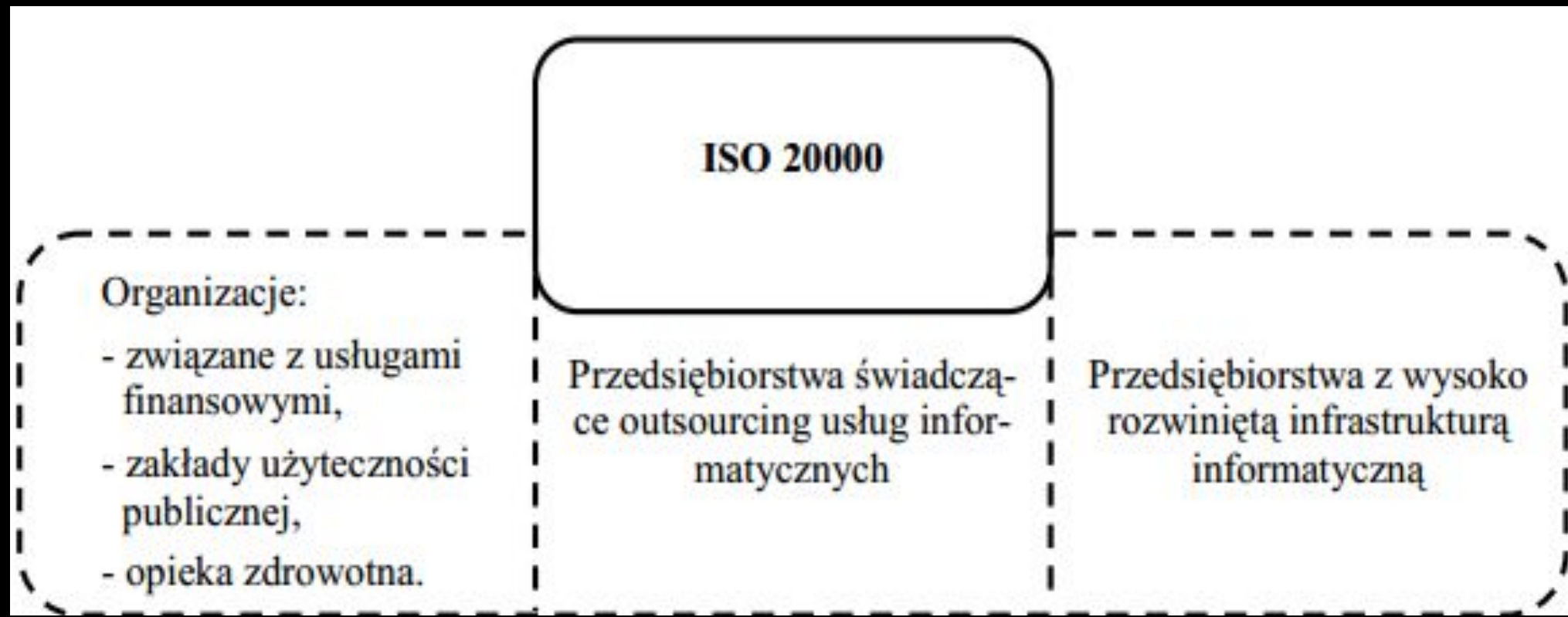
**SZKOLENIA  
PRACOWNIKÓW Z  
ZAKRESU  
NOWYCH  
REGULACJI –  
WDROŻENIE**

**AUDITY  
WEWNĘTRZNE  
ISO 9001**

**AUDIT  
CERTYFIKUJĄCY  
ZGODNOŚĆ Z  
WYMAGANIAMI  
ISO 9001**

# ISO 2000

- PN-ISO/IEC 20000-1: 2007 - Technika informatyczna - Zarządzanie usługami - Część 1: Specyfikacja
- PN-ISO/IEC 20000-2: 2007 - Technika informatyczna - Zarządzanie usługami - Część 2: Reguły postępowania.





