Kontrola zarządcza IT

Spotkanie audytorów wewnętrznych w Ministerstwie Finansów w dniu 26.08.2010r.

Przygotowała:
mgr inż. Joanna Karczewska CISA
j.karczewska@poczta.onet.pl

Ustawa o finansach publicznych

Rozdział 6 Kontrola zarządcza oraz koordynacja kontroli zarządczej w jednostkach sektora finansów publicznych

Art. 68.

1. **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.

2. Celem kontroli zarządczej jest zapewnienie w szczególności:

1) zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi;
2) skuteczności i efektywności działania;
3) wiarygodności sprawozdań;
4) ochrony zasobów;
5) przestrzegania i promowania zasad etycznego postępowania;
6) efektywności i skuteczności przepływu informacji;
7) zarządzania ryzykiem.

Ustawa o finansach publicznych

Komunikat Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych

1. Cel i charakter standardów

1.1. Standardy kontroli zarządczej dla sektora finansów publicznych, zwane dalej „standardami”, określają podstawowe wymagania odnoszące się do kontroli zarządczej w sektorze finansów publicznych.

1.2. Celem standardów jest promowanie wdrażania w sektorze finansów publicznych spójnego i jednolitego modelu kontroli zarządczej zgodnego z międzynarodowymi standardami w tym zakresie [COSO, INTOSAI, Komisja Europejska], z uwzględnieniem specyficznych zadań jednostki, która ją wdraża i warunków, w których jednostka działa.

1.3. Standardy stanowią uporządkowany zbiór wskazówek, które osoby odpowiedzialne za funkcjonowanie kontroli zarządczej powinny wykorzystać do tworzenia, oceny i doskonalenia systemów kontroli zarządczej.

Ustawa o finansach publicznych

Komunikat Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych

II. Standardy kontroli zarządczej

C. Mechanizmy kontroli

… System kontroli zarządczej powinien być elastyczny i dostosowany do specyficznych potrzeb jednostki. Mechanizmy kontroli powinny stanowić odpowiedź na konkretne ryzyko. Koszty wdrożenia i stosowania mechanizmów kontroli nie powinny być wyższe niż uzyskane dzięki nim korzyści.

15. Mechanizmy kontroli dotyczące systemów informatycznych

Należy określić mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych.

Ustawa o finansach publicznych

Dział VI Audyt wewnętrzny oraz koordynacja audytu wewnętrznego w jednostkach sektora finansów publicznych

Art. 272.

1. **Audyt wewnętrzny** jest działalnością niezależną i obiektywną, której celem jest wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze.

2. Ocena, o której mowa w ust. 1, dotyczy w szczególności adekwatności, skuteczności i efektywności kontroli zarządczej w dziale administracji rządowej lub jednostce.

Ustawa o finansach publicznych

Rozporządzenie Ministra Finansów z dnia 1 lutego 2010 r. w sprawie przeprowadzania i dokumentowania audytu wewnętrznego

§ 24. 1. Po przedstawieniu kierownikom komórek audytowanych ustaleń stanu faktycznego audytor wewnętrzny sporządza sprawozdanie, w którym w sposób jasny, rzetelny i zwięzły przedstawia wyniki audytu wewnętrznego.

2. Sprawozdanie zawiera w szczególności:

4) ustalenia stanu faktycznego wraz ze sklasyfikowanymi wynikami ich oceny według kryteriów, o których mowa w § 19 ust. 1 pkt 6;

5) wskazanie słabości kontroli zarządczej oraz analizę ich przyczyn;

6) skutki lub ryzyka wynikające ze wskazanych słabości kontroli zarządczej;

7) zalecenia w sprawie wyeliminowania słabości kontroli zarządczej lub wprowadzenia usprawnień, zwane dalej „zaleceniami”;

8) opinię audytora wewnętrznego w sprawie adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze ryzyka objętym zadaniem zapewniającym.

Ustawa o finansach publicznych

Ministerstwo Finansów / Bezpieczeństwo Finansowe / Audyt sektora finansów publicznych / Najczęściej zadawane pytania

Kryteria oceny ustaleń stanu faktycznego

Kryteria oceny muszą być:

1. odpowiednie (tj. powinny odnosić się do zakresu objętego zadaniem),
2. wiarygodne (tj. powinny odnosić się do wiarygodnych wyznaczników/danych),
3. istotne (tj. powinny odnosić się do kwestii istotnych z punktu widzenia danej jednostki, obszaru/procesu),
4. neutralne (tj. powinny pozwolić na obiektywną i niezależną ocenę badanego obszaru/procesu),
5. zrozumiałe (tj. powinny być zrozumiałe dla samego audytora wewnętrznego, kierownika jednostki, jak i kierownika/pracowników komórki audytowanej),
6. kompletne (tj. powinny obejmować całe spektrum badanego procesu/obszaru).

Ustawa o finansach publicznych

Ministerstwo Finansów / Bezpieczeństwo Finansowe / Audyt sektora finansów publicznych / Najczęściej zadawane pytania

Kryteria oceny ustaleń stanu faktycznego

Kryteria oceny są zatem punktami odniesienia, według których audytor wewnętrzny może ocenić w badanym obszarze/procesie m.in.: zgodność podjętych działań, adekwatność systemów kontroli zarządczej, a także gospodarność, wydajność lub efektywność konkretnych działań jednostki/komórki organizacyjnej.

Źródłami kryteriów oceny mogą być m.in.:

1. przepisy prawa i regulacje wewnętrzne,
2. standardy, normy oraz inne wskazówki o charakterze standardów opracowane przez uznane profesjonalne organizacje, organy, instytucje,
3. plany działalności i sprawozdania z planów działalności działu,
4. wytyczne kierownictwa jednostki,
5. dobre praktyki,
6. wyniki kontroli i audytu wewnętrznego.

Metodyka DAS

Podręcznik kontroli wykonania zadań

http://eca.europa.eu

1.2.4 System kontroli wewnętrznej służący zapewnieniu należytego zarządzania finansami

W celu uzyskania wystarczającej pewności, że cel należytego zarządzania finansami został osiągnięty, Komisja i inne jednostki kontrolowane muszą ustanowić odpowiedni system kontroli wewnętrznej.

Systemy informatyczne stanowią część systemu kontroli wewnętrznej w Komisji, co jest zgodne z proponowanym przez **COBIT** modelem dotyczącym stosowania ładu informatycznego w zarządzaniu informacjami i zasobami informatycznymi.

Europejski Trybunał Obrachunkowy: "finansowe sumienie" Unii Europejskiej

INTOSAI

GOV 9100 Guidelines for Internal Control Standards for the Public Sector

http://www.issai.org

2.3 Control Activities

Control activities are the policies and procedures established to address risks and to achieve the entity's objectives.

[Czynności kontrolne to polityki i procedury ustanowione, by zająć się ryzykami i osiągać cele podmiotu.]

2.3.1 Information Technology Control Activities

Information systems imply specific types of control activities.

[Systemy informatyczne wymagają specyficznych rodzajów czynności kontrolnych.]

Further guidance on information technology control activities can be obtained from the Information Systems Audit and Control Association (ISACA), in particular the ISACA Control Objectives for Information and Related Technology (**COBIT**) reference framework, and the proceedings of the INTOSAI IT-audit committee.

[Dodatkowe wytyczne dotyczące czynności kontrolnych IT można uzyskać od stowarzyszenia ISACA, w szczególności metodykę **COBIT**, oraz znaleźć w sprawozdaniach komitetu audytu IT INTOSAI.]

Metodyka COBIT®

- Jest to metodyka kontroli zarządczej IT - umożliwia opracowanie jednoznacznej polityki i dobrych praktyk nadzoru nad IT w całej firmie.
- Wspiera firmę w upewnianiu się, że:
  - IT jest dopasowane do potrzeb firmy,
  - IT napędza podmiot i maksymalizuje korzyści,
  - zasoby IT są wykorzystywane w sposób odpowiedzialny,
  - ryzyka IT są odpowiednio zarządzane.
- Warto wdrożyć COBIT jako model kontroli zarządczej IT, ponieważ:
  - umożliwia lepsze dopasowanie IT, bazujące na potrzebach firmy,
  - daje pogląd na to, co robi IT, zrozumiały dla kierownictwa,
  - jasno określa własność i odpowiedzialność, w oparciu o procesy,
  - jest uznawany przez strony trzecie i prawodawców,
  - zapewnia zrozumienie przez wszystkich interesariuszy,
  - spełnia wymogi COSO dotyczące środowiska kontrolnego IT.

Metodyka COBIT®

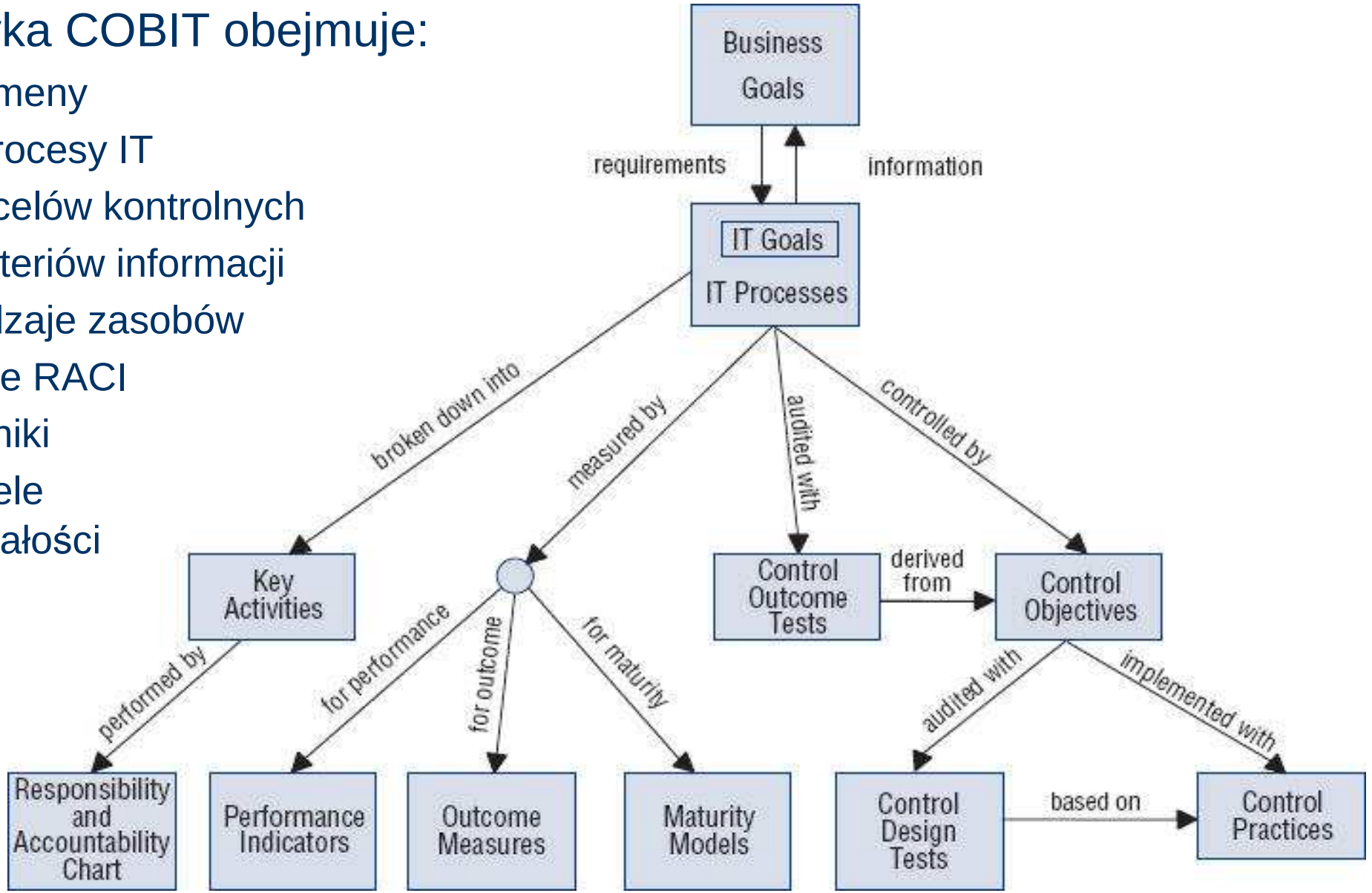
- Z metodyki COBIT mogą korzystać:
  - dyrekcja firmy [executive management] – w celu osiągania wartości z inwestycji IT oraz zrównoważenia ryzyka i kontroli inwestycji w środowisku IT, które dość często bywa nieprzewidywalne,
  - kierownictwo działów merytorycznych [business management] – w celu uzyskania zapewnienia w sprawach zarządzania i kontroli usług IT dostarczanych przez służby wewnętrzne lub dostawców zewnętrznych,
  - kierownictwo IT [IT management] – w celu dostarczania kontrolowanych i zarządzanych usług IT wymaganych przez firmę dla wsparcia strategii firmowej,
  - audytorzy [auditors] – w celu potwierdzenia swoich opinii i/lub udzielania kierownictwu rad dotyczących wewnętrznych mechanizmów kontrolnych.

