
AUDYT
SYSTEMÓW
INFORMATYCZNYCH

Kontakt

- **Dr. prof.** Swietłana Kaszuba
- e-mail:

swietlana.kashuba@byd.pl

tel. 570004779

Plan zajęcia

Bibliografia

Materiał teoretyczny

Zadania

Bibliografia

1. Marian Molski, Małgorzata £acheta , Przewodnik audytora systemów informatycznych, Helion 2016
2. Krzysztof Liderman, Adam E. Patkowski: Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego Krzysztof Liderman, Adam E. Patkowski: Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego. WAT, 2003
3. *COBIT 3rd Edition,* IT Governance Institute, 2002.
4. *ISO/IEC 9126 : Information technology – Software Product Evaluation – Quality characteristics and guidelines for their use,* 1991.
5. *strona internetowa metodyki PRINCE2,* www.prince2.org.uk, www.prince2.com.
6. Davis C., Schiller M., Wheeler K., IT Auditing Using Controls to Protect Information Assets, McGraw-Hill Osborne, 2011
7. Andrzej Zalewski, Rafał Cegieła, Krzysztof Sacha

Modele i praktyka audytu informatycznego

Instytut Automatyki i Informatyki Stosowanej, Wydział Elektroniki i

AUDYT SYSTEMÓW INFORMATYCZNYCH

Co to jest?

- „Sprawdzenie procedur stosowanych w systemie przetwarzania danych w celu oceny ich skutecznosci i poprawnosci oraz w celu zalecenia ulepszen"
- Źródło: PN-I-02000:2002, pkt 3.1.007

Cele audytu

- Audyt jest prowadzony w celu stwierdzenia stopnia zgodności ocenianego systemu z określonym standartem lub normą wybraną jako punkt odniesienia. W przypadku audytu informatycznego są to normy dotyczące zarządzania procesami IT (ISO/IEC 20000Audyt jest prowadzony w celu stwierdzenia stopnia zgodności ocenianego systemu z określonym standartem lub normą wybraną jako punkt odniesienia. W przypadku audytu informatycznego są to normy dotyczące

Zadania Audytu IT

1. Przegląd zasad i procedur dotyczących systemów informatycznych mający na celu ocenę, czy zostały one opracowane przy uwzględnieniu wymagań kierownictwa firmy i istniejących przepisów wewnętrznych i zewnętrznych
2. Przegląd zasad i procedur dotyczących systemów informatycznych mający na celu ocenę, czy są one efektywne i zapewniają niezawodność przetwarzania i bezpieczeństwo danych

Zadania Audytu IT

3. Analiza i uzgadnianie nowych zasad i procedur
4. Sprawdzenie, czy systemy i aplikacje zapewniają odpowiednie mechanizmy kontroli
5. Ocena, czy mechanizmy kontroli w systemach i aplikacjach zapewniają ochronę przed stratami lub poważnymi błędami
6. Sprawdzenie, czy systemy i aplikacje są efektywne i ekonomiczne w użytkowaniu
7. Przegląd i ocena integralności systemów operacyjnych

Zadania Audytu IT

8. Ocena, czy systemy komputerowe, sieci telekomunikacyjne i programy komputerowe posiadają odpowiednią dokumentację, a ich użytkownicy posiadają właściwe umiejętności, co pozwala na ograniczenie/ wyeliminowanie potencjalnych błędów
9. Przegląd mechanizmów kontroli w aplikacjach służących do przetwarzania danych mający na celu ocenę ich niezawodności, a także terminowości, dokładności i kompletności przetwarzania danych

Zadania Audytu IT

0. Udział w:
   - opiniowaniu, projektowaniu oraz badaniu zgodności mechanizmów kontroli w ww. aplikacjach z polityką firmy i wymogami zewnętrznymi,
   10. opracowywaniu lub wprowadzaniu istotnych modyfikacji do systemów komputerowych lub aplikacji.
2. Przegląd zabezpieczeń fizycznych i logicznych sprzętu komputerowego i oprogramowania,
3. Przegląd zabezpieczeń fizycznych danych

Zadania Audytu IT

3. opracowywanie zaleceń działań korygujących w przypadku zidentyfikowania problemów w zakresie zasad, procedur i mechanizmów kontroli
4. przegląd zabezpieczeń fizycznych sprzętu komputerowego mający na celu weryfikację istnienia i adekwatności planu awaryjnego zapewniającego kontynuację działania kluczowych aplikacji w przypadku zakłóceń (np. zasilanie awaryjne, urządzenia zapasowe, transport pracowników i sprzętu)

Zadania Audytu IT

15. przegląd zabezpieczeń fizycznych zbiorów danych mający na celu ocenę adekwatności mechanizmów kontroli dostępu i regularności tworzenia kopii zapasowych
16. przegląd adekwatności mechanizmów kontroli systemów komputerowych zawartych w programach komputerowych (weryfikacja zakresu ich wdrożenia, a także możliwości ich obejścia)
17. przegląd procesu rozwoju aplikacji (tj. ocena adekwatności i efektywności rozwoju nowych aplikacji, a także zasad i procedur korzystania z dostawców zewnętrznych)

Zadania Audytu IT

8. przegląd mechanizmów kontroli aplikacji mający na celu ocenę:
   - mechanizmów kontroli autoryzacji
   - kompletności danych wejściowych

18. dokładności danych wejściowych

- przegląd mechanizmów kontroli aplikacji mający na celu ocenę:

18. integralności danych
19. kompletności i dokładności procesu uzgadniania danych
    - kompletności, dokładności i kosztu przechowywania danych

18. poziomu ograniczenia dostępu do aktywów i rejestrów

Zadania Audytu IT

0. przegląd struktury organizacyjnej, podziału obowiązków i uprawnień
   w ramach komórek informatycznych
1. przegląd istnienia odpowiedniej struktury zapewniającej przeszkolenie pracowników
   w różnych dziedzinach lub obecność pracowników, którzy mogą zastąpić kluczowych pracowników w przypadku ich nieobecności
2. sprawdzenie, czy podział obowiązków zapewnia odpowiedni poziom kontroli (np. rozdzielenie funkcji związanych
   z rozwojem programów i systemów obsługi komputerów, kontroli danych wejściowych i grup zajmujących się mechanizmami kontroli aplikacji)

Modele audytu informatycznego

Przedmiotem oceny w audycie informatycznym są:

- kontrola/nadzór nad systemami informacyjnymi w organizacji;
- sposób zarządzania przedsięwzięciami informatycznymi;
- konkretne rozwiązania informatyczne (działające lub projektowane).

Modele audytu

modele audytu:

- model klasyczny – ocena kontroli i nadzoru nad systemami informacyjnymi w organizacji;
- audyt formalny – ocena organizacji przedsięwzięć;
- audyt merytoryczny – ocena rozwiązań informatycznych.

Główne problemy, jakie stają przed audytorem, to:

- określenie kryteriów oceny;
- pozyskanie informacji o przedmiocie audytu;
- posiadanie lub uzyskanie wiedzy niebędnej dla przeprowadzenia oceny.

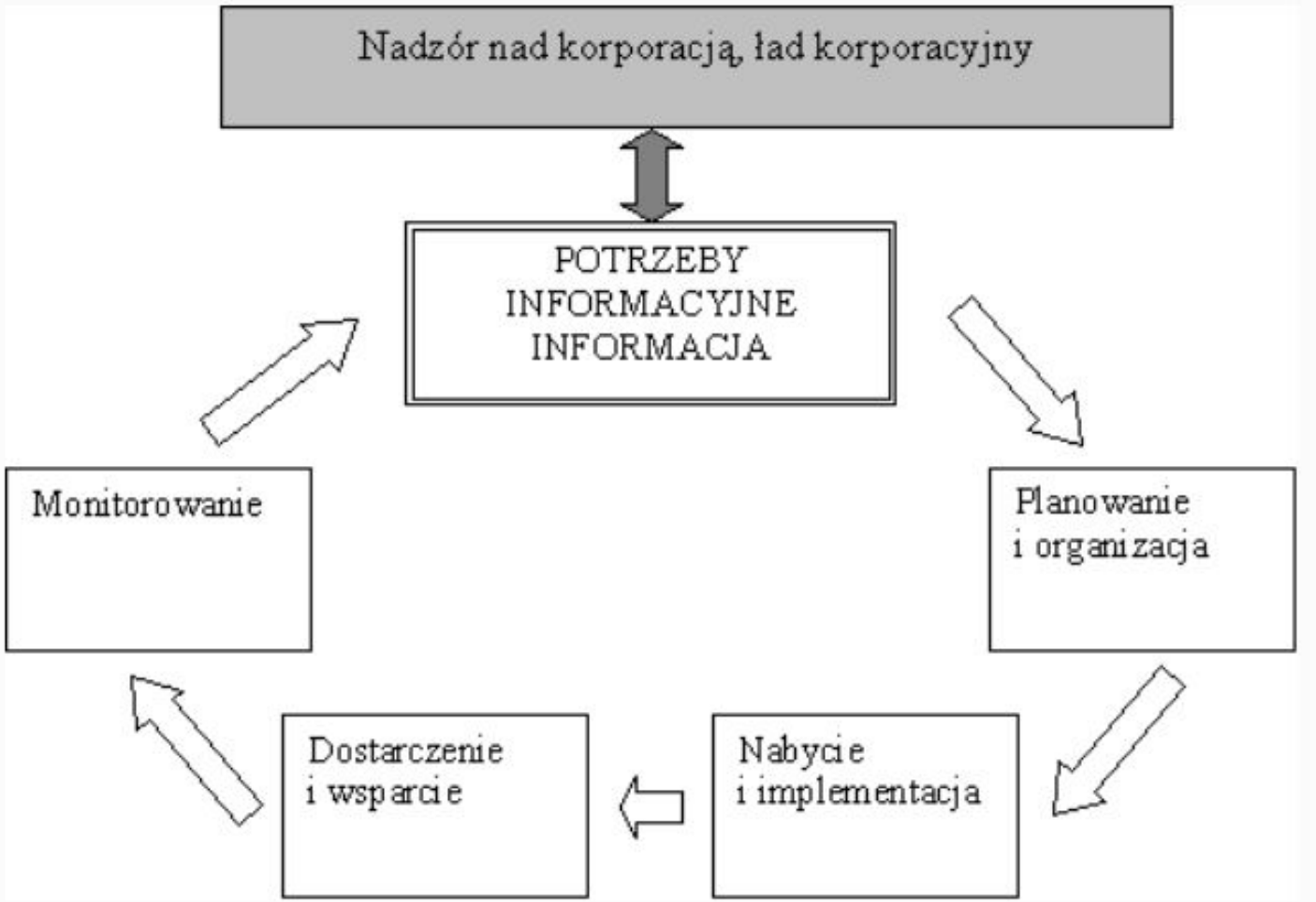
Model klasyczny#

- W modelu klasycznym audyt informatyczny stanowi jeden z mechanizmów nadzoru nad organizacją. **Jego celem jest odpowiedź na pytanie: czy dana organizacja posiada wystarczający nadzór nad wykorzystywanymi w niej systemami informacyjnymi oraz ich rozwojem.** W modelu tym ocenia się rozwiązania techniczne i organizacyjne składające się na funkcjonowanie systemów informacyjnych w danej organizacji względem modelu referencyjnego. Najpowszechniej stosowany jest model opisany w standardzie COBIT (ang. *Control Objectives for Information and Related Technology*) [COBIT].

Model klasyczny#

- Standard ten określa wzorcowy model procesów organizacyjnych zapewniających prawidłowy nadzór nad funkcjonowaniem i rozwojem infrastruktury teleinformatycznej przedsiębiorstwa. W modelu tym wyróżniono 4. dziedziny (ang. *domains*) odpowiadające cyklowi życia rozwiązań informatycznych w organizacji (por. rysunek 1). Obejmują więc one: planowanie i organizację, nabycie i implementację, dostarczenie i wsparcie, monitorowanie. W każdej z dziedzin wyróżniono procesy niezbędne dla prawidłowego nadzoru nad systemami informatycznymi w organizacji. Dla każdego procesu zdefiniowane zostały:
- cel biznesowy,
- kryteria oceny systemu zależne od realizacji procesu,
- kluczowe wskaźniki celu i wydajności,
- krytyczne czynniki sukcesu,
- zasoby konieczne do realizacji procesu,
- 6-stopniowy model dojrzałości,
- kluczowe i szczegółowe mechanizmy kontrolne.

Dziedziny modelu COBIT



Rysunek 1. Dziedziny modelu COBIT.

Model audytu formalnego

Istotą audytu formalnego jest ocena procesu wytwarzania (budowy) systemu informatycznego.

Organizację przedsięwzięcia informatycznego można zobrazować jako strukturę dwuwarstwową, na którą składa się:

- Przyjęta metodyka zarządzania projektem;
- Stosowane w ramach tej metodyki metody projektowania.

Co oceniamy

W audycie formalnym podstawą oceny są metodyki zarządzania i projektowania.

- **Metodyka zarządzania** określa zwykle: procesy związane z zarządzaniem przedsięwzięciem i ich wzajemne powiązania, strukturę zespołu projektowego oraz sposób dokumentowania jego przebiegu.
- **Metodyki projektowania** definiują sam proces projektowania konkretnych rozwiązań informatycznych, sposób dokumentowania rozwiązań konstrukcyjnych (notacje i modele) oraz artefakty będące rezultatem poszczególnych faz projektowania.

Co badamy

W audycie formalnym bada się:

- Czy i jak w zarządzaniu przedsięwzięciem realizowane są procesy określone w metodyce?
- Czy przedsięwzięcie jest dokumentowane zgodnie z przyjętą metodyką?
- Czy zgodne z dokumentacją procesu wytwarzania systemu informatycznego, organizowany zespół projektowy?
- Czy wszystkie artefakty procesu projektowego zostały wytworzone?

Źródłem informacji o przedmiocie audytu jest przede wszystkim dokumentacja związana z procesem projektowym oraz dokumentacja projektowa.

Model audytu merytorycznego

Audyt merytoryczny ma na celu ocenę konkretnych rozwiązań informatycznych, a także całych systemów informatycznych na różnych etapach ich cyklu życia. Typowe sytuacje, w których przeprowadzany audyt, to:

- Trwająca realizacja projektu – audyt stanowi wówczas jeden z mechanizmów nadzoru organizacji nad przedsięwzięciem – zwykle dotyczy on wielkich przedsięwzięć informatycznych, gdy zlecająca ich realizację organizacja nie posiada wystarczającej wiedzy merytorycznej by „zapanować” nad realizowanymi rozwiązaniami;
- Związany jest z procesem odbioru zamówionego rozwiązania informatycznego;
- Po klęsce przedsięwzięcia – w poszukiwaniu przyczyn klęski.

Kryteria oceny

Celem audytu merytorycznego jest najogólniej: ocena *sprawności* rozwiązań informatycznych

W praktyce rozwiązania informatyczne oceniane są pod kątem właściwości takich, jak:

- użyteczność,
- jakość,
- wydajność,
- niezawodność,
- bezpieczeństwo,
- wiarygodność,
- zgodność z odpowiednimi normami technicznymi (np. kategorie okablowania).

Użyteczność

Przez użyteczność rozumiemy spełnienie przez system wymagań funkcjonalnych, przy założeniu, że osiągnięte parametry wydajności i niezawodności systemu umożliwiają badanie funkcjonalności.

Przedmiotem oceny może być rozwiązanie informatyczne na dowolnym etapie jego cyklu życia, w skrajnym przypadku ocenie podlegać może specyfikacja wymagań względem dokumentów źródłowych.

Jakość

Jakość nie jest pojęciem samoistnym lecz agregatem pojęciowym łączącym w sobie inne cechy składające się na to pojęcie

Jakość

Grupa kryteriów	Kryterium
Funkcjonalność	Adekwatność Dokładność Współdziałanie Zgodność Bezpieczeństwo
Niezawodność	Dojrzałość Tolerancja błędów Odtwarzalność
Użyteczność	Zrozumiałość Łatwość nauki Łatwość użytkowania
Wydajność	Charakterystyki czasowe Gospodarka zasobami
Pielęgnowalność	Podatność na analizę Podatność na zmiany Stabilność Testowalność
Przenośność	Łatwość adaptacji Łatwość instalacji Zgodność Zastępowalność

Wydajność

Ocena wydajności, w teorii, winna polegać na porównaniu wymaganych parametrów wydajnościowych rozwiązania z ich wartościami osiągniętymi przez zrealizowane rozwiązanie.

Głównymi przeszkodą w zastosowaniu tego podejścia jest:

- Brak standardów regulujących sposób definiowania parametrów wydajnościowych;
- Niepełna adekwatność stosowanych miar wydajności – np. miara liczby transakcji przetwarzanych w ciągu sekundy nie jest adekwatna we wszystkich sytuacjach;
- Brak możliwości użycia istniejących modeli analitycznych do oceny rzeczywistych rozwiązań komercyjnych;

Wydajność

Zagadnienie oceny wydajności rozwiązania informatycznego w wielu sytuacjach może zostać zdekomponowane na:

- Ocenę wydajności systemu wprowadzania danych do systemu z wykorzystaniem np. tradycyjnych modeli systemów masowej obsługi;
- Ocenę wydajności przetwarzania danych realizowanego przez system informatyczny.

