Informatyka w kontroli i audycie

Informatyka w kontroli i audycie

mgr inż Marcin Kwiecień

Wstęp

Terminy zajęć

- 30.11.2013 - godzina 8:00 - 9:30 ; 9:45 - 11:15
- 15.12.2013 - godzina 8:00 - 9:30 ; 9:45 - 11:15
- 05.04.2014 - godzina 15:45 - 17:15

Zaliczenie

test zaliczeniowy 05.04.2014 roku na pierwszych zajęciach, ok. 20 minut

Informatyka w kontroli i audycie

Wykład **informatyka w kontroli i audycie** zawiera zagadnienia dotyczące teorii systemów informatycznych wspomagających zarządzanie organizacją oraz przewidywania i określenia ryzyka informatycznego.

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Program ćwiczeń zawiera tworzenie informatycznych systemów kontroli oraz tworzenia baz danych w procesie kontroli i audytu.

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Systemy informatyczne wspomagające zarządzanie organizacją, Informatyczne systemy kontrolii.

Bazy danych w procesie kontrolii i audytu.

Ryzyka informatyczne.

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Książki:
Przewodnik audytora systemów informatycznych; M. Molski, M. Łacheta, Helion 2007

Normy dotyczące audytów informatycznych

Narzędzia informatyczne do wspomagania audytu

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Czym jest informatyka dzisiaj ?

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Czym jest informatyka dzisiaj ?

- narzędziem wspomagającym procesy w przedsiębiorstwach,
- podstawową dziedziną przedsiębiorstw,
- elementem ułatwiającym kontakt,
- ważna i szeroko stosowana,
- brak dziedzin w których nie można jej zastosować,
- podstawowy element łączący ze sobą wszystkie gałęzie administracyjne,
- ułatwiająca i przyśpieszająca pracę,

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Czym jest informatyka dzisiaj ?

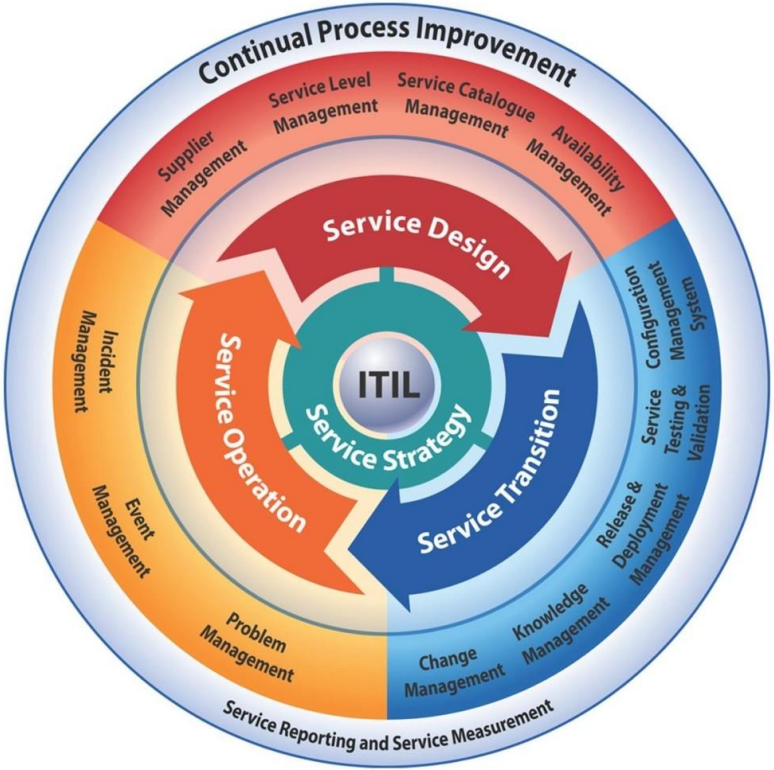
- systemy informatyczne są skomplikowane i złożone

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Czym jest informatyka dzisiaj ?

Information Technology Infrastructure Library



Informatyka w kontroli i audycie

Czym jest informatyka dzisiaj ?

- nowy trend to praca w “chumarch” obliczeniowych (cloud computing)

- ważne staje sie odpowiednie zabezpieczanie elementów systemów, w tym danych do których dostęp powinny mieć tylko zaufane osoby

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Informatyka w przedsiębiorstwie staje się elementem łączącym i scalającym wszystkie działy ze sobą. Jest kluczowa dla każdego elementu zarówno w administracji, produkcji etc.

Umiejscowienie informatyka i informatyki w firmie jest o tyle ważne, że automatycznie definiują one jej role informatyki w całym procesie technologicznym oraz i przede wszystkim decyzyjnym.

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Informatyka jako przedmiot audytu

Informatyka jako pomoc w audycie

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Informatyka jako przedmiot audytu

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Informatyka jako przedmiot audytu

Pierwszą i najważniejszą rzeczą jaka pojawia się w miarę zastanawiania się nad tym problemem, to założenie, że audyt informatyczny to sprawdzenie legalności oprogramowania i inwentaryzacji sprzętu.

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Takie założenie sprowadza audyt to uruchomienia programów i weryfikacji dokumentacji z otrzymywanymi wynikami, i taki audyt jest także pożądany, ale tak naprawdę jest tylko jego namiastką i elementem wyrwanym z całości procesu do, którego musi należeć.

W ramach działania informatyki, system informatyczny przestaje być prosty i jednolity, a często jego podziały są dla użytkowników nie widoczne, natomiast z punktu działania i funkcjonowania przedsiębiorstwa, administracji, gdzie należy dążyć do określenia pewnych kluczowych procesów, a najlepiej wszystkich najważniejszych, system taki powinien nieść ze sobą bezpieczeństwo i minimalizacje ryzyka związanego ze skutkami jego awarii.

mgr inż Marcin Kwiecień

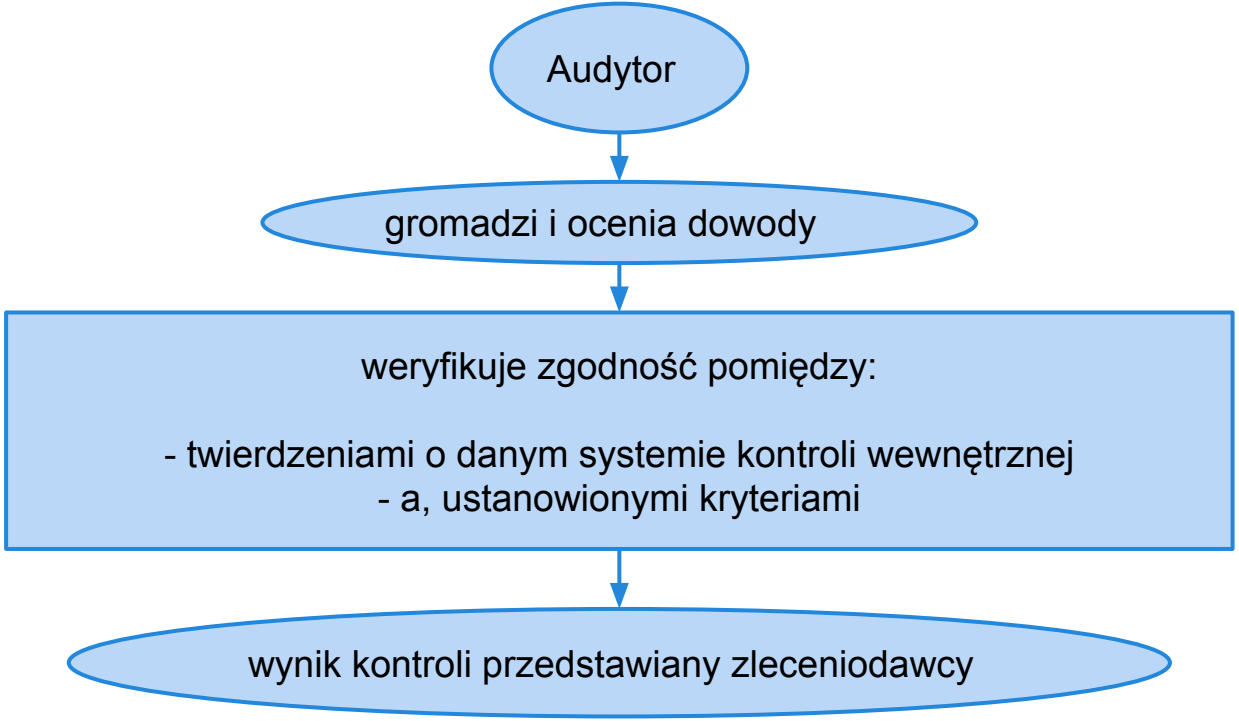
Informatyka w kontroli i audycie

System informatyczny

- komputery
- sieć teleinformatyczna
- serwer (bazy danych)
- strony www
- elementy peryferyjne (drukarki, skanery, czytniki kart, itd.)
- monitroing (kamery)
- elementy bezpieczeństwa budynków (systemy BMS, zarządzanie)

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie



Informatyka w kontroli i audycie

Systemy informatyczne mogą być róznego typu, jednak w ramach każdego z nich zakres określonych procedur musi być stosowany w odpowiedni sposób.

Inne systemy działają w górnictwie, kolejnictwie, w urzędzie gminy, ale część stosowanych procedur w tych systemach jest stała i można ją określić.

Do sprawdzenie poprawności działania takiego systemu należy przede wszystkim zatrudniać osoby kompetentne i doświadczone w ramach konkretnych branż które one reprezentują, w tym stosować odpowiednie dla danej branży standardy i narzędzia.

przykład: Informatyk programista nie może sprawdzać działania komputerów

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Do przyprowadzenia takiego audytu nalezy zasosować właściwą metodykę jego prowadzenia.

Metodyka prowadzenia audytu nie może być oderwana od elementów zarządzania bezpieczeństwem takiego systemu.

Powinna stać się jednym z jego procesów, przede wszystkim dla tego, że w tak dynamicznie rozwijającej się branży, jak informatyka, nie sposób przewidzieć i sprawdzić wszystkich jego elementyów.

Informatyk jest osobą której rozwój zawodowy musi podlegać specjalizacji i szkoleniu zawodowego w sposób ciągły, a audytowanie ma w dużej mierze **pomagać** także jemu w pracy.

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Definicje (wg. PN-I-02000:2002) :

Audyt bezpieczeństwa

dokonanie niezależnego przeglądu i oceny działania systemu w celi przetestowania adekwatności środków nadzoru systemu, upewnienie się, czy system działa zgodnie z ustalona polityką bezpieczeństwa i zgodnie z procedurami operacyjnymi oraz w celu wykrycia przełamań bezpieczeństwa i zalecenia wskazanych zmian w środkach nadzorowania, polityce bezpieczeństwa oraz w procedurach

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Definicje (wg. PN-I-02000:2002) :

Audyt systemu informatycznego

sprawdzanie procedur stosowanych w systemie przetwarzania danych w celu oceny ich skuteczności i poprawności oraz w celu zalecenie ulepszeń

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Kto jest odpowiedzialny za uporządkowanie systemów informatycznych w przedsiębiorstwach ?

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Należy to do zakresu obowiązków kadry kierowniczej oraz zarządu i obejmuje swym zakresem przywództwo, struktury organizacyjne praz procesy dzięki, którym działy informatyczne, informatyka może wspierać i rozwijać wspólne cele i strategie organizacji.

Czyli dokładnie tak jak powinna, ale z zastrzeżeniem, że procesy i dobór tych środków muszą być elementem konsultacji kadry kierowniczej i przez nie wspierane i zarządzane, dlatego, że są oni także częścią procesu tworzenia tego działu a przede wszystkim, porządku jaki w nim panuje.

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

PN-I-02000:2002

Administrator - osoba związana z przedmiotem oceny odpowiedzialna za utrzymywanie jego zdolności operacyjnej

Administrator bezpieczeństwa – użytkownik lub przyznana mu rola administrowania określonym systemem bezpieczeństwa w celu zapewnienia ciągłości prawidłowego działania przedmiotu oceny

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

PN-I-02000:2002

Bezpieczeństwo informacji – bezpieczeństwo polegające na zachowaniu poufności, integralności i dostępności informacji

Gestor danych – statutowy organ, osoba lub organizacja odpowiedzialna za szczególną kategorie informacji lub aktualne dane zawarte w informacji lub określone typy, do których należy sygnalizowanie użytkownikom i zarządzającym danymi potrzeby stosowania pewnych procedur obsługi danych, związanych z bezpieczeństwem

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

PN-I-02000:2002

Integralność systemu – właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcje w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej

Naruszenie bezpieczeństwa – przypadek, w którym użytkownik lub inna osoba pomija lub niszczy środki nadzoru systemu w celi pozyskania niuprawnionego dostępu do informacji w nim zawartej lub do jego zasobów

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

PN-I-02000:2002

Plan odtworzenia po awarii – plan obejmujący procedury składowani, działania doźne i odzyskiwanie po wystąpieniu poważnej awarii

Polityka bezpieczeństwa – plan lub sposób postępowania przyjęty w celi zapewnienia bezpieczeństwa systemu

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

PN-I-02000:2002

Ryzyko – prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów

Testy penetracyjne – sprawdzanie funkcji systemu przetwarzania danych w celu wyszukania sposobów obejścia bezpieczeństwa systemu Informatycznego

Zasoby – wszystko co ma wartość dla organizacji

mgr inż Marcin Kwiecień

Informatyka w kontroli i audycie

Elementy bezpieczeństwa

- zasoby
- zagrożenia
- podatność
- ryzyko
- zabezpieczenia

mgr inż Marcin Kwiecień