Metodyka COBIT®

- Metodyka COBIT:
  - tworzy powiązania celów IT z celami podmiotu,
  - identyfikuje podstawowe zasoby IT,
  - organizuje czynności IT według powszechnie akceptowanego modelu procesowego,
  - wyznacza mierniki i modele dojrzałości, za pomocą których można zmierzyć osiąganie celów oraz zidentyfikować odpowiedzialność właścicieli procesów (właścicieli biznesowych i IT),
  - definiuje cele kontrolne, czyli ogólne deklaracje minimalnych dobrych praktyk stosowanych przez kierownictwo w celu zapewnienia kontroli nad każdym procesem IT,
  - zawiera praktyki kontrolne, czyli kluczowe mechanizmy kontrolne, które wspierają osiąganie celów kontrolnych oraz zapobieganie, wykrywanie i naprawianie niepożądanych zdarzeń,
  - podaje deklaracje wartości i ryzyk, czyli przykłady korzyści dla firmy wynikających z osiągnięcia celu kontrolnego oraz ryzyk, które można zmniejszyć.

Metodyka COBIT®

- Metodyka COBIT obejmuje:
  - 4 domeny
  - 34 procesy IT
  - 210 celów kontrolnych
  - 7 kryteriów informacji
  - 4 rodzaje zasobów
  - tabele RACI
  - mierniki
  - modele dojrzałości



Źródło: COBIT 4.1. ©1996-2007 ITGI. All rights reserved. Used by permission

DS5 - Zapewnienie bezpieczeństwa systemów

Kontrolę nad procesem IT
zapewnienia bezpieczeństwa systemów

który spełnia wymagania biznesu wobec IT **Cele IT**
utrzymania integralności informacji i infrastruktury, która je przetwarza oraz minimalizacji wpływu podatności i incydentów dotyczących bezpieczeństwa

poprzez skupienie się na **Cele procesu**
ustalaniu polityk, planów i procedur dotyczących bezpieczeństwa IT oraz monitorowaniu, wykrywaniu, raportowaniu i wyjaśnianiu podatności i incydentów dotyczących bezpieczeństwa

osiąga się **Cele czynności**
- rozumiejąc wymogi, podatności i zagrożenia dotyczące bezpieczeństwa
- zarządzając w sposób ujednolicony tożsamością i autoryzacją użytkowników
- regularnie testując bezpieczeństwo

i mierzy za pomocą **Kluczowe mierniki**
- liczby incydentów szkodzących reputacji podmiotu wśród społeczeństwa
- liczby systemów, w których nie są spełnione wymogi bezpieczeństwa
- liczby naruszeń dotyczących rozdziału obowiązków

DS5 - Zapewnienie bezpieczeństwa systemów

- Cele kontrolne:

  DS5.1 Zarządzanie bezpieczeństwem teleinformatycznym

  DS5.2 Plan bezpieczeństwa IT

  Należy przełożyć wymagania podmiotu, oraz wymogi dotyczące ryzyka i zgodności na ogólny plan bezpieczeństwa IT, uwzględniając infrastrukturę IT oraz podejście podmiotu do bezpieczeństwa. Należy zadbać o to, by plan został ujęty w politykach i procedurach bezpieczeństwa i towarzyszyły mu odpowiednie inwestycje w usługi, pracowników, oprogramowanie i sprzęt. Z politykami i procedurami bezpieczeństwa należy zaznajomić interesariuszy i użytkowników.

  DS5.3 Zarządzanie tożsamością

  DS5.4 Zarządzanie kontami użytkowników

  DS5.5 Testowanie, nadzorowanie i monitorowanie bezpieczeństwa

  DS5.6 Definiowanie incydentów dot. bezpieczeństwa

  DS5.7 Ochrona środków technicznych dot. bezpieczeństwa

  DS5.8 Zarządzanie kluczami szyfrującymi

  DS5.9 Złośliwe oprogramowanie - zapobieganie, wykrywanie i działania naprawcze

  DS5.10 Bezpieczeństwo sieci

  DS5.11 Wymiana danych wrażliwych

DS5 - Zapewnienie bezpieczeństwa systemów

- Tabela RACI:

Stanowiska / Czynności	Szef jednostki	Gł.Księgowy		Kierownik DI					Audytor	
Definiowanie i utrzymanie polityki bezpieczeństwa informacji										
Define, establish and operate an identity (account) management process.										
Monitor potential and actual security incidents.										
Periodically review and validate user access rights and privileges.										
Establish and maintain procedures for maintaining and safeguarding cryptographic keys.										
Implement and maintain technical and procedural controls to protect information flows across networks.										
Conduct regular vulnerability assessments										

R - odpowiedzialny, **A** - decyzyjny, **C** - konsultowany, **I** - informowany

DS5 - Zapewnienie bezpieczeństwa systemów

- Mierniki:
  - Liczba incydentów mających wpływ na działalność podmiotu
  - Liczba systemów, w których nie są spełnione wymogi bezpieczeństwa
  - Czas nadawanie, zmiany i cofnięcia praw dostępu
  - Liczba i rodzaje domniemanych i faktycznych naruszeń dostępu
  - Liczba naruszeń dotyczących rozdziału obowiązków
  - Procent użytkowników, którzy nie stosują się do standardów dot. haseł
  - Liczba i rodzaj kodów złośliwych, którym udało się zapobiec
  - Częstotliwość i przegląd typów zdarzeń dot. bezpieczeństwa, które należy monitorować
  - Liczba i typ zdezaktualizowanych kont
  - Liczba nieautoryzowanych adresów IP, portów i zablokowanych typów ruchu
  - Procent kluczy kryptograficznych ujawnionych i cofniętych
  - Liczba praw dostępu autoryzowanych, cofniętych, zresetowanych lub zmienionych

- Model dojrzałości – poziomy od 0 (nieistniejący) do 5 (zoptymalizowany)

DS5 - Zapewnienie bezpieczeństwa systemów

- Praktyki kontrolne:

  np. Należy zebrać wymagania dotyczące bezpieczeństwa informacji zawarte w planach taktycznych IT (PO1), klasyfikacji danych (PO2), standardach technologicznych (PO3), politykach bezpieczeństwa i kontroli (PO6), zarządzaniu ryzykiem (PO9) oraz zewnętrznych wymogach zgodności (ME3) i uwzględnić je w ogólnym planie bezpieczeństwa IT.

- Wyznaczniki ryzyka [Risk Drivers]

  np. Plan bezpieczeństwa IT niedopasowany do wymagań podmiotu.
  np. Różnice pomiędzy zaplanowanymi i wdrożonymi środkami bezpieczeństwa IT

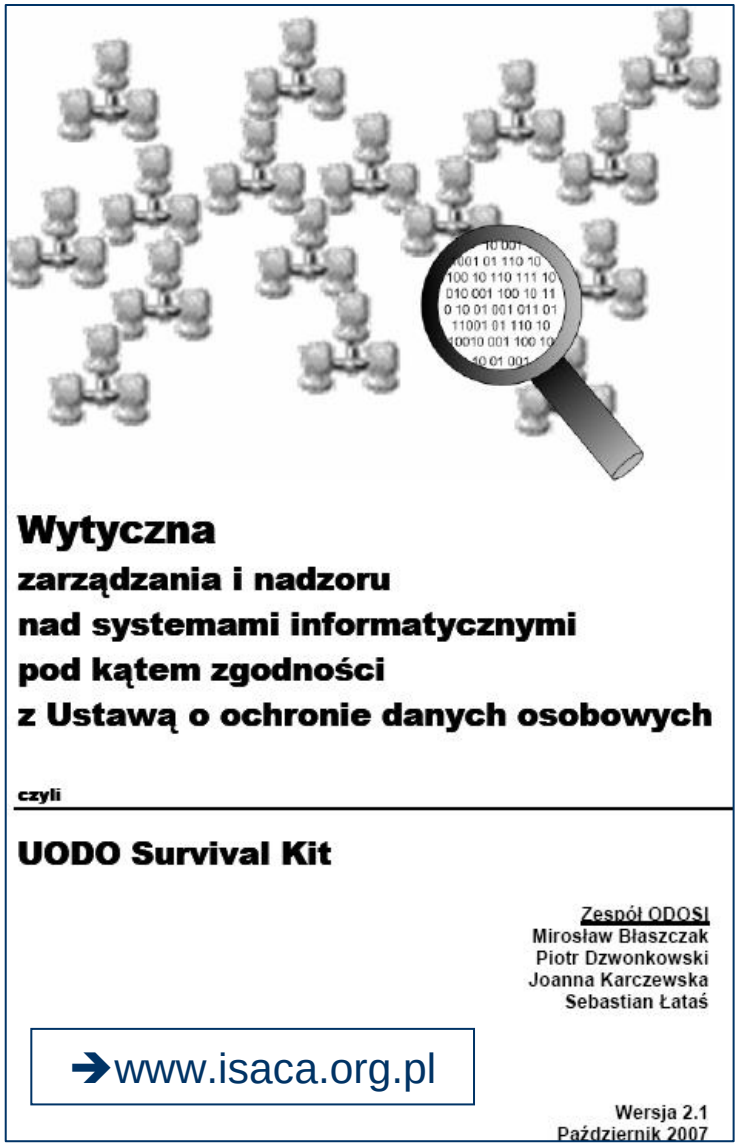
- Wytyczne audytu i zapewnienia

  np. Należy ustalić, czy istnieje proces regularnej aktualizacji planu bezpieczeństwa IT i czy ten proces wymaga, by odpowiedni szczebel kierownictwa dokonywał przeglądu zmian i je akceptował.

  np. Należy zwrócić się do działu kadr o informacje dot. kilku przeniesień pracowników oraz rozwiązań umowy o pracę i ustalić, czy dostęp został odpowiednio i w stosownym czasie zmodyfikowany lub cofnięty, poprzez sprawdzenie konfiguracji kont i poziomów dostępu tych użytkowników do systemów.

Metodyka COBIT®

- Przykład zastosowania – Ustawa o ochronie danych osobowych



MAPOWANIE	
UODO	**Cele kontrolne COBIT 4.1**
Artykul 26 Ustawy: 1. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były: 1)... 3)... 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. 2.	ME3.1-4, PO2.3, PO4.8-9, PO6.3, **DS11.2** DS11.4

Rozporządzenie	Cele kontrolne COBIT 4.1
§ 1.	ME3.1-4, PO6.2
§ 2.	ME3.1-4
§ 3.	PO4.8, DS5.2
§ 4.	PO2.2-3, DS5.2, DS5.7, DS5.10, DS12.1-2
§ 5.	PO6.2
pkt 1)	DS5.3-4
pkt 2)	AI2.3-4, DS5.3-4
pkt 3)	PO7.8

Metodyka COBIT®

- Zastosowanie do audytów informatycznych:
  - Biuro Trybunału Konstytucyjnego
  - Ministerstwo Finansów
  - Ministerstwo Rozwoju Regionalnego
  - Naczelna Dyrekcja Archiwów Państwowych
  - Urząd Regulacji Energetyki
  - Wojewódzki Fundusz Ochrony Środowiska i Gospodarki Wodnej w Poznaniu

Publikacje ISACA

Metodyka COBIT

- COBIT 4.1
- COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition
- IT Assurance Guide: Using COBIT
- COBIT Security Baseline, 2nd Edition
- COBIT and Application Controls: A Management Guide
- COBIT Quickstart, 2nd Edition

Audyt i zapewnienie

- Standards, Guidelines, and Tools and Techniques
- ITAF™: A Professional Practices Framework for IT Assurance
- Monitoring of Internal Controls and IT (Exposure Draft)

IT Governance

- Board Briefing on IT Governance, 2nd Edition
- Implementing and Continually Improving IT Governance

Metodyka Val IT

- Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0
- Enterprise Value: Governance of IT Investments, Getting Started With Value Management
- Value Management Guidance for Assurance Professionals - Using Val IT 2.0
- The Business Case Guide - Using Val IT 2.0

Metodyka Risk IT

- The Risk IT Framework
- The Risk IT Practitioner Guide