ISO 2000 - Wdrożenie efektywne procesu zarządzania zdarzeniami w ramach organizacji będzie miało następujące korzyści:

ZARZĄDZANIE DOSTAWCĄ	ZARZĄDZANIE ŁAŃCUCHEM DOSTARCZANIA USŁUG	ZGODNOŚĆ Z WYMAGANIAMI KLIENTA	LEPSZE ZROZUMIENIE ORGANIZACJI
COST REDUCTION	POSZANOWANIE ZAINTERESOWANYCH STRON	OCHRONA REPUTACJI ORAZ MARKI	REPUTACJA
PRZEWAGA KONKURENCYJNA	ZGODNOŚĆ Z PRZEPISAMI PRAWA	EWALUACJA, PORÓWNANIE ORAZ ULEPSZANIE USŁUG	ZGODNOŚĆ Z UMOWĄ

# WDRAŻANIE ZA POMOCĄ METODOLOGII IMS2

## ZAPLANUJ

1.1 Określić zakres

1.2 Przegląd  
Odpowiedzialność

1.3 Zarządzanie i  
Firmy Zewnętrzne

1.4 Zarządzanie  
Dokumentacją  
Zarządzania

1.5 Zarządzanie  
Zasobami

1.6 Plan Zarządzania  
Usługami

## WYKONAJ

2.1. Projektowanie i  
Przechodzenie na Nowe  
lub Zmienione Usługi

2.2 Proces Dostarczania  
Usług

2.3 Procesy dot.  
Relacji

2.4 Procesy dot.  
Rozwiązywania  
Problemów

2.5 Procesy  
Kontrolne

## SPRAWDŹ

3.1 Monitorowanie i  
Mierzenie

3.2 Audyt  
Wewnętrzny

3.3 Przegląd  
Zarządzania

## POPRAW

4.1 Określenie braków  
zgodności

4.2 Obsługa braków  
zgodności

4.3 Trwałe  
ulepszanie



## INFRASTRUKTURA

- Budynki, pomieszczenia
- Systemy zasilające
- Systemy klimatyzacyjne
- Systemy przeciwpożarowe i gaśnicze
- Systemy kontroli dostępu i monitoringu
- Serwery i łącza sieciowe pomiędzy nimi
- Najczęściej infrastruktura należy do jednego właściciela, np. uczelni, urzędu, banku



## SYSTEM KLIMATYZACJI

- Klimatyzacja rzędowa, precyzyjna, zamknięte szafy
- Czynnik chłodzący – freon, woda, glikol
- Bezpośrednie chłodzenie komponentów cieczą
- Redundancja
- Temperatura czynnika i pomieszczenia
- Monitoring i sterowanie poszczególnych elementów układu
- Uszczelnianie szaf serwerowych, zabudowa korytarzy
- Testy poprawności działania

## BACK-UP

W przestrzeni użytkownika:

- rdiff-backup
- rsnapshot
- Areca backup
- Duplicati

W przestrzeni infrastruktury wirtualnej:

- Vmware data protection
- Veeam

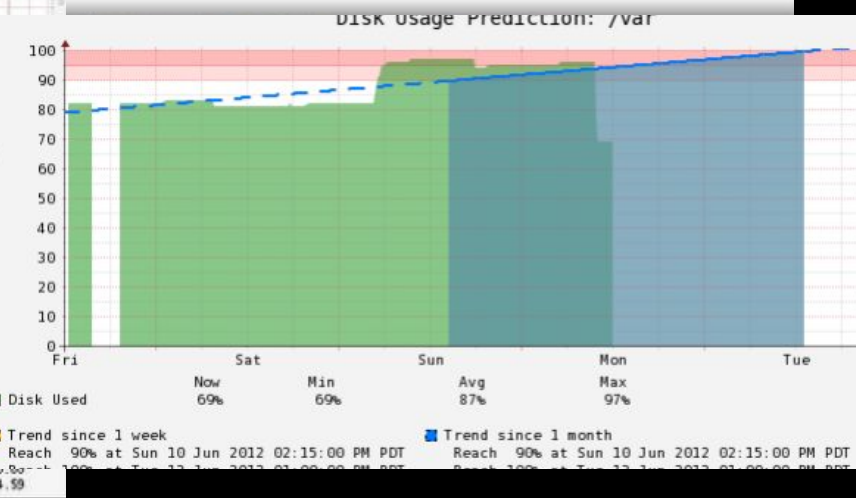
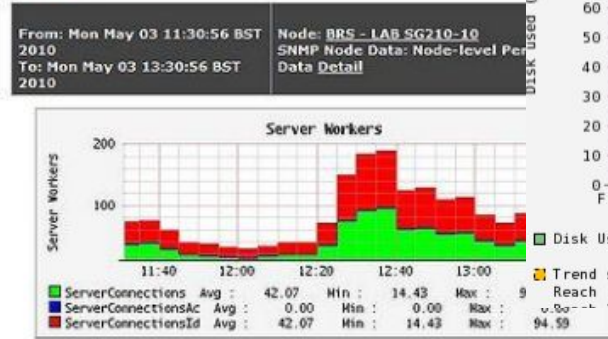
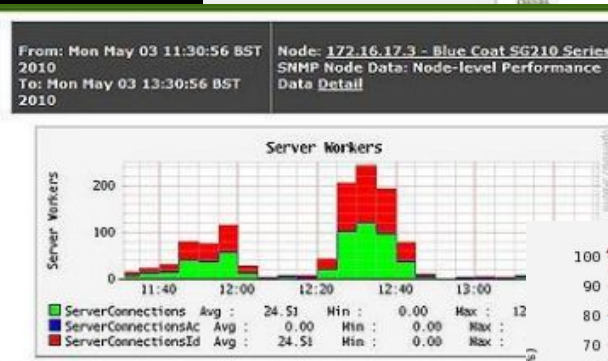
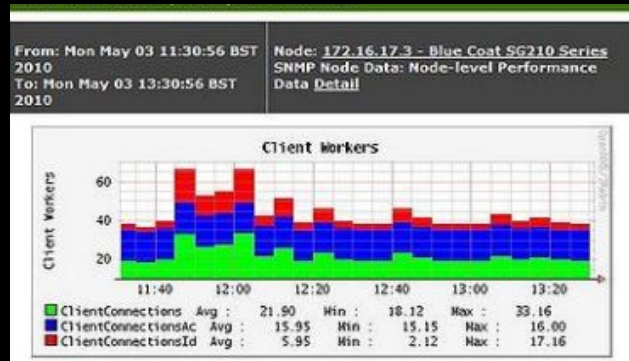
Backup Systemy backupu i archiwizacji:

- IBM TSM
- Simpana

# SYSTEM MONITOROWANIA

Dostępne rozwiązania do monitoringu typu open source, w niektórych z nich konfiguracja jest identyczna pomiędzy nimi:

- Shinken
- Ganglia
- Zenoss
- Cacti
- Check\_mk
- Icinga
- Nagios
- Zabbix
- Pandora FMS
- OpenNMS





# ZARZĄDZANIE INCYDENTAMI ORAZ WNIOSKAMI O USŁUGĘ

Przykład:

Rejestracja zgłoszeń - użytkownik zgłasza sprawy poprzez:

- wysłanie wiadomości na jasno określone adresy,
- telefon na podane numery.

Sprawy są rejestrowane w systemie ticketowym.

# ISO 27001 opisuje system ochrony informacji, który zapewnia:

**Samoulepszalność systemu - (pętla Deminga z pomiarem skuteczności zabezpieczeń)**

Norma ISO 27001

**Adekwatność biznesowa – (Zarządzanie Ryzykiem z metodami szacowania i kryteriami akceptowania)**

Normy : ISO 27001 ISO 27005

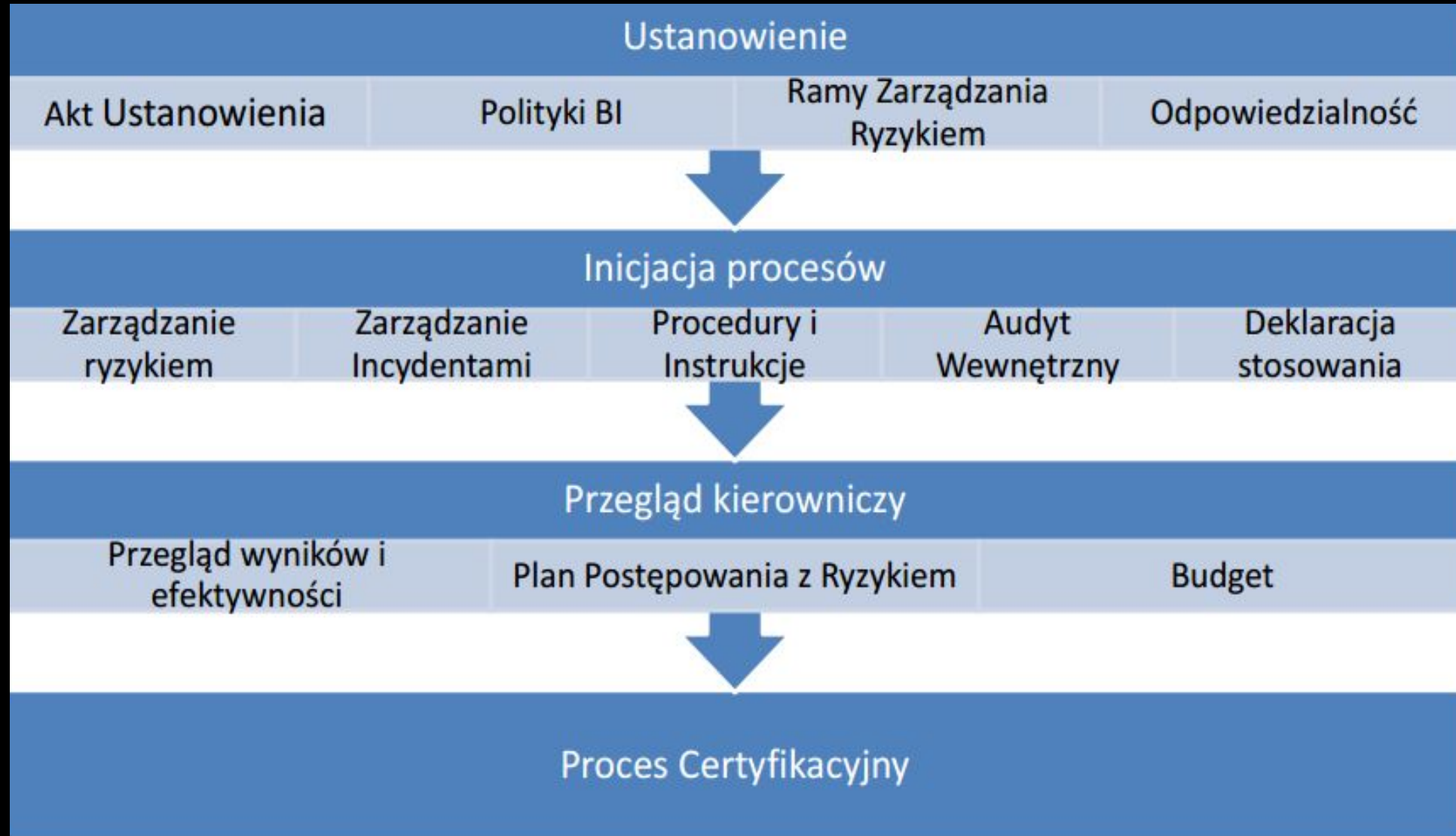
**Kompletność ochrony – (133 punkty kontrolne zabezpieczeń w 39 obszarach i w 11 rozdziałach)**

Zał. A do ISO 27001  
wspierany przez ISO  
17799 i 24762

# ISO 27000

- 27000 – Information Security Management System (SZBI) – overview and vocabulary – SZBI podstawy i terminologia
- ISO/IEC 27001:2005 = PN ISO/IEC 27001:2007 - ISMS requirements – SZBI wymogi – charakter normatywny
- ISO/IEC 27002 = PN-ISO/IEC 17799:2007 – Praktyczne zasady zarządzania bezpieczeństwem informacji – zalecenia
- ISO 27003 – SZBI implementation guidance – SZBI wytyczne wdrożenia
- ISO 27004 - SZBI measurement – SZBI pomiar
- ISO/IEC 27005:2008 Information Security Risk Management = PN ISO/IEC 27005:2010 Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji
- ISO/IEC 27006:2007 = PN ISO/IEC 27006:2009 – Wymagania dla jednostek prowadzących audyt i certyfikację SZBI
- ISO 27007 – Wytyczne dla audytorów SZBI
- ISO/IEC 27011 – Wytyczne bazujące na 27001 do zarządzania BI dla sektora telekomunikacji
- ISO/IEC 27033-1 – Bezpieczeństwo sieci – Podstawy i pojęcia
- PN-EN ISO 27799:2010 – Informatyka w ochronie zdrowia -- Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002

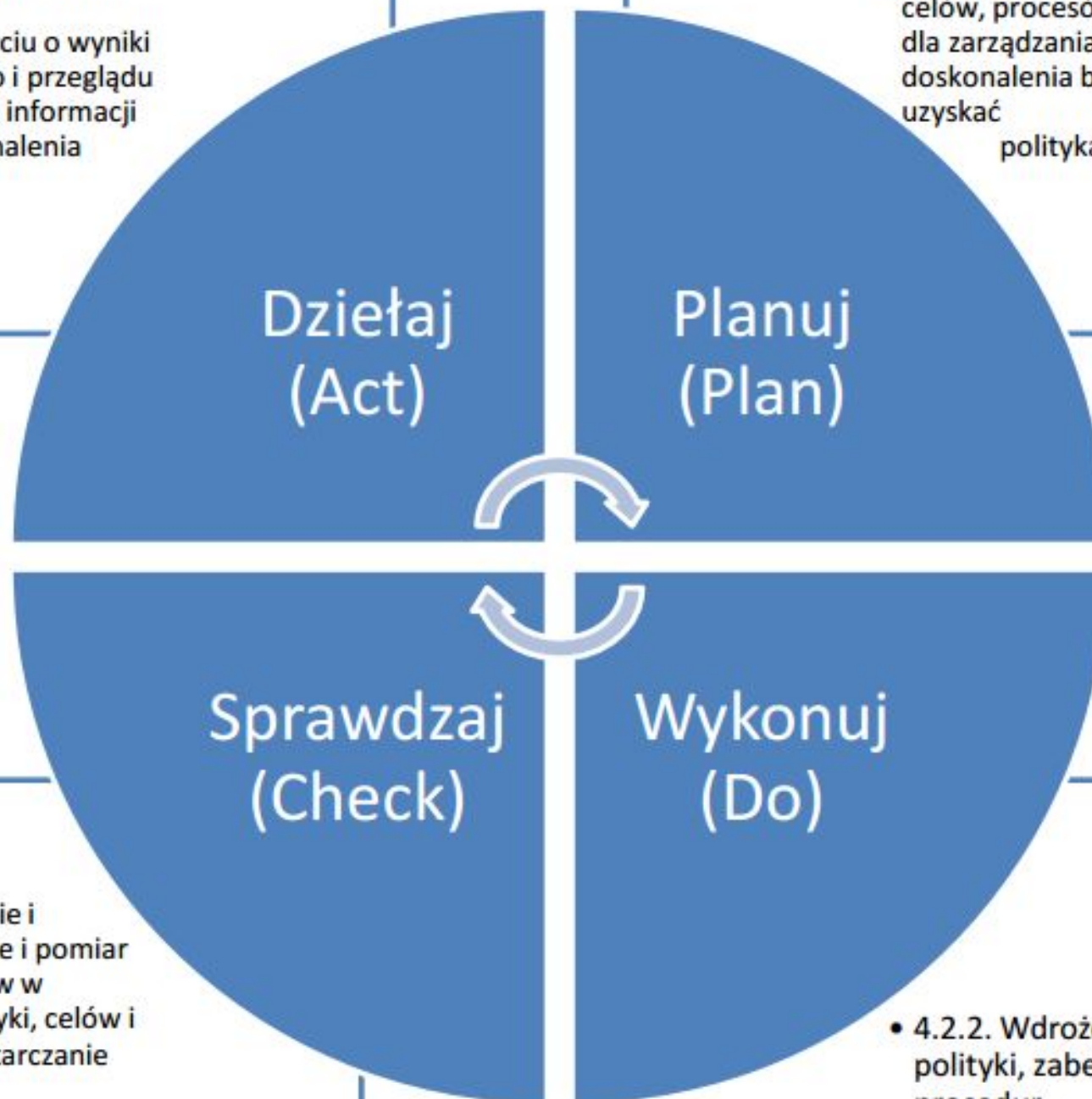
# Etapy wdrożenia ISO 27000





- 4.2.4. Utrzymanie i doskonalenie  
Działania korygujące i zapobiegawcze w oparciu o wyniki Audytu Wewnętrznego i przeglądu kierowniczego i innych informacji w celu ciągłego doskonalenia

- 4.2.1. Ustanowienie SZBI: polityki, celów, procesów, procedur istotnych dla zarządzania ryzykiem i dla doskonalenia bezpieczeństwa aby uzyskać wyniki zgodne z politykami i z celami.



- 4.2.3. Monitorowanie i przegląd. Szacowanie i pomiar wydajności procesów w odniesieniu do polityki, celów i doświadczenia, Dostarczanie raportów

- 4.2.2. Wdrożenie i eksploatacja polityki, zabezpieczeń, procesów, procedur



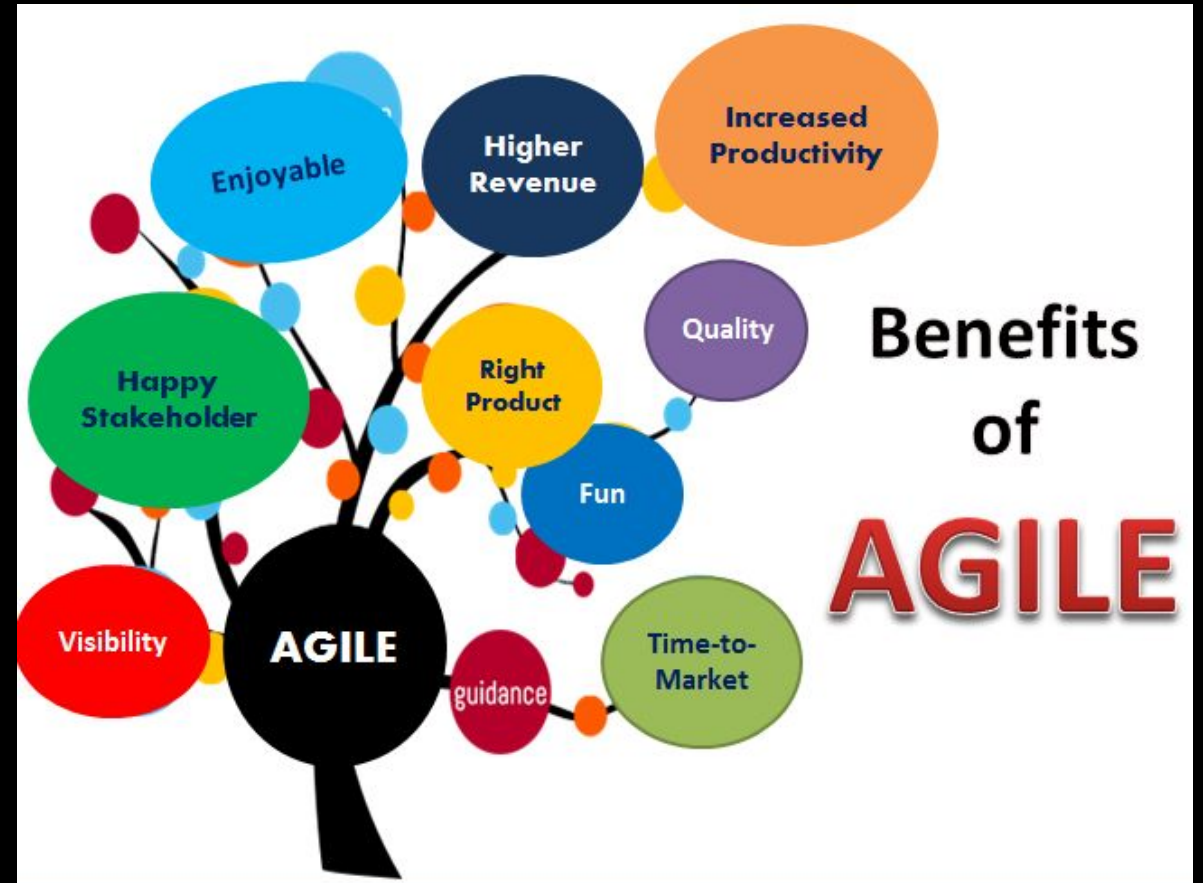
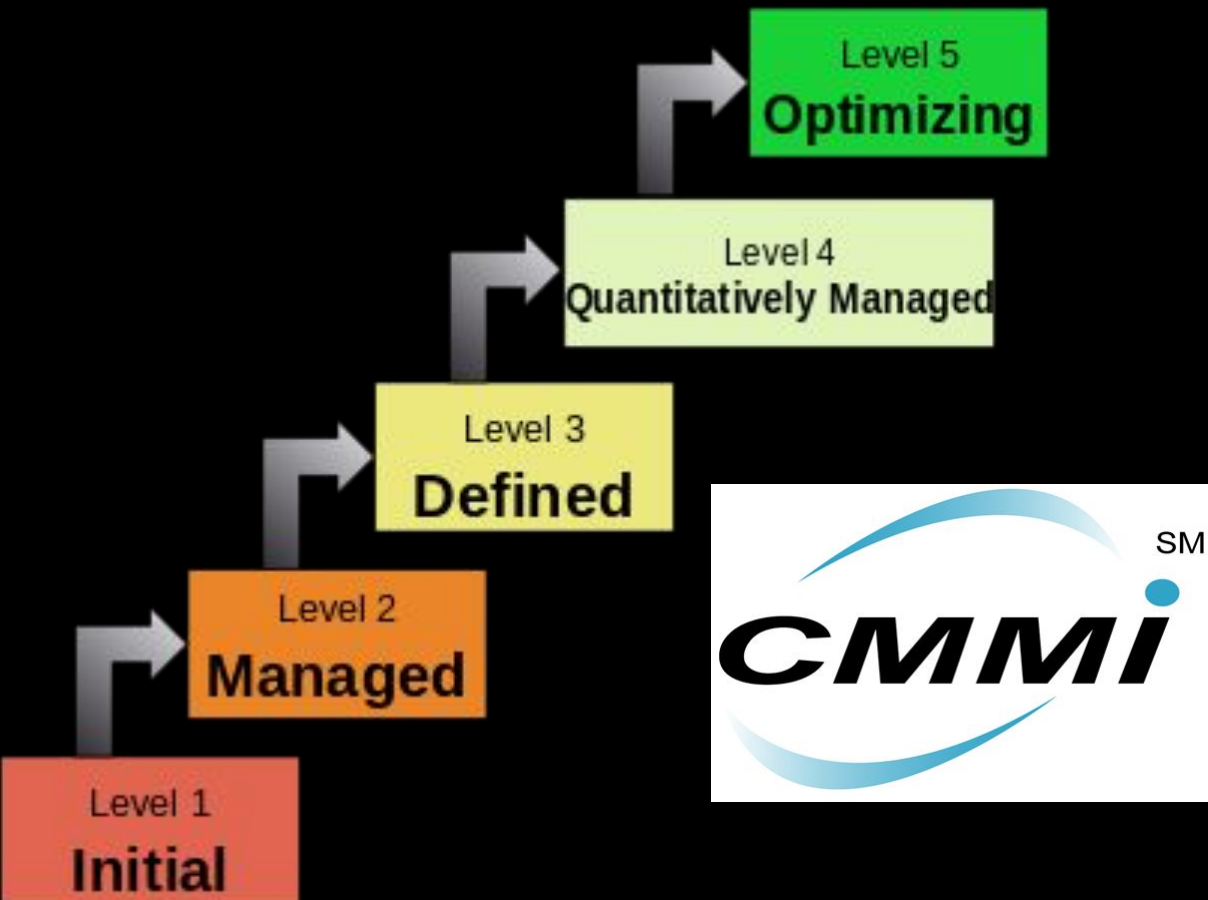
# ISO 27000

- Nawet jeśli prokuratura/prasa ujawnia fakt zaniedbań BI to zawsze pozostaje nam argument, że postępowaliśmy zgodnie z zaleceniami ISO, co nawet zostało potwierdzone przez niezależną jednostkę certyfikacyjną.

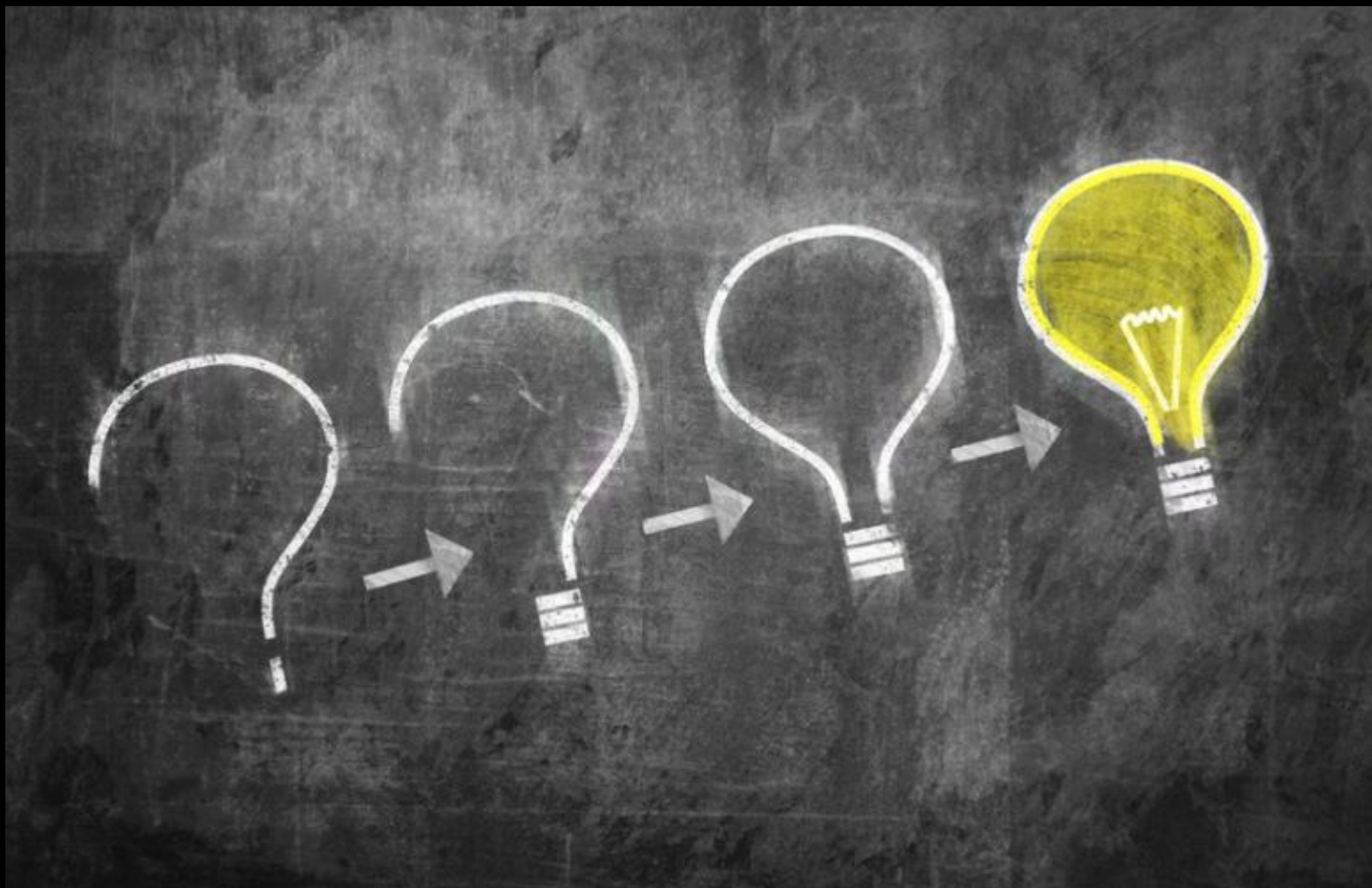


# Alternatywy

## Characteristics of the Maturity levels



# Questions?







**DZIEKUJE ZA**

**UWAGE!**