INSTYTUT BADAŃ SYSTEMOWYCH
POLSKIEJ AKADEMII NAUK

ANALIZA SYSTEMOWA W FINANSACH I ZARZĄDZANIU

Wybrane problemy
Tom 4

Pod redakcją
Jerzego HOŁUBCA

Warszawa 2002

INSTYTUT BADAŃ SYSTEMOWYCH
POLSKIEJ AKADEMII NAUK

ANALIZA SYSTEMOWA W FINANSACH I ZARZĄDZANIU

Wybrane problemy
Tom 4

Pod redakcją
Jerzego HOŁUBCA

Warszawa 2002

Wykaz opiniodawców artykułów zamieszczonych w tomie:

doc. dr hab. Mieczysław KŁOPOTEK

prof. dr hab. Stanisław PIASECKI

prof. dr Elżbieta RAKUS-ANDERSON

prof. dr hab. Andrzej STRASZAK

doc. dr hab. Sławomir WIERZCHOŃ

dr Sławomir ZADROŻNY

Publikacja dofinansowana przez
Agencję Wydawniczo-Poligraficzną "ARGRAF", Warszawa

ISBN 83-85847-74-X

Wydawca: INSTYTUT BADAŃ SYSTEMOWYCH PAN
ul. Newelska 6 01-447 Warszawa

Redakcja: Dział Informacji Naukowej i Wydawnictw
Barbara Kotuszewska, Joanna Runowska, tel. 837-68-22
Druk: Agencja Wydawniczo-Poligraficzna "ARGRAF", Warszawa
Nakład 200 egz., 15 ark.wyd.; 12,8 .ark. druk.

AUDYT SYSTEMÓW INFORMATYCZNYCH ZORIENTOWANY NA RYZYKO

Piotr Welenc
Zaoczne Studia Doktoranckie IBS PAN

Wiele lat dynamicznego wzrostu rynku nowych technologii spowodowało liczne zmiany w podejściu do tworzenia i funkcjonowania systemów informatycznych. Z powodu znaczącej wartości dodanej jaka uzyskano na bazie informacji dostarczanych przez zintegrowane systemy wspierające zarządzanie, coraz mocniej zwracano uwagę na czynniki które generowały te wartość. Były to jakość, bezpieczeństwo, integralność, dostępność itp. Lista takich czynników może być dłuższa, ponieważ trudno przecenić znaczenie systemów informatycznych dla funkcjonowania organizacji. Znalazło to odzwierciedlenie w stwierdzeniu o systemie informatycznym jako krwioobiegu organizacji. Dość wcześnie zaistniała potrzeba kontroli tworzenia, eksploatacji i zabezpieczenia tychże systemów w celu zapewnienie jeszcze wyższej jakości, wydajności, użyteczności itp. Stała analiza i kontrola funkcjonowania środowiska IT w organizacji z czasem nazwana została audytem informatycznym (IS Audit).

Keywords: Risk Management, Audit IS, Management of Organizations.

1. Wstęp

Do dzisiejszego dnia nie ma jednoznacznej definicji audytu IS. Definiowany jest np. „jako proces gromadzenia i oceny dowodów, czy systemy komputerowe gwarantują bezpieczeństwo, integralność, poufność danych i poprzez zarządzanie tymi elementami pozwalają osiąga cele organizacyjne przy optymalnym wykorzystaniu zasobów". (Weber)

Audyt systemów informatycznych jest stosunkowo młodą dziedzina. U podstaw zapotrzebowania na audyt systemów informatycznych leżało co najmniej kilka przyczyn. W pierwszym rzędzie były to tzw. potrzeby negatywne, które wynikły z braku dostatecznej kontroli jakości, wydajności

lub bezpieczeństwa tworzonego oprogramowania. Występowały także przyczyny pozytywne jakimi były: poprawa szybkości, niezawodności, lepsza integracja, stwierdzenie prawidłowości pracy samego oprogramowania, prawidłowości pracy użytkownika z oprogramowaniem.

Audyt informatyczny rozwinął się wraz z systemami wysokiej użyteczności materialnