Standard COBIT
(Control Objectives for Information and Related Technology)

Dr. prof. Swietłana Kaszuba
e-mail:
swietlana.kashuba@byd.pl
tel. 570004779

Bibliografia

1. Marian Molski, Małgorzata £acheta , Przewodnik audytora systemów informatycznych, Helion 2016
2. Harmer Geoff, Governance of Enterprise It Based on COBIT 5: A Management Guide, 2019
3. Sarbanes-Oxley Guide for Finance and Information Technology Professionals - 2012 - Anand - COBIT 3 Executive Summary
4. https://www.techtarget.com/searchsecurity/definition/COBIT
5. https://fliphtml5.com/kcznw/hsyb/basic/51-100
6. https://www.youtube.com/watch?v=Zq5ZHIPs3TI
7. https://www.isaca.org/why-isaca

Standard COBIT

COBIT (Control Objectives for Information and Related Technology) – Cele Kontrolne dla Technologii Informacyjnych i Powiązanych jest najbardziej znanym i powszechnie stosowanym standardem wdrożeniowym strategii oraz nadzoru IT

Standard COBIT odpowiada na biznesowe potrzeby związane z zarządzaniem informacją i technologiami informatycznymi oraz tworzeniem i utrzymywaniem ładu korporacyjnego w obszarze Informatyki – szczególnie z perspektywy audytorów, którzy w swojej pracy muszą posługiwać się jasno określonymi, wymiernymi kryteriami.

Dla kogo jest adresowana metodykaCOBIT

- **Kadra zarządzająca — aby mogła uzyskać wartość z inwestycji w IT oraz zrównoważyć ryzyko i inwestycje w system kontroli** w często nieprzewidywalnym środowisku IT.
- **Kierujący działalnością biznesową — aby mogli otrzymać zapewnienie co do zarządzania i kontroli nad usługami IT** świadczonymi wewnętrznie lub przez strony trzecie.
- **Kierownictwo IT — aby mogło świadczyć usługi IT wymagane przez biznes w celu realizacji strategii biznesowej w** kontrolowany i kierowany sposób.
- **Audytorzy — aby mogli uzasadniać swoje opinie i/lub służyć doradztwem w sprawie wewnętrznych mechanizmów kontrolnych.**

Zalety CobiT

- Dla wielu odbiorców (zarządy firm, audytorzy, kierownictwo IT)
- Kompleksowy i uniwersalny (kontrola oraz zarządzanie IT w każdej firmie) Zawiera wskazówki, praktyki, modele oraz narzędzia służące uporządkowaniu i usprawnieniu obszarów IT w organizacji oraz związanych z tym procesów biznesowych.
- Efekt wieloletnich badań prowadzonych przez ISACF (Information Systems Audit and Control Foundation) oraz doświadczeń członków ISACA (Information Systems Audit and Control Association) – zbiór najlepszych praktyk
- Zgodny z COSO (Committee of Sponsoring Organizations of the Treadway Commission), ITIL (brytyjski standard zarządzania IT)
- Najbardziej aktualny (wydanie 5 z 2019 roku)
- Materiały pomocnicze (dodatkowe), np. metodologia wdrożenia, kwestionariusze itp.
- COBIT jest otwartym standardem, a za jego wdrożenie nie jest pobierana opłata licencyjna

Historia

- Twórcą COBIT jest IT Governance Institute, jednostka badawcza będąca częścią organizacji branżowej o nazwie ISACA - Information Systems Audit and Control Association.
- Pierwsza wersja standardu ujrzała światło dzienne w roku 1996 i kładła nacisk głównie na obszar audytu.
- Przedostatnia wersja, wydana w 2012 roku, nosi numer 5 i skupia się na wartości, jaką IT dostarcza organizacji.
- W 2019 roku wersja 5 została zaktualizowana w najnowszym wydaniu kładzie się duży nacisk na komponenty dotyczące zarówno „twardych" obszarów, które tworzą strukturalny szkielet działalności organizacji (np. struktury organizacyjne, oprogramowanie, procesy), jak i „miękkich", związanych z kapitałem ludzkim, kulturą pracy i obiegiem informacji (przykładowo: umiejętności i kompetencje, etyka, pryncypia).

Zasady COBIT

Podstawowa zasada brzmi, iż informacja jest podstawową wartością w każdej organizacji. Podlega ona procesom wytworzenia, wykorzystania, przechowywania, ujawniania i zniszczenia.

Technologia zaś ulega upowszechnieniu i pełni kluczową rolę w tych procesach.

Ponadto model COBIT charakteryzuje grupa pięciu formalnych zasad (principles), które pozwalają organizacji opracować skuteczną metodykę nadzoru i zarządzania, optymalizującą inwestycje w informacje i technologie informatyczne oraz ich wykorzystanie z korzyścią dla interesariuszy.

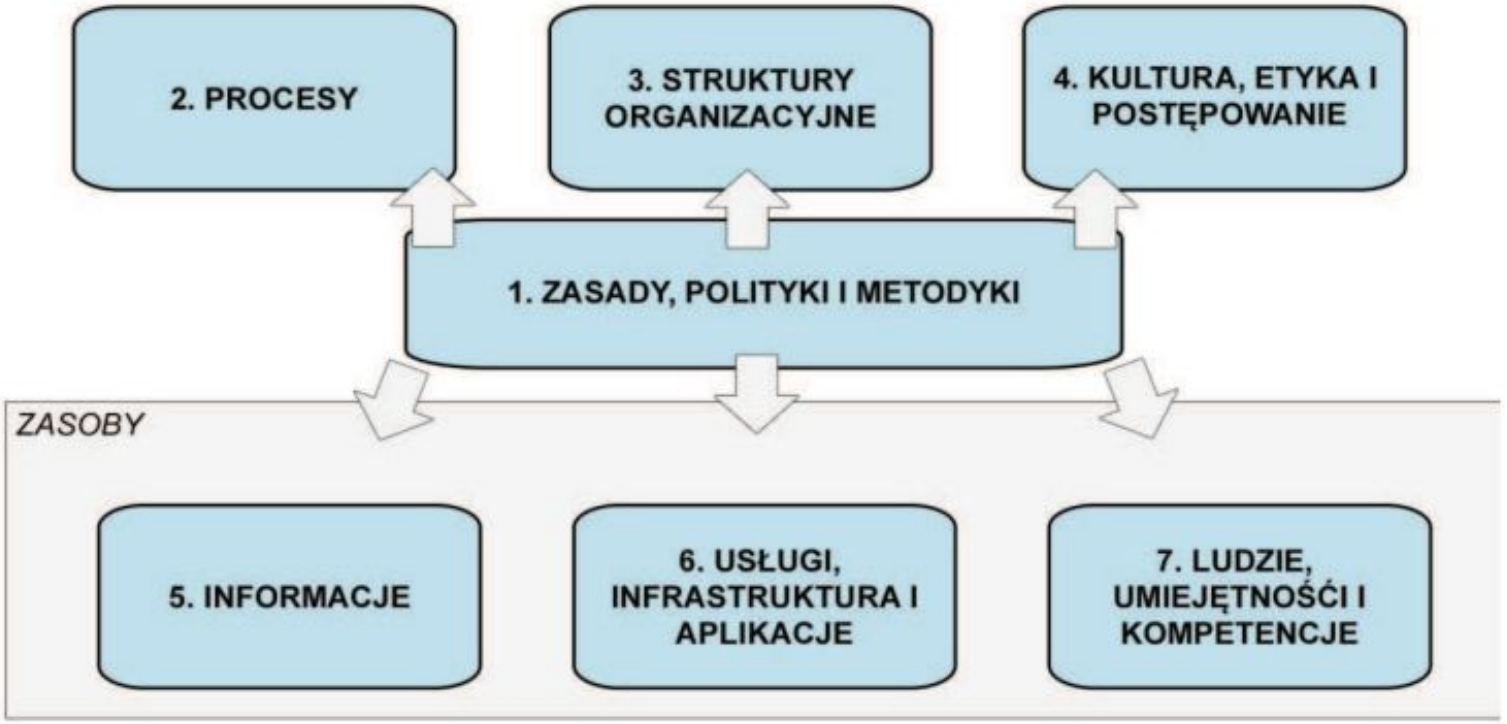
Zasady te są następujące:

1. Spełniać potrzeby interesariuszy.
2. Uwzględniać cały podmiot (objęcie całego przedsiębiorstwa, organizacji).
3. Stosować jedną, spójną metodykę (zastosowanie pojedynczych zintegrowanych ram biznesowych).
4. Umożliwiać całościowe podejście.
5. Oddzielać nadzór od zarządzania (ładu IT od zarządzania IT).

Czynnikami umożliwiające realizację standartu COBIT

1. Zasady, polityki i metody.
2. Procesy.
3. Struktury organizacyjne.
4. Kultura, etyka i postępowanie.
5. Informacje.
6. Usługi, infrastruktura i aplikacje.
7. Ludzie, umiejętności i kompetencje

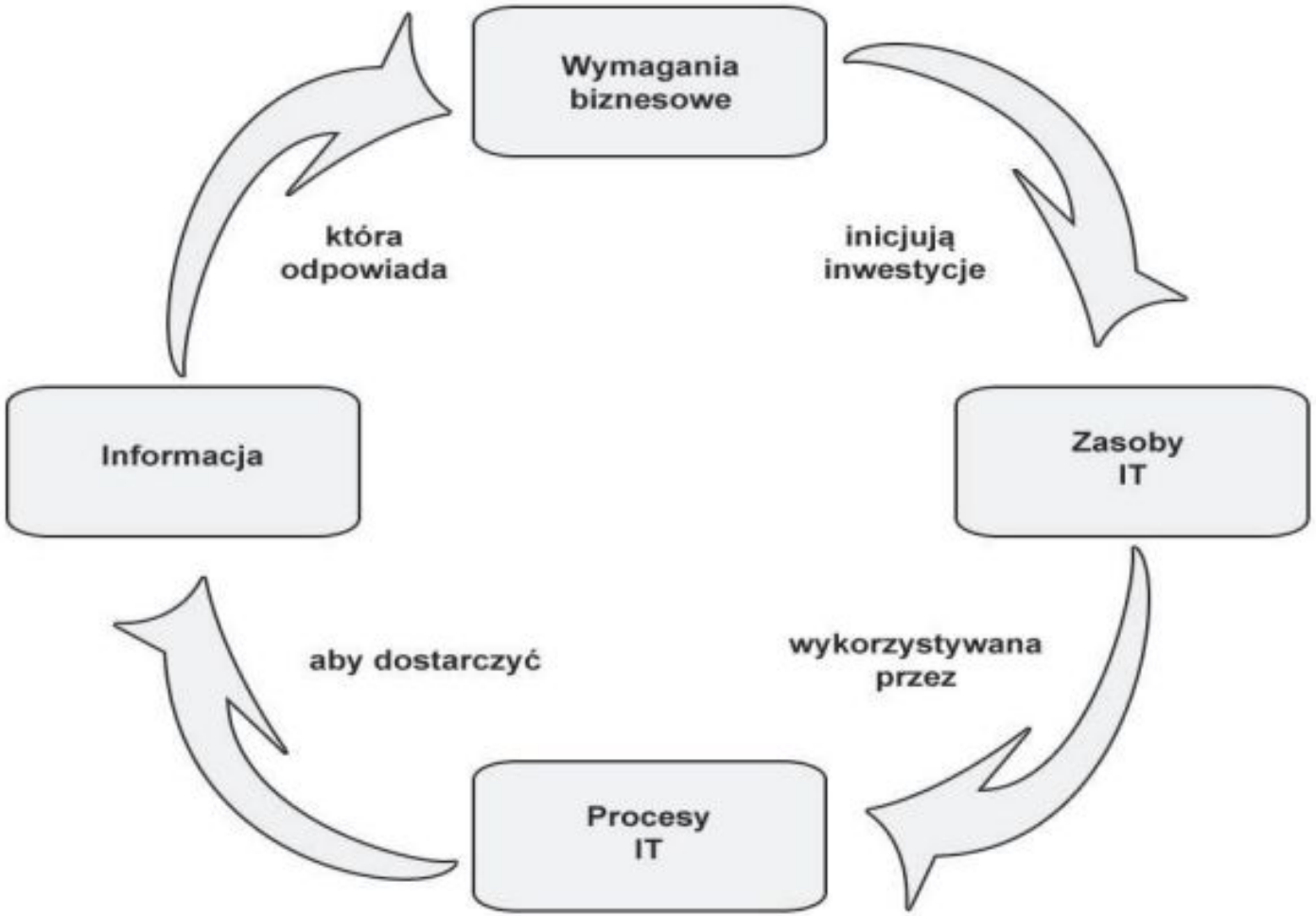
Wzajemne oddziaływanie na siebie czynników umożliwiających prezentuje się w sposób następujący:



Rysunek 1. **Czynniki umożliwiające COBIT** Figure 1. COBIT Enablers Źródło. Board Brie!ng on IT Governance

Podstawowa zasada to dostarczenie informacji, której przedsiębiorstwo (organizacja) potrzebuje do zrealizowania swoich celów. Aby to osiągnąć, musi ono inwestować i zarządzać zasobami IT, wykorzystując uporządkowany wzór procesów po to, aby zapewnić usługi, które dostarczą wymaganej informacji.

Mapa zależności COBIT



Rysunek 2. Mapa zależnośći COBIT Figure 2. Map of COBIT`s internal dependencies Źródło. Board Brie□ng on IT Governance.

Domeny i procesy COBIT

COBIT dostarcza dobre praktyki, metryki i modele dojrzałości do pomiaru stopnia realizacji celów biznesowych i IT zorganizowane w domeny i procesy.

Struktura pięciu zasadniczych domen dzieli się na **domeny ładu** (nadzorcze – governance) i **zarządcze** (management):

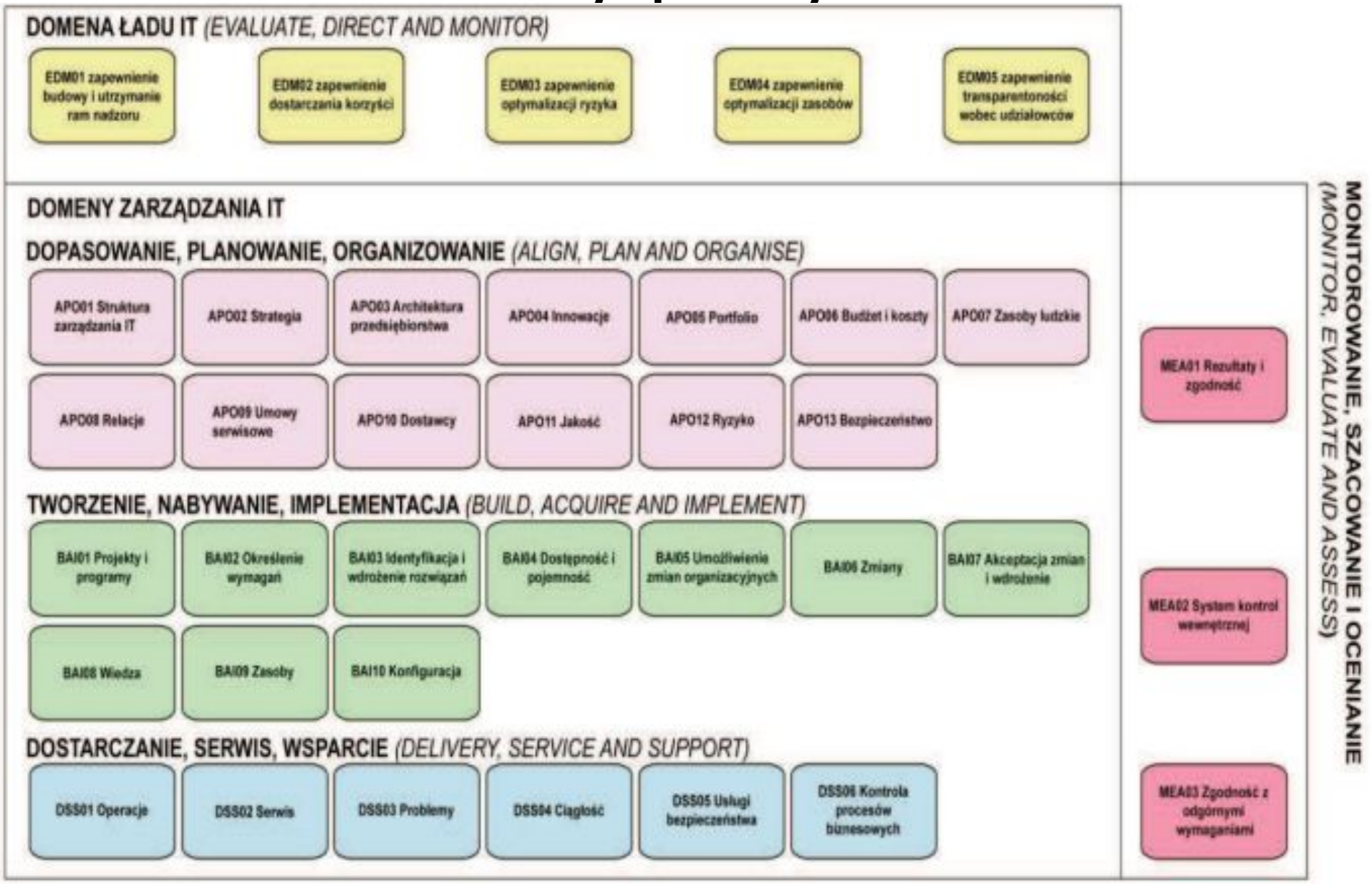
I. Domena ładu: I. EDM (Evaluate, Direct and Monitor):

- EDM1: zapewnienie budowy i utrzymanie ram nadzoru,
- EDM2: zapewnienie dostarczania korzyści,
- EDM3: zapewnienie optymalizacji ryzyka,
- EDM4: zapewnienie optymalizacji zasobów,
- EDM 5: zapewnienie transparentności wobec udziałowców.

II. Domeny zarządcze zgodne z obszarami odpowiedzialności planowania, budowy, uruchamiania i monitorowania uwzględniają wszystkie aspekty IT:

1. Planowanie i organizowanie (PO – Plan and Organize).
2. Zakupy i implementacja (AI – Acquire and Implement).
3. Dostawy i utrzymanie (DS – Deliver and Support).
4. Monitorowanie i ocena (ME – Monitor and Evaluate).

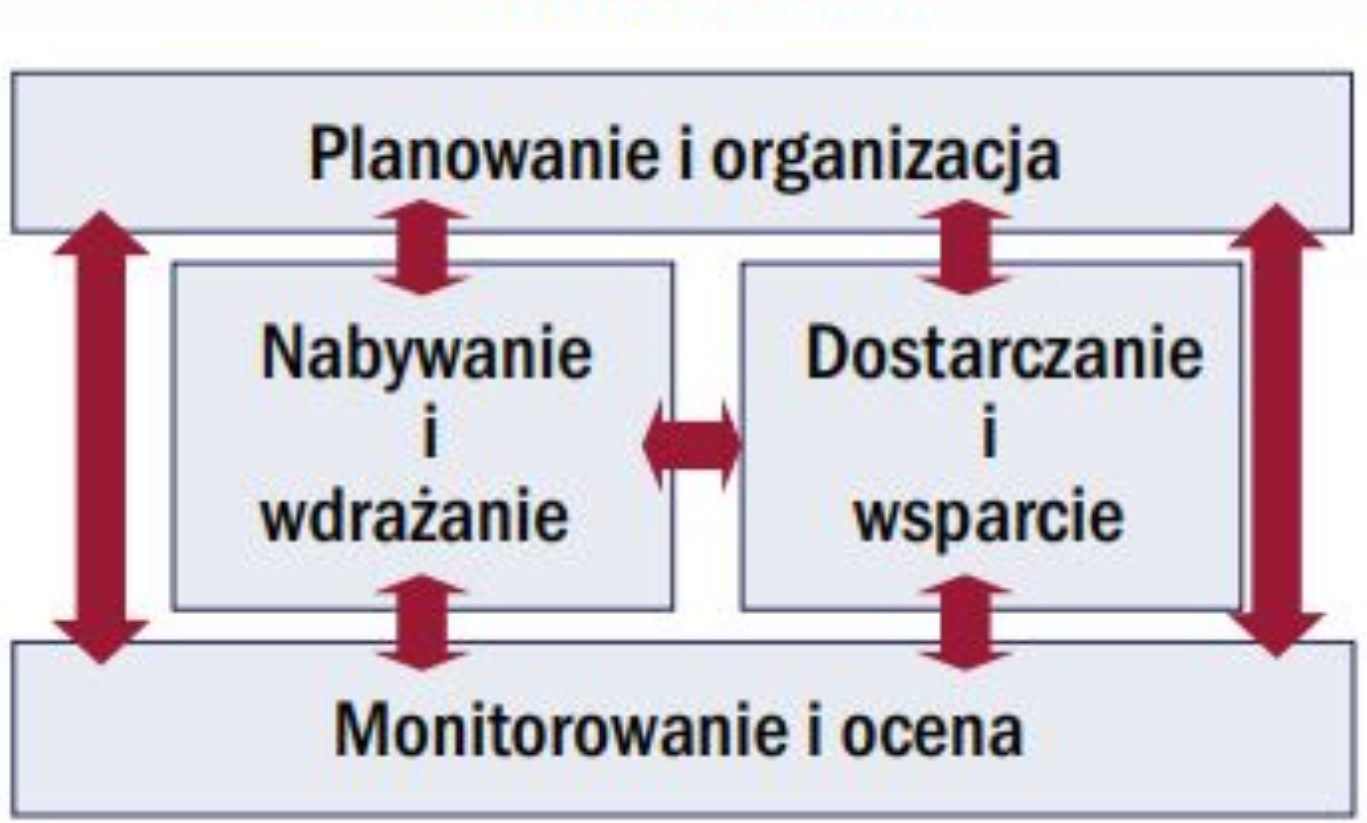
Domeny i procesy COBIT



Rysunek 3: Domeny i procesy COBIT 5 Figure 3: Domains and processes of COBIT Źródło: Board Brie□ng on IT Governance.

Cztery powiązane domeny metodyki COBIT

Domeny zarządzania IT



Domeny zarządzania IT

1. Planowanie i organizacja (PO) — określa kierunek dla dostarczania rozwiązań i świadczenia usług.
2. Nabywanie i wdrażanie (AI) — obejmuje dostarczanie rozwiązań i przekazywanie ich w celu zamiany w usługi.
3. Dostarczanie i wsparcie (DS) — obejmuje odbiór rozwiązań i przystosowanie ich, aby były użyteczne dla użytkowników końcowych.
4. Monitorowanie i ocena (ME) — obejmuje monitorowanie wszystkich procesów, aby zapewnić podążanie w określonym kierunku.

Planowanie i organizacja (PO)

Domena ta, obejmująca zagadnienia strategiczne i taktyczne, dotyczy określenia sposobu, w jaki działalność IT mogłaby najlepiej przyczynić się do osiągnięcia celów biznesowych.

Realizacja wizji strategicznej powinna być planowana, komunikowana i zarządzana z uwzględnieniem różnych perspektyw. Wymaga również zapewnienia odpowiedniej organizacji i infrastruktury technicznej.

Domena ta zwykle odpowiada na następujące pytania związane z zarządzaniem:

- Czy strategia IT jest dostosowana do strategii biznesowej?
- Czy przedsiębiorstwo w optymalny sposób wykorzystuje swoje zasoby?
- Czy wszyscy w organizacji rozumieją cele IT?
- Czy znane jest ryzyko IT i czy zarządza się nim?
- Czy jakość systemów informatycznych jest odpowiednia do potrzeb firmy?

Planowanie i organizacja (PO). Procesy

PO1 Definiowanie planu strategicznego IT
PO2 Definiowanie architektury informacji
PO3 Ustalanie kierunku technologicznego
PO4 Definiowanie procesów IT, organizacji i wzajemnych zależności
PO5 Zarządzanie inwestycjami IT
PO6 Komunikowanie celów i kierunku zarządzania
PO7 Zarządzanie zasobami ludzkimi w IT
PO8 Zarządzanie jakością
PO9 Ocena i zarządzanie ryzykiem informatycznym PO10 Zarządzanie projektami

Nabywanie i wdrażanie (AI)

Aby możliwa była realizacja strategii IT, konieczne jest określenie i stworzenie lub nabycie rozwiązań informatycznych, a następnie ich wdrożenie i zintegrowanie z procesem biznesowym.

Ponadto domena ta obejmuje również zmiany i utrzymanie istniejących systemów, aby mogły one nadal realizować cele biznesowe.

Domena ta zwykle odpowiada na następujące pytania związane z zarządzaniem:

- Czy nowe projekty są w stanie dostarczyć rozwiązania, które będą spełniać potrzeby firmy?
- Czy nowe projekty mogą być zrealizowane terminowo i w ramach budżetu?
- Czy nowe systemy po ich wdrożeniu będą działać prawidłowo?
- Czy można wprowadzić zmiany bez zakłócania bieżącej działalności biznesowej?

Nabywanie i wdrażanie (AI). Procesy

AI1 Identyfikowanie rozwiązań zautomatyzowanych

AI2 Nabywanie i utrzymywanie aplikacji

AI3 Nabywanie i utrzymywanie infrastruktury technicznej

AI4 Umożliwianie działania i użytkowania

AI5 Nabywanie zasobów IT

AI6 Zarządzanie zmianami

AI7 Instalowanie i akredytowanie rozwiązań i zmian

Dostarczanie i wsparcie (DS)

Domena ta dotyczy rzeczywistego dostarczania potrzebnych usług, które obejmuje świadczenie usług, zarządzanie bezpieczeństwem i ciągłością, wsparcie techniczne dla użytkowników oraz zarządzanie danymi i infrastrukturą operacyjną.

Zwykle odpowiada ona na następujące pytania związane z zarządzaniem:

- Czy usługi IT są dostarczane zgodnie z priorytetami biznesowymi?
- Czy koszty IT są zoptymalizowane?
- Czy pracownicy są w stanie korzystać z systemów IT w produktywny i bezpieczny sposób?
- Czy zapewniona jest odpowiednia poufność, integralność i dostępność gwarantująca bezpieczeństwo informacji?

Dostarczanie i wsparcie (DS). Procesy

DS1 Definiowanie i zarządzanie poziomami usług
DS2 Zarządzanie usługami zewnętrznymi
DS3 Zarządzanie wydajnością i pojemnością
DS4 Zapewnianie ciągłości usług
DS5 Zapewnienie bezpieczeństwa systemów
DS6 Identyfikowanie i rozliczanie kosztów
DS7 Kształcenie i szkolenia użytkowników
DS8 Zarządzanie jednostką Service Desk i incydentami
DS9 Zarządzanie konfiguracją
DS10 Zarządzanie problemami
DS11 Zarządzanie danymi
DS12 Zarządzanie środowiskiem fizycznym
DS13 Zarządzanie operacjami

Monitorowanie i ocena (ME)

Wszystkie procesy IT powinny być regularnie poddawane ocenie pod kątem ich jakości i zgodności z wymaganiami kontrolnymi. Domena ta obejmuje kwestie zarządzania wydajnością, monitorowania systemu kontroli, zgodności z wymaganiami regulacyjnymi i nadzoru.

Zwykle odpowiada ona na następujące pytania związane z zarządzaniem:

- Czy wydajność IT podlega pomiarowi, aby wykrywać problemy zanim jest za późno?
- Czy kierownictwo dba o to, aby wewnętrzne mechanizmy kontrolne były efektywne i wydajne?
- Czy efekty działalności IT można powiązać z celami biznesowymi?
- Czy istnieją odpowiednie mechanizmy kontroli poufności, integralności i dostępności w celu zapewnienia bezpieczeństwa informacji?

Monitorowanie i ocena (ME). Procesy

ME1 Monitorowanie i ocena wydajności IT

ME2 Monitorowanie i ocena kontroli wewnętrznej

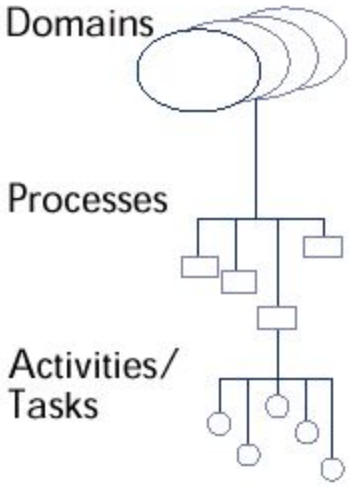
ME3 Zapewnianie zgodności z zewnętrznymi regulacjami

ME4 Zapewnienie ładu informatycznego

Składniki standardu

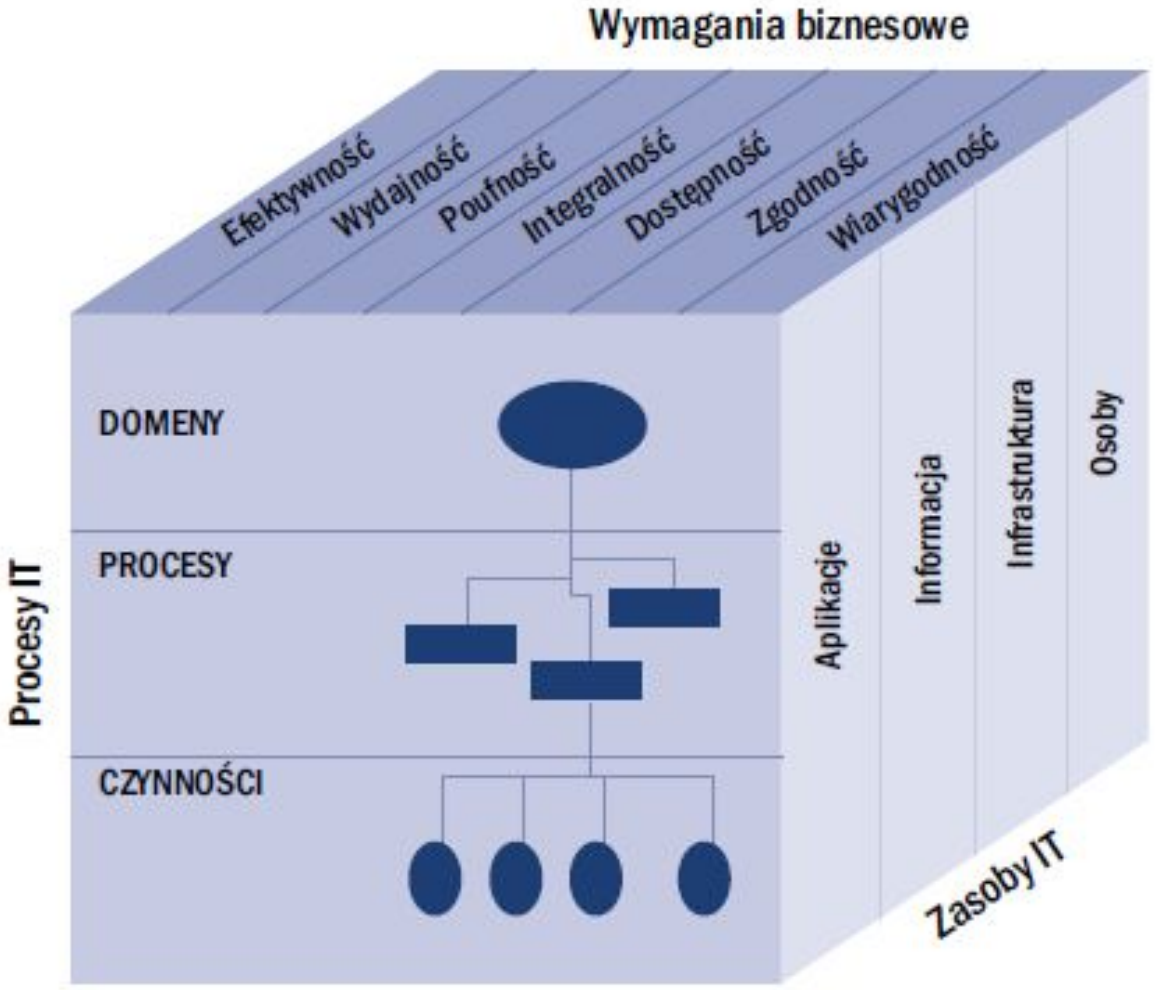
- Framework (dla zarządu firmy)
- Executive Summary (dla kierownictwa)
- Control Objectives (spis celów kontroli)
- Audit Guidelines (szczegółowy poradnik dla audytorów)
- Management Guidelines (dla zarządzających IT w firmie - nowość)

Struktura CobiTu



- 4 domeny
- 34 procesy IT
- 318 celów kontroli
- Szczegółowe wytyczne w zakresie kontroli IT: testowanie, zestaw zapytań
- Szczegółowe wytyczne w zakresie zarządzania IT, oceny wydajności, efektywności

Kostka CobiT. Sześcian CobiT



Jak korzystać z CobiT

- Audyt wg kryteriów informacji
- Audyt wg zasobów IT
- Audyt poszczególnych procesów IT
- Audyt całych domen IT
- Zarządzanie IT wg „Management Guidelines”

Agenda

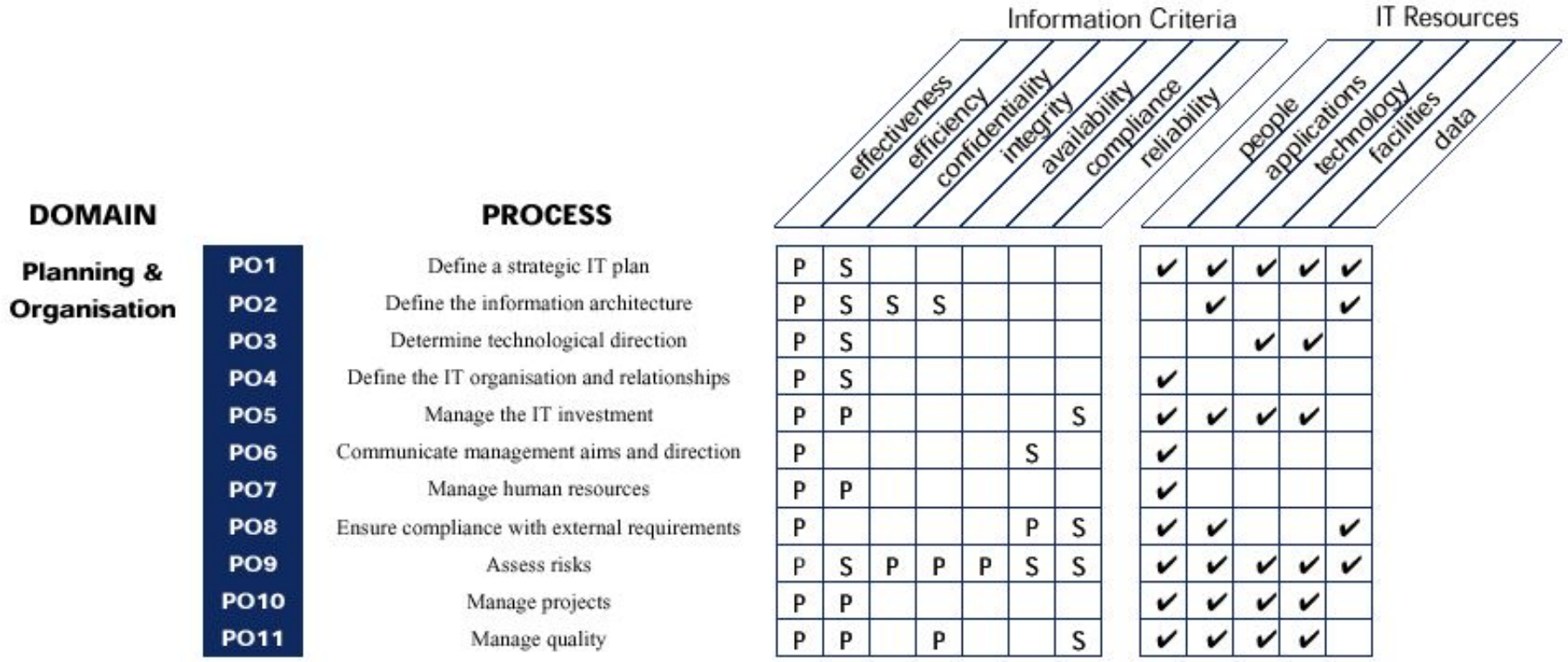
- CobiT: domena nr 1: „Planowanie i organizacja”
  - Definiowanie planu strategicznego dla IT
  - Wyznaczanie architektury informatycznej
  - Ustalanie kierunku technologicznego
  - Określanie organizacji i stosunków w IT
  - Zarządzanie inwestycjami IT
  - Przedstawianie kierownictwu celów i kierunków
  - Zarządzanie zasobami ludzkimi
  - Zapewnianie zgodności z wymogami zewnętrznymi
  - Szacowanie ryzyka
  - Zarządzanie projektami
  - Zarządzanie jakością

Planowanie i organizacja

			Kryteria informacji							Zasoby IT				
DOMENA		**PROCES**	efektywność	wydajność	poufność	integralność	dostępność	zgodność	rzetelność	ludzie	aplikacje	technologia	urządzenia	dane
Planowanie i organizacja	**PO1**	Definiowanie planu strategicznego dla IT	P	S						✓	✓	✓	✓	✓
	PO2	Wyznaczanie architektury informatycznej	P	S	S	S					✓			✓
	PO3	Ustalanie kierunku technologicznego	P	S								✓	✓	
	PO4	Określanie organizacji i stosunków w IT	P	S						✓				
	PO5	Zarządzanie inwestycjami IT	P	P					S	✓	✓	✓	✓	
	PO6	Przedstawianie kierownictwu celów i kierunków	P					S		✓				
	PO7	Zarządzanie zasobami ludzkimi	P	P						✓				
	PO8	Zapewnianie zgodności z wymogami zewnętrznymi	P					P	S	✓	✓			✓
	PO9	Szacowanie ryzyka	S	S	P	P	P	S	S	✓	✓	✓	✓	✓
	PO10	Zarządzanie projektami	P	P						✓	✓	✓	✓	
	PO11	Zarządzanie jakością	P	P		P			S	✓	✓			

P=czynnik podstawowy (Primary) S=czynnik drugorzedny (Secondary)

Planning & Organisation



DOMAIN		PROCESS	Information Criteria							IT Resources				
			effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	people	applications	technology	facilities	data
Planning & Organisation	PO1	Define a strategic IT plan	P	S						✔	✔	✔	✔	✔
	PO2	Define the information architecture	P	S	S	S					✔			✔
	PO3	Determine technological direction	P	S								✔	✔	
	PO4	Define the IT organisation and relationships	P	S						✔				
	PO5	Manage the IT investment	P	P					S	✔	✔	✔	✔	
	PO6	Communicate management aims and direction	P					S		✔				
	PO7	Manage human resources	P	P						✔				
	PO8	Ensure compliance with external requirements	P					P	S	✔	✔			✔
	PO9	Assess risks	P	S	P	P	P	S	S	✔	✔	✔	✔	✔
	PO10	Manage projects	P	P						✔	✔	✔	✔	
	PO11	Manage quality	P	P		P			S	✔	✔	✔	✔	

Definiowanie planu strategicznego dla IT

Cele kontrolne

- IT jako część planu długo- i krótkozasięgowego organizacji
- Długoterminowy plan IT
- Długoterminowe planowanie IT — podejście i struktura
- Długoterminowe zmiany planu IT
- Planowanie krótkoterminowe dla funkcji IT Komunikacja planów IT
- Monitorowanie i ocena planów IT
- Ocena istniejących systemów

Wyznaczanie architektury informatycznej

Cele kontrolne

- Model architektury informacji
- Korporacyjny słownik danych i reguły składni danych
- Schemat Klasyfikacji Danych
- Poziomy bezpieczeństwa

Ustalanie kierunku technologicznego

Cele kontrolne

- Planowanie infrastruktury technologicznej
- Monitorowanie przyszłych trendów i regulacji Awaryjne
- Infrastruktura Technologiczna
- Plany nabycia sprzętu i oprogramowania Standardy technologiczne

Określanie organizacji i stosunków w IT

Cele kontrolne

- Planowanie IT lub Komitet Sterujący Rozmieszczenie organizacyjne funkcji IT
- Przegląd osiągnięć organizacyjnych
- Role i obowiązki
- Odpowiedzialność za zapewnienie jakości
- Odpowiedzialność za bezpieczeństwo logiczne i fizyczne
- Własność i opieka
- Dane i własność systemu
- Nadzór Podział obowiązków
- Personel IT
- Opisy stanowisk lub stanowisk dla personelu IT
- Kluczowy personel IT
- Zasady i procedury dotyczące pracowników kontraktowych Relacje

Zarządzanie inwestycjami IT

Cele kontrolne

- Roczny budżet operacyjny IT
- Monitorowanie kosztów i korzyści
- Uzasadnienie kosztów i korzyści

Przedstawianie kierownictwu celów i kierunków

Cele kontrolne

- Pozytywne środowisko kontroli informacji
- Odpowiedzialność kierownictwa za polityki
- Komunikacja polityk organizacji
- Zasoby dotyczące wdrażania polityki
- Utrzymanie polityk
- Zgodność z politykami, procedurami i standardami
- Zaangażowanie w jakość
- Polityka ramowa bezpieczeństwa i kontroli wewnętrznej
- Prawa własności intelektualnej
- Komunikacja świadomości bezpieczeństwa IT

Zarządzanie zasobami ludzkimi

Cele kontrolne

- Rekrutacja i awans personelu
- Kwalifikacje personelu
- Role i obowiązki
- Szkolenie personelu
- Szkolenie przekrojowe lub wsparcie personelu
- Procedury odprawy personelu
- Ocena wydajności pracy pracownika
- Zmiana pracy i wypowiedzenie

Zapewnianie zgodności z wymogami zewnętrznymi

Cele kontrolne

- Przegląd wymagań zewnętrznych
- Praktyki i procedury zgodności z wymaganiami zewnętrznymi
- Bezpieczeństwo i zgodność z ergonomią
- Prywatność, własność intelektualna i przepływ danych
- Handlu elektronicznego
- Zgodność z umowami ubezpieczeniowymi

Szacowanie ryzyka

Cele kontrolne

- Ocena ryzyka biznesowego
- Podejście do oceny ryzyka Identyfikacja ryzyka
- Pomiar ryzyka
- Plan Działania na rzecz
- Ryzyka Akceptacja ryzyka
- Wybór zabezpieczeń
- Zobowiązanie do oceny ryzyka

Zarządzanie projektami

Cele kontrolne

- Ramy zarządzania projektami
- Udział działu użytkowników w inicjowaniu projektów
- Członkostwo i obowiązki w zespole projektowym
- Definicja projektu
- Zatwierdzenie projektu
- Zatwierdzenie fazy projektu
- Plan generalny projektu P
- lan zapewnienia jakości systemu
- Planowanie metod atestacyjnych F
- ormalne zarządzanie ryzykiem projektu
- Plan testów Plan treningowy Plan przeglądu powdrożeniowego

Zarządzanie jakością

Cele kontrolne

- Ogólny plan jakości
- Podejście do zapewnienia jakości
- Planowanie zapewnienia jakości
- Przegląd zapewnienia jakości przestrzegania standardów i procedur IT
- Metodologia cyklu życia rozwoju systemu
- Metodologia cyklu życia rozwoju systemu dla poważnych zmian w istniejącej technologii
- Aktualizacja metodologii cyklu życia rozwoju systemu Koordynacja i komunikacja
- Ramy pozyskiwania i utrzymania infrastruktury technologicznej
- Relacje z zewnętrznymi wykonawcami
- Standardy dokumentacji programu
- Standardy testowania programu
- Standardy testowania systemu
- Testy równoległe/pilotażowe
- Dokumentacja testowania systemu
- Ocena zapewnienia jakości przestrzegania standardów rozwoju
- Przegląd zapewnienia jakości realizacji celów IT
- Wskaźniki jakości
- Sprawozdania z przeglądów kontroli jakości

Podsumowanie

- Audyt IT to nie tylko kontrola ale szersze pojęcie coraz częściej uwzględniane w strategiach firm
- Audyt ma nie tylko zapobiegać, równierz tworzyć wartość dodaną dla firm.
- Audyt nie eliminuje ryzyka, lecz wybiera świadomy, akceptowalny poziom w zależności od kosztu.

Pytania

- Co jest przedmiotem oceny w audycie informatycznym
- Jakie są modele audytu? Opisz główne zasady klasycznego.
- Kostka COBIT. Jak ją rozumiesz?
- Procesy główne według modelu CobiT: domena nr 1: „Planowanie i organizacja”
- Procesy główne według modelu CobiT: domena 2 „Nabywanie i wdrażanie”
- Procesy główne według modelu CobiT : domena 3 : „Dostarczanie i wsparcie”
- Procesy główne według modelu CobiT : domena 4 „Monitorowanie i ocena „
- Jakie cele kontrolne w zarządzaniu jakością w modelu COBIT?