Niezawodność

Niezawodność jest miarą odporności rozwiązań na awarie.

Wymagania niezawodnościowe winny być formułowane w sposób ilościowy. W odniesieniu do rozwiązań sprzętowych korzysta się zwykle z modelu średniego czasu między awariami (MTBF – ang. *Mean Time Between Failure*) – producenci poszczególnych komponentów systemu, zwłaszcza tych mechanicznych podają parametry tego typu dla wytwarzanych przez nich urządzeń.

Niezawodność

Ocena niezawodności złożonych rozwiązań informatycznych obejmuje:

- Ocenę adekwatności, dostateczności i poprawności zastosowanych rozwiązań;
- Ocenę parametrów niezawodnościowych stosowanego sprzętu;
- Ocenę realności i adekwatność wymagań na maksymalny czas trwania awarii;
- Ocenę skuteczności mechanizmów ograniczających skutki awarii i czas ich trwania.

Bezpieczeństwo

Bezpieczeństwo systemu jest miarą jego podatności na niepożądane zmiany i ingerencje. Właściwym punktem odniesienia dla oceny bezpieczeństwa są istniejące i uznawane standardy bezpieczeństwa

Wiarygodność

Pod pojęciem *wiarygodności rozwiązania informatycznego* rozumiemy stopień racjonalnego umotywowania poszczególnych decyzji konstrukcyjnych.

- W prawidłowo prowadzonych projekcie informatycznym każda istotna decyzja projektowa powinna zmierzać do osiągnięcia założonego celu, jakim jest realizacja zidentyfikowanych wymagań obejmujących zarówno funkcjonalność, jak i inne pożądane właściwości w tym właściwości niefunkcjonalne.
- Przedmiotem oceny staje się więc istnienie i poprawność ww. elementów.
- Źródłami informacji są tutaj: w idealnym przypadku dokumentacja projektowa, a w praktyce także wywiady z autorami poszczególnych rozwiązań i innymi osobami zaangażowanymi w projekt.

Zgodność z odpowiednimi normami technicznymi

Ocena względem tego kryterium dotyczy wyłącznie rozwiązań sprzętowych i polega na zbadaniu czy dane rozwiązanie posiada właściwości określone w odpowiednich normach technicznych.

Ocena ta jest przeprowadzana w drodze badania deklaracji zgodności z odpowiednimi normami dawanymi przez wytwórców sprzętu lub bezpośrednich pomiarów ocenianej instalacji lub urządzeń.

Źródła informacji

Sposób pozyskania i źródła informacji w audycie merytorycznym są silnie uzależnione od konkretnej sytuacji projektowej: w idealnym przypadku informacje o przedmiocie audytu uzyskuje się na podstawie dokumentacji projektowej, powykonawczej, projektu i raportów testów oraz dokumentacji technicznej zastosowanych narzędzi komercyjnych

W praktyce audytu często zachodzi konieczność konsultacji z ekspertami dziedzinowymi.

Podsumowanie

- Klasycznym audyt informatyczny stanowi jeden z mechanizmów nadzoru nad organizacją. Do przeprowadzenia audytu niezbędna jest wiedza na temat modelu referencyjnego opisanego w standardzie COBIT.
- Audyt formalny wymaga wiedzy z zakresu metodyk projektowania rozwiązań informatycznych oraz zarządzania projektami. Może on zostać przeprowadzony również przez osoby nie posiadające specjalistycznej wiedzy dziedzinowej, w szczególności informatycznej.
- Audyt merytoryczny wymaga szczegółowej wiedzy specjalistycznej pozwalającej poznać i ocenić rzeczywiste rozwiązania techniczne i organizacyjne. Wymaga on samodzielnego, indywidualnego zdefiniowania kryteriów oceny

Zadanie

Charakteryzuj modele audytu

	Audyt klasyczny	Audyt formalny	Audyt merytoryczny
Źródła informacji o przedmiocie oceny			
Przedmiotem oceny			
Kryteria oceny			
Zakres niezbędnej wiedzy			

Dziękuję Państwu za uwagę.