Wymogi norm ISO seria 27000

Dr Piotr Dzwonkowski CISA, CISM, CRISC

Definicje SZBI

Korzyści z wdrożenia i certyfikacji ISO 27k

Korzyści z wdrożenia ISO 27001

- ISO 27001 jest standardem Systemu Zarządzania Bezpieczeństwem Informacji, który jest rozpoznawalny na całym świecie.
  - Właściciel spółki przejmującej inną spółkę (w której również wdrożono ISO 27001) gdziekolwiek na świecie ma pojęcie na temat zarządzania BI w tej spółce. Wie, że jego pracownicy, dogadają się szybko z tymi drugimi.
- Standard ISO 27001 określa, w jaki sposób proces zarządzania bezpieczeństwem informacji może się doskonalić i zapewniać coraz lepszą ochronę aktywów informacyjnych.
  - Właściciel firmy wie, że postępując zgodnie z zaleceniami ISO będzie w sposób usystematyzowany coraz lepiej dostosowywał poziom BI do wymogów organizacji

Korzyści z wdrożenia ISO 27001

- Standard ISO 27001 dostarcza **kompletną** listę celów kontrolnych i zabezpieczeń dla BI.
  - W rezultacie, w wyniku wdrożenia Zarząd upewnia się, że ochrona dotyczy wszystkich aspektów Bezpieczeństwa Informacji.
- Proces Zarządzania Bezpieczeństwem Informacji działa bazując na wynikach procesu zarządzania ryzykiem.
  - W rezultacie Zarząd może skierować odpowiednie środki tam gdzie doszukano się największego ryzyka.

Korzyści z wdrożenia ISO 27001

- Spełnienie wymogów prawnych
- Obniżenie kosztów,
- Lepsza ochrona aktywów informacyjnych
- Wzrost świadomości BI,
- Zredukowany czas na badania naruszeń bezpieczeństwa
- Łatwość zmiany firmy doradczej

Korzyści z Certyfikacji ISO 27001

Wdrożenie SZBI powinno zabezpieczyć w sposób efektywny kosztowo, spójny i całościowy przed wydarzeniami takimi jak:

- W czasie przetargu na 100 M PLN jedna strona dzięki informacjom nabytym nielegalną drogą zna pozycje negocjacyjne konkurentów.
- Uczeń gimnazjum doprowadza do tygodniowej niedostępności strony internetowej.
- Na stronie internetowej pojawiają się dostępne dane osobowe lub dane medyczne pacjentów
- System komputerowy ulega awarii na 1 tydzień

Korzyści z Certyfikacji ISO 27001

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.

Dodatkowe korzyści z Certyfikacji

Uzyskanie certyfikatu ISO 27001 (System Zarządzania Bezpieczeństwem Informacji) niesie za sobą również następujące korzyści:

- Wyznaczenie celu dla organizacji.
- Niezależna ocena wdrożenia,
- Wzmocnienie wizerunku organizacji
- Wzmocnienie zaufania do organizacji
- Duma i motywacja pracowników
- Ograniczenie sporów sądowych

Definicje SZBI

Normy ISO 27k

Normy ISO rodziny 27k

- 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

Normy ISO rodziny 27k

- **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

Drogi rozwoju - Normy ISO rodziny 27000 w przygotowaniu

- ISO/IEC 27007 - Guidelines for information security management systems Audyting (focused on the management system)
- ISO/IEC 27008 - Guidance for Auditors on SZBI controls (focused on the information security controls)
- ISO/IEC 27013 - Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- ISO/IEC 27014 - Information security governance framework
- ISO/IEC 27015 - Information security management guidelines for the finance and insurance sectors
- ISO/IEC 27031 - Guideline for ICT readiness for business continuity (essentially the ICT continuity component within business continuity management)
- ISO/IEC 27032 - Guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)
- ISO/IEC 27033 - IT network security, a multi-part standard based on ISO/IEC 18028:2006 (part 1 is published already)
- ISO/IEC 27034 - Guideline for application security
- ISO/IEC 27035 - Security incident management
- ISO/IEC 27036 - Guidelines for security of outsourcing
- ISO/IEC 27037 - Guidelines for identification, collection and/or acquisition and preservation of digital evidence

Normy ISO inne normy

- ~~ISO/IEC TR 13335 – uchylona~~
- **PN-ISO 31000:2012**– Zarządzanie ryzykiem -- Zasady i wytyczne
- ISO 38500 – Zarządzanie IT – IT Governance – Ład Informatyczny
- ISO 22301 :2012 (BS 25999) – Societal security – Business continuity management systems – Requirements - ciągłość działania
- **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
- **PN-ISO/IEC 24762:2010** - Guidelines for information and communications technology disaster recovery services
- PN-ISO/IEC 12207:2007 - Technika informatyczna -- Procesy cyklu życia oprogramowania

Kilka słów na temat COBIT

Kompletny system opisujący procesy związane z przetwarzaniem informacji dostarcza ISACA/ITGI w swoich Dokumentach Ramowych

Kilka słów na temat COBIT V5

Section I. Information Security

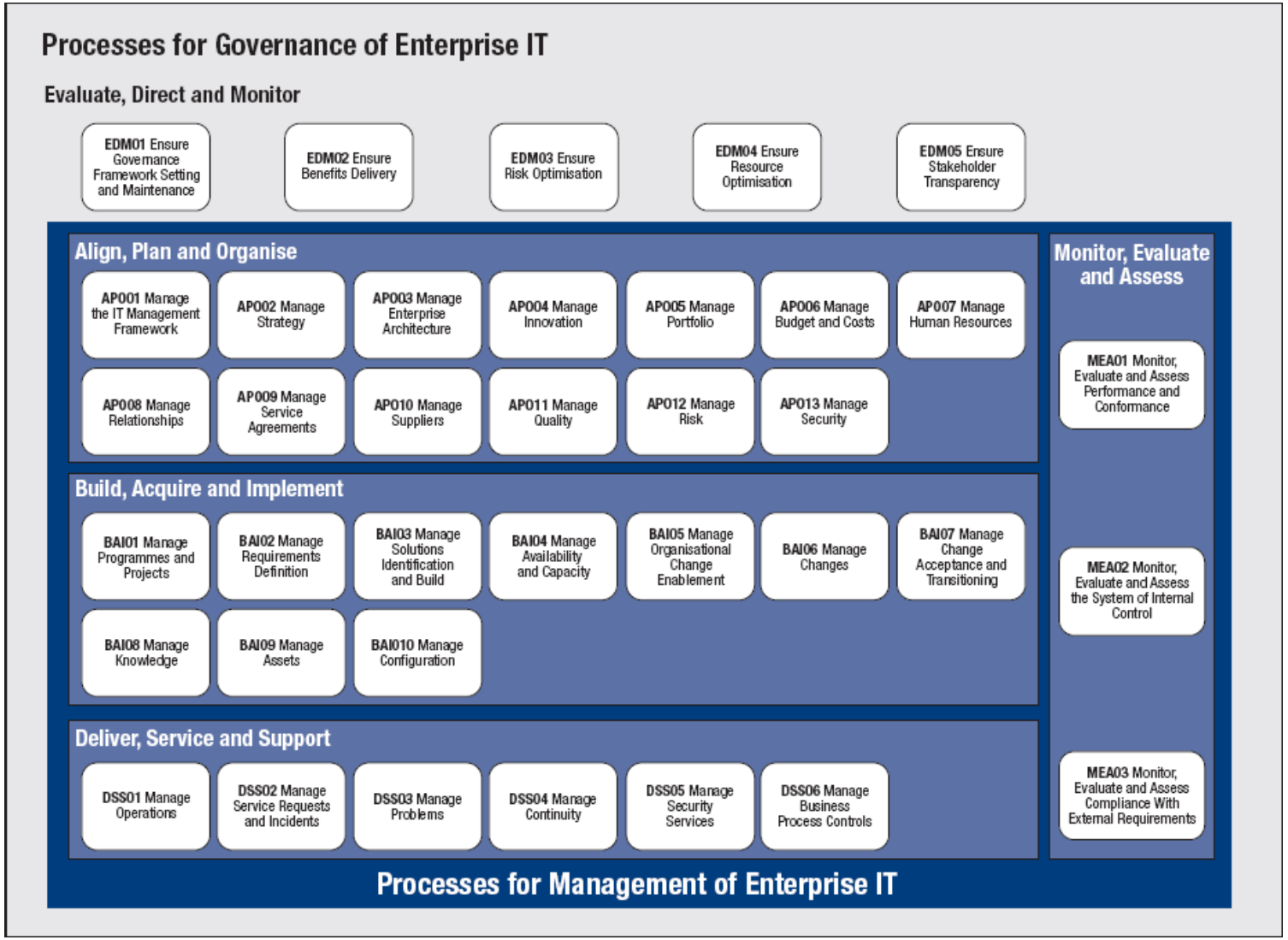
Chapter 1 - Information Security Defined

ISACA defines information security as something that:

Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability).

- confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.
- integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- availability means ensuring timely and reliable access to and use of information.

Kilka słów na temat COBIT V5



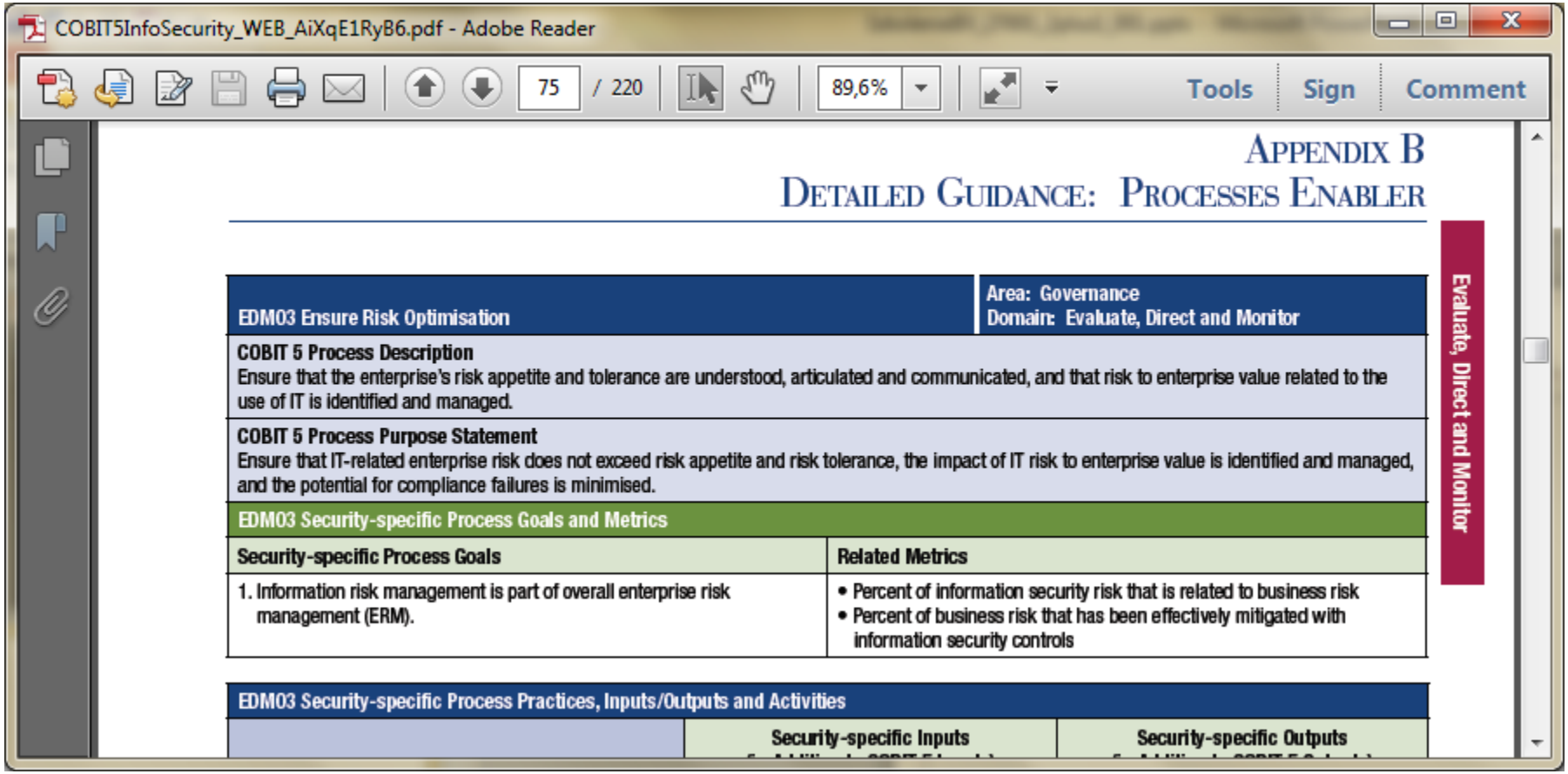
Kilka słów o COBIT V5

- Dla każdego procesu mamy zdefiniowane:

1. Cele (cele procesu i cele związane z IT) – dla każdego celu biznesowego oraz celu IT definiuje się **metryki**
2. Praktyki (zarządcze), dla każdej praktyki mamy
    - listę RACI,
    - listę Wejścia / Wyjścia oraz
    - Szczegółowe działania

Mamy też tabelkę podporządkowującą poszczególnym procesom IT punkty normy 27001 i 27001. W ten sposób możemy znaleźć metryki aby mierzyć wydajność procesu.

AP013 Manage Security	Area: Management Domain: Align, Plan and Organise
Process Description Define, operate and monitor a system for information security management.	
Process Purpose Statement Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines


COBIT5InfoSecurity_WEB_AiXqE1RyB6.pdf - Adobe Reader
75 / 220
89,6%
Tools
Sign
Comment
APPENDIX B
DETAILED GUIDANCE: PROCESSES ENABLER
Evaluate, Direct and Monitor
EDM03 Ensure Risk Optimisation
Area: Governance
Domain: Evaluate, Direct and Monitor
COBIT 5 Process Description
Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.
COBIT 5 Process Purpose Statement
Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.
EDM03 Security-specific Process Goals and Metrics
Security-specific Process Goals
Related Metrics
1. Information risk management is part of overall enterprise risk management (ERM).
• Percent of information security risk that is related to business risk
• Percent of business risk that has been effectively mitigated with information security controls
EDM03 Security-specific Process Practices, Inputs/Outputs and Activities
Security-specific Inputs
Security-specific Outputs

Definicje SZBI

System Zarządzania Bezpieczeństwem Informacji

Definicje SZBI

System Zarządzania

Bezpieczeństwem Informacji

Definicje

- Aktywa*:* wszystko, co ma wartość dla organizacji (Patrz 3.1)
- Informacje to aktywa, które podobnie jak inne ważne aktywa biznesowe, są niezbędne do działalności biznesowej organizacji i z tego powodu zaleca się ich odpowiednią ochronę. (Patrz ISO 27002 0.1)

Definicje

Bezpieczeństwo informacji (ISO 27002 0.1) oznacza jej ochronę przed szerokim spektrum zagrożeń w celu zapewnienia

- ciągłości działania,
- minimalizacji ryzyka i maksymalizacji zwrotu z inwestycji
- Możliwości biznesowych

Bezpieczeństwo informacji (Patrz 3.4) – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności takie jak autentyczność, rozliczalność, niezaprzeczalność, niezawodność.

Atrybuty informacji wg ISO 27001

- Poufność (patrz 3.3) – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom
- Integralność (patrz 3.8) – właściwość polegająca na zapewnieniu dokładności i kompletności
- Dostępność (patrz 3.2) – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu

Inne cechy charakterystyczne informacji

- **Rozliczalność** (ang. *accountability*) – odpowiedzialność podmiotu za jego akcje i decyzje
  (jedna z podstawowych funkcji bezpieczeństwa zapewniająca, że określone działanie dowolnego podmiotu może być jednoznacznie przypisane temu podmiotowi)
  W bezpieczeństwie teleinformatycznym funkcja ta jest realizowana najczęściej za pomocą różnych form rejestrowania zdarzeń (logowania) w połączeniu z ochroną integralności, niezaprzeczalności oraz autentyczności zapisów w rejestrze.
- **Niezaprzeczalność** (ang. non-repudiation) – zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz, że dany podmiot je wywołał, w celu rozstrzygnięcia sporu w zakresie wystąpienia lub niewystąpienia tego zdarzenia lub tej akcji oraz zaangażowania podmiotów w to zdarzenie.
  (brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie).
  Zapewnienie niezaprzeczalności wiadomości jest jedną z cech bezpiecznego podpisu weryfikowanego kwalifikowanym certyfikatem.
- **Autentyczność** (ang. *authenticity*) — 1. właściwość, która polega na tym, że podmiot jest tym za kogo się podaje 2. właściwość polegającą na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane;
  (stan danych w komputerach i sieciach, uzyskiwany za pomocą szyfrowania i podpisów cyfrowych)

Biznesowe kryteria informacji w/g COBIT 4.1

- **Skuteczność** (effectiveness)- to cecha informacji dostarczonej do procesu biznesowego. Informacja taka musi być odpowiednia i istotna a także dostarczona na czas, w poprawny, spójny i nadający się do użycia sposób.
- **Wydajność** (efficiency) opisuje informację dostarczoną poprzez optymalne (najbardziej produktywne i ekonomiczne) użycie środków
- **Poufność** (confidentiality) dotyczy ochrony wrażliwej informacji przed nieautoryzowanym dostępem -
- **Integralność** (integrity) to cecha jaką posiada informacja kompletna i dokładna, a także ważna dla wartości i oczekiwań biznesu.
- **Dostępność** (availability) odnosi się do informacji, która jest dostępna wtedy gdy proces biznesowy jej potrzebuje lub będzie potrzebował. Dotyczy także zachowania potrzebnych środków i związanych z nimi zdolności do działania.
- **Zgodność** (compliance) mówi o zgodności z prawem, regulacjami i zobowiązaniami kontraktowymi, a także o zgodności z procedurami wewnętrznymi
- **Wiarygodność** (reliability) mówi o dostarczaniu odpowiedniej informacji dla kierownictwa organizacji aby mogło utrzymywać działania bieżące i pełnić swoją odpowiedzialność powierniczą i zarządczą

Inne cechy charakterystyczne informacji

.

- Possesion – posiadania i kontrola nad informacją (i możliwość wykazania tego)
- Utility – użyteczność albo pasowanie do celów (przypadek zgubienia klucza kryptograficznego)

Podstawowe standardy

PN-ISO/IEC 27005:2010, Dodatek B Identyfikowanie i wartościowanie aktywów oraz szacowanie skutków

Rodzaje aktywów:

- **Aktywa podstawowe:**
  - **Procesy i działania biznesowe**
  - **Informacje**
- **Aktywa wspierające:**
  - **Sprzęt**
  - **Oprogramowanie**
  - **Sieć**
  - **Personel**
  - **Siedziba**
  - **Struktura organizacyjna**

PN-ISO/IEC 27005:2010, Technika Informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji

Podstawowe standardy

PN-ISO/IEC 27005:2010, Dodatek B Identyfikowanie i wartościowanie aktywów oraz szacowanie skutków

- **Aktywa podstawowe:**
  - **Procesy i działania biznesowe:**
    - ✓ **Których utrata lub pogorszenia uniemożliwia wypełnianie misji**
    - ✓ **Zawierające procesy poufne lub wykorzystujące technologię objętą własnością intelektualną**
    - ✓ **Które, jeśli zostaną zmodyfikowane mogą wpłynąć na realizację misji**
    - ✓ **Które są niezbędne do osiągnięcia zgodności z wymaganiami (umowy, przepisy prawa)**
  - **Informacje**
    - ✓ **Potrzebne do realizacji misji lub działalności biznesowej**
    - ✓ **Dane osobowe**
    - ✓ **Strategiczne, wymagane do osiągnięcia celów strategicznych**
    - ✓ **O dużej wartości, których przetwarzanie (np. pozyskanie, transmitowanie …) wymaga długiego czasu lub wysokich nakładów**

Definicje

System informacyjny ≠ System informatyczny

SZB Informacji ≠ SZB Systemów Informatycznych

Rodzaje informacji w SZBI

- Wewnętrzne – nie powinny dotrzeć do konkurencji - **P**ID
- Dotyczące klientów, konsumentów, kontrahentów – nie powinny być ujawnione gdyż oni tego nie chcą - **P**ID
- Informacje, które muszą być przekazane innym partnerom handlowym - P**I**D

Definicje SZBI

System Zarządzania

Bezpieczeństwem

Informacji

Systemy zarządzania

System zarządzania to **najlepszy sposób** zarządzania.

- **PN-EN ISO 9001:2009** Systemy zarządzania jakością -- Wymagania
- **PN-EN ISO 14001:2005** Systemy zarządzania środowiskowego -- Wymagania i wytyczne stosowania
- **PN-N-18001:2004** Systemy zarządzania bezpieczeństwem i higieną pracy -- Wymagania
- **PN-EN ISO 22000:2006** Systemy zarządzania bezpieczeństwem żywności -- Wymagania dla każdej organizacji należącej do łańcucha żywnościowego
- **PN-ISO/IEC 27001:2007 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji – Wymagania**
- **PN-EN ISO 50001:2012** Systemy zarządzania energią -- Wymagania i zalecenia użytkowania

ale

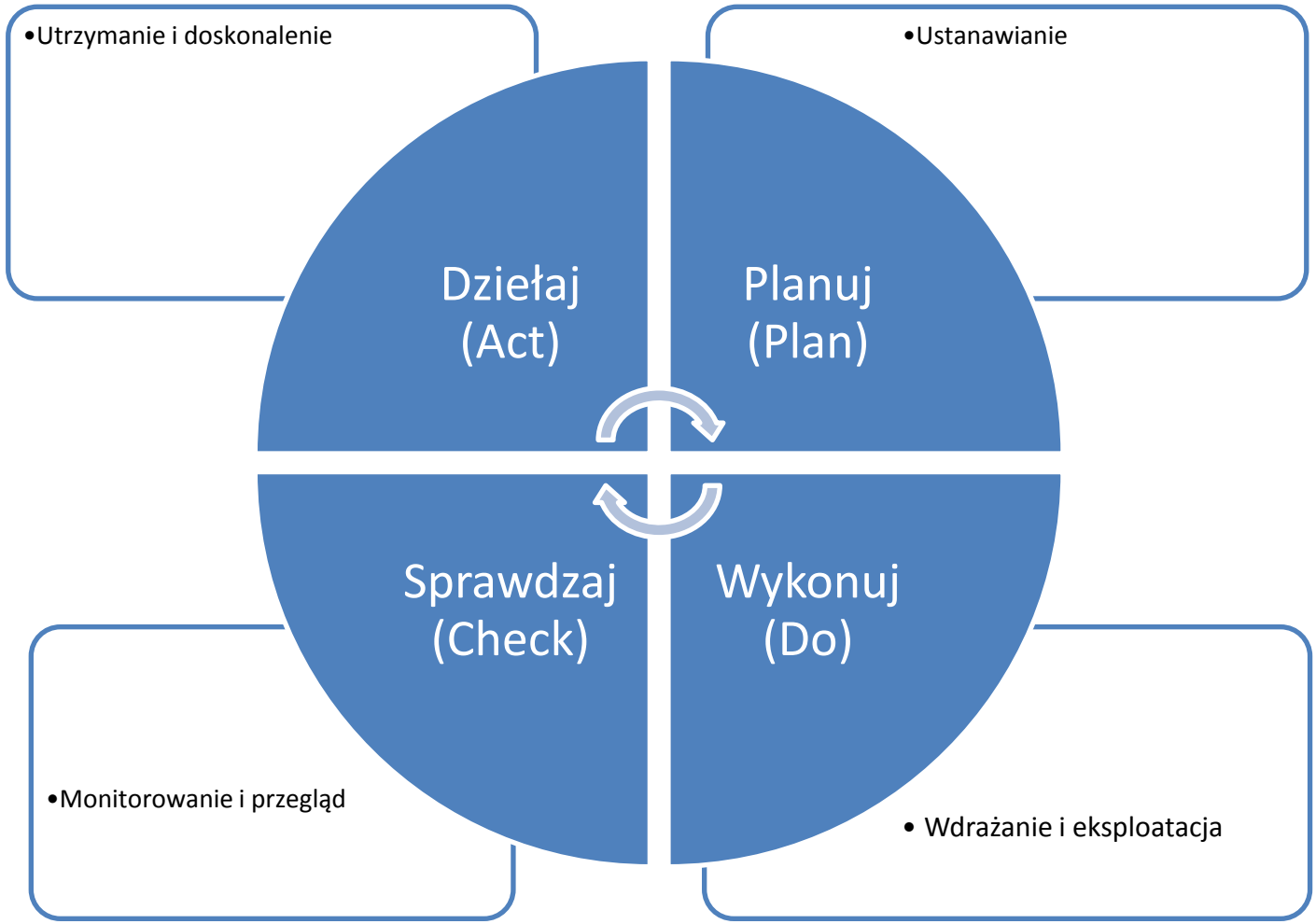
ISO 27005 – Zarządzanie ryzykiem w bezpieczeństwie informacji
ISO 31000 – Zarządzanie ryzykiem

System zarządzania ISO – podejście procesowe

Proces to (ISO 9000):
Zbiór działań wzajemnie powiązanych lub wzajemnie oddziałujących, które przekształcają wejścia w wyjścia

We wszystkich systemach zarządzania ISO stosuje się model PDCA.

Model Deminga – PDCA / PWSD



System Zarządzania Bezpieczeństwem Informacji

Definicja SZBI w ISO/EIC 27001

System Zarządzania Bezpieczeństwem Informacji SZBI (patrz 3.7) to

- część całościowego systemu zarządzania,
- oparta na podejściu wynikającym z ryzyka biznesowego,
- odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.

Uwaga: System zarządzania zawiera strukturę organizacyjną, polityki, planowane działania, zakresy odpowiedzialności, zasady procedury, procesy i zasoby.

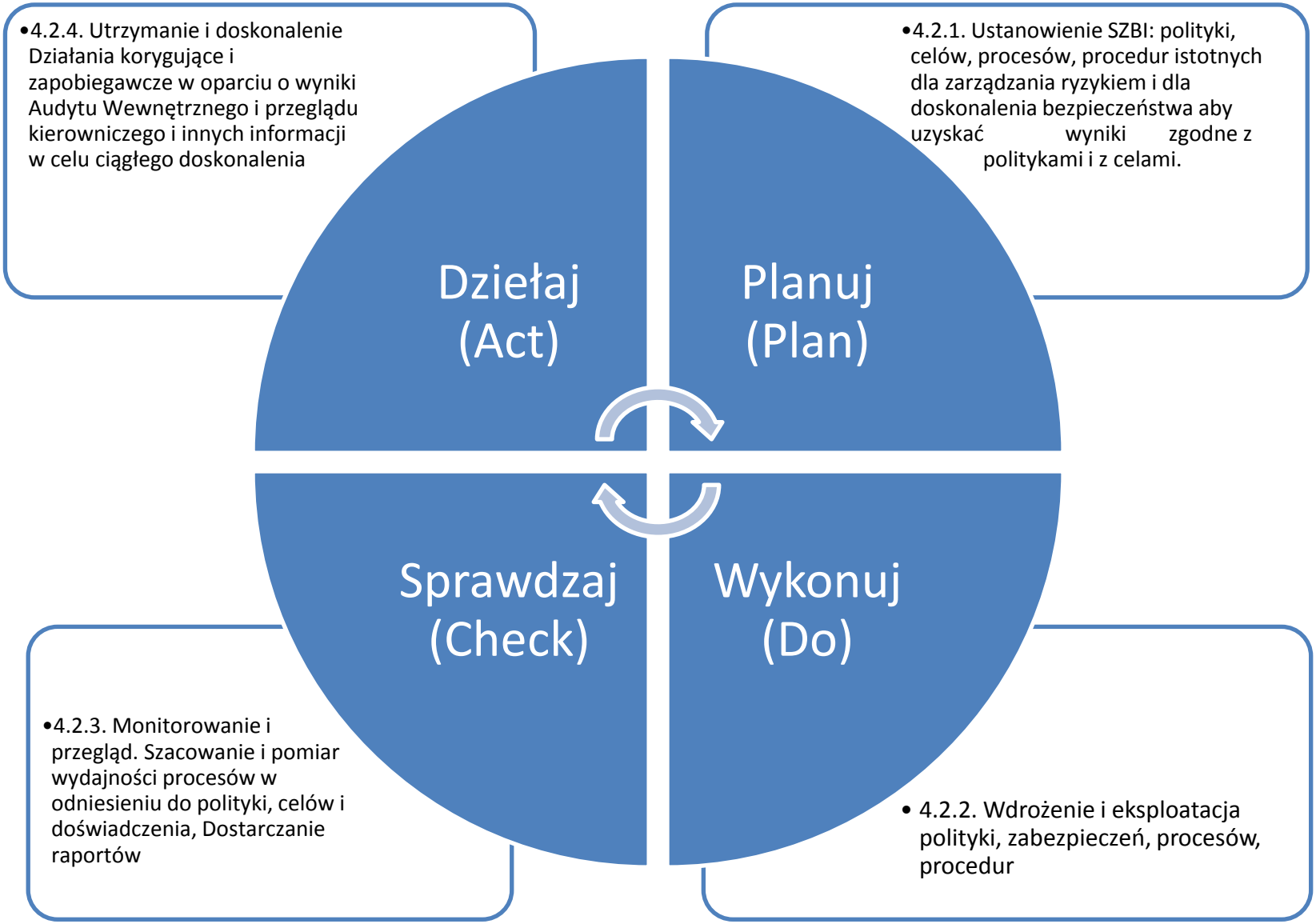
Systemy zarządzania

System zarządzania ISO – podejście procesowe

Proces to (ISO 9000):
Zbiór działań wzajemnie powiązanych lub wzajemnie oddziałujących, które przekształcają wejścia w wyjścia

Podejście procesowe w ISO 27001 (patrz 0.2) zwraca uwagę na:

Model Deminga w p. 0.2 normy 27001



Źródła wymagań bezpieczeństwa ISO 27002 0.3

- Wyniki szacowania ryzyka dla organizacji przy uwzględnieniu całościowej strategii biznesowej i celów organizacji.
- Wymagania prawne, statutowe, regulacje wewnętrzne
- Wymagania kontraktowe w stosunku do organizacji, kontrahentów, dostawców
- Zbiór zasad, celów i wymagań dotyczących przetwarzania informacji, które organizacja wypracowała w celu wspierania swej działalności

Krajowe Ramy Interoperacyjności

§ 20.

1. Podmiot realizujący zadania publiczne
opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali

system zarządzania bezpieczeństwem informacji

zapewniający
poufność, dostępność i integralność informacji
z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

2. Zarządzanie bezpieczeństwem informacji **realizowane jest w szczególności przez zapewnienie przez kierownictwo** podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań *(...14 punktów...)*

Krajowe Ramy Interoperacyjności

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy **PN-ISO/IEC 27001**, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;

2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;

3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

4. Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych **analizą ryzyka** w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

§ 21. 1. Rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach) (… *5 ustępów*…)

Zarządzanie Ryzykiem IT

Definicja ryzyka 1/2

- Zagrożenie (thread) – Potencjalna przyczyna incydentu, którego skutkiem może być szkoda dla systemu lub instytucji
- Podatność (vulnerability) – Słabość aktywów, która może być wykorzystana przez zagrożenie
- Skutek (impact) – Rezultat niepożądanego incydentu
- Prawdopodobieństwo (probability) – Stopień pewności, że incydent się zdarzy
- Incydent BI (information security incident) – Pojedyncze zdarzenie lub seria niepożądanych lub nieoczekiwanych zdarzeń związanych z BI, które ze znaczącym prawdopodobieństwem mogą powodować zagrożenie dla działalności biznesowej o BI.

Definicja ryzyka 2/2

PN-ISO/IEC 27005:2010

Ryzyko związane z bezpieczeństwem Informacji (3.2)

Potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów powodując w ten sposób szkodę dla organizacji

UWAGA Ryzyko jest mierzone jako kombinacja prawdopodobieństwa zdarzenia i jego następstw

Podstawowe standardy

PN-ISO/IEC 27005:2010, Zarządzanie ryzykiem w bezpieczeństwie informacji

Standard definiuje proces zarządzania ryzykiem w bezpieczeństwie informacji, zawierający następujące kroki:

- **Ustanowienie kontekstu**
- **Szacowanie ryzyka (27005 - 8)**
  - **– Analiza ryzyka (27005 – 8.2)**
    - **. Identyfikowanie ryzyka**
    - **- Estymacja ryzyka**
  - **- Ocena ryzyka (27005 – 8.3)**
- **Postępowanie z ryzykiem**
- **Akceptowanie ryzyka**
- **Informowanie o ryzyku**
- **Monitorowanie i przegląd ryzyka**


Lista Aktywów Informacyjnych
Lista Zagrożeń z miarą wartości utraconej
Lista scenariuszy prowadzących do strat z miarą częstości
Poziom ryzyka

Matryca Ryzyka

Częstość zdarzenia							
	raz na dzień	**5**	5	10	15	20	25
	raz na tydzień	**4**	4	8	12	16	20
	raz na miesiąc	**3**	3	6	9	12	15
	raz na rok	**2**	2	4	6	8	10
	raz na 10 lat	**1**	1	2	3	4	5
			1	**2**	**3**	**4**	**5**
			20 min (i mniej) przychodu	3 godziny przychodu	3 dni przychodu	1 miesiąc przychodu	1 rok (i więcej) przychodu
			Wartość				

Poziomy ryzyka
Akceptowalne
Tolerowane na bieżącym etapie
Nieakceptowalne
Wykluczone

Wymagania normy - ISO 27001

Struktura ISO 27001:2005

0. Wprowadzenie
1. Zakres normy
2. Powołania normatywne
3. Terminologia i definicje
4. **System zarządzania bezpieczeństwem informacji SZBI**
5. **Odpowiedzialność kierownictwa**
6. **Wewnętrzne audyty SZBI**
7. **Przeglądy SZBI realizowane przez kierownictwo**
8. **Doskonalenie SZBI**

Załącznik A: Cele stosowania zabezpieczeń i zabezpieczenia

Wymagania normatywne SZBI

ISO/IEC 27001:2005 (wymagania)

4. System zarządzania bezpieczeństwem informacji SZBI

- 4.1 Wymagania ogólne
- 4.2 Wdrożenie i zarządzanie systemem bezpieczeństwa informacji
- 4.3 Wymagania odnośnie dokumentacji

5. Odpowiedzialność kierownictwa

- 5.1 Zaangażowanie najwyższego kierownictwa
- 5.2 Zarządzanie zasobami

6. Wewnętrzne audyty SZBI

7. Przeglądy SZBI realizowane przez kierownictwo

8. Doskonalenie SZBI

- 8.1 Ciągłe doskonalenie
- 8.2 Działania korygujące
- 8.3 Działania zapobiegawcze

Wymagania normatywne SZBI

ISO/IEC 17799:2005 (wytyczne)

A5. Polityka bezpieczeństwa
A6. Organizacja bezpieczeństwa informacji
A7. Zarządzanie aktywami
A8. Bezpieczeństwo zasobów ludzkich
A9. Bezpieczeństwo fizyczne i środowiskowe
A10. Zarządzanie systemami i sieciami
A11. Kontrola dostępu do systemu
A12. Nabycie systemu informacyjnego, rozwój i utrzymanie
A13 Zarządzanie incydentami bezpieczeństwa informacji
A14. Zarządzanie ciągłością działania
A15. Zgodność (z wymaganiami prawa i ustalonymi zasadami)

ISO 27001 opisuje system ochrony informacji, który zapewnia:

Samoulepszalność systemu - (pętla Deminga z pomiarem skuteczności zabezpieczeń)	Adekwatność biznesowa – (Zarządzanie Ryzykiem z metodami szacowania i kryteriami akceptowania)	Kompletność ochrony – (133 punkty kontrolne zabezpieczeń w 39 obszarach i w 11 rozdziałach)
Norma ISO 27001	Normy : ISO 27001 ISO 27005	Zał. A do ISO 27001 wspierany przez ISO 17799 i 24762

Kilka uwag na temat kompletności

- Kompletność podejścia oznacza zajęcie się całą organizacją i wszystkimi procesami przetwarzania informacji.
- Kompletność jest zasadniczym elementem, gdyż aktywa informacyjne są na tyle bezpieczne na ile jest najsłabsze zabezpieczenie.
- Tylko poprawna inicjalizacja projektu przez Zarząd może zagwarantować, że zabezpieczenia obejmą całość organizacji.

Minimalne wymagania bezpieczeństwa dokumentacji medycznej

Porównanie wymogów

Porównanie wymogów

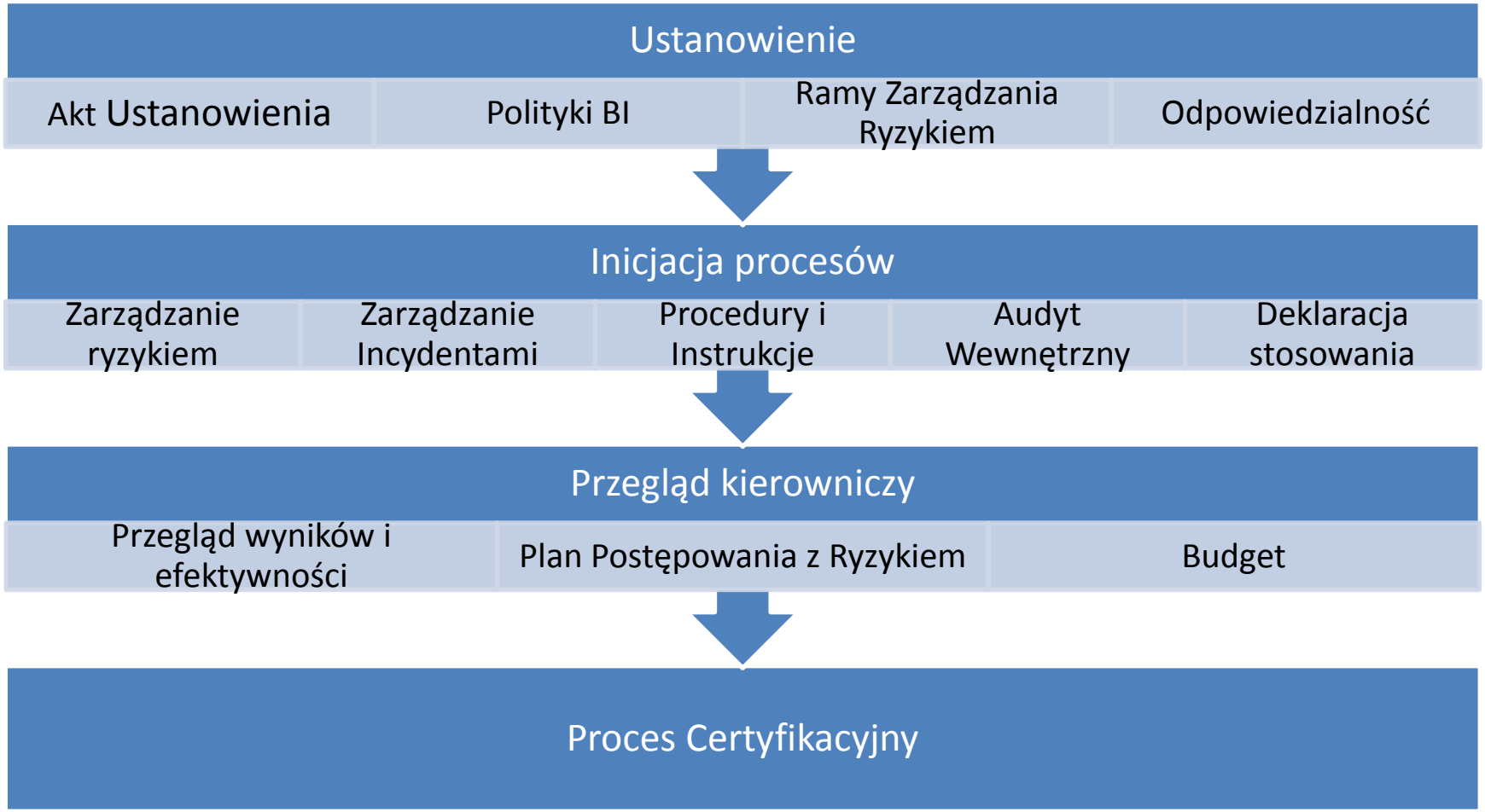
Wymagania dotyczące BI w Krajowych Ramach Interoperacyjności	ISO 27001 1	ISO 27001 2	ISO 27001 3
20. 1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność	N1.1	N3.4	N1
20.2 Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:	N5	N4.2.3.c)	N5
20.2.1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;	N4.2.3d)		N4
20.2.2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;	N4.2.3d)	A7	A7
20.2.3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;	N4.2.3d)		N3
20.2.4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;	N5.2.2		N5
20.2.5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;	A11.2		A11
20.2.6a) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji,	A8.2.2		A8
20.2.6b) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,	A8.2.2		

Porównanie wymogów

ISO27	KRI	Komentarz - nazwa rozdziału ISO 27001
N0	#N/D!	Wprowadzenie
N1	N1	
N2	#N/D!	Powołania normatywne
N3	N3	
N4	N4	
N5	N5	Odpowiedzialność Kierownictwa
N6	N6	Wewnętrzne Audyty SZBI
N7	#N/D!	Przeglądy SZBI realizowane przez Kierownictwo
N8	#N/D!	Doskonalenie SZBI
A5	#N/D!	Polityka Bezpieczeństwa
A6	A6	
A7	A7	
A8	A8	
A9	A9	
A10	A10	
A11	A11	
A12	A12	
A13	A13	
A14	#N/D!	Zarządzanie Ciągłością Działania
A15	A15	

Etapy wdrożenia i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji

Etapy wdrożenia



Zakończenie i kontakt

Zachęcam do podnoszenia swych kwalifikacji zawodowych przez uczestnictwo w pracach stowarzyszeń:

ISSA Polska – https://issa.org.pl/

ISACA Polska - http://www.isaca.waw.pl/

http://www.isaca.org/chapters8/Katowice/Pages/default.aspx

Dziękuję za uwagę

LINKIES. Management Consulting Polska

- Dr. Piotr Dzwonkowski
  - M +48 784 268 542
  - E-Mail
    - **piotr.dzwonkowski @linkies.eu**

LINKIES. Management Consulting to międzynarodowa grupa konsultantów specjalizująca się procesach zarządzania ryzykiem, a szczególnie ryzykiem związanym z przetwarzaniem informacji. W centrum naszych zainteresowań leżą:

- konfiguracja zabezpieczeń aplikacji SAP wraz z system autoryzacji
- wspomaganie wdrożeń ISO 27001
- szkolenia ISO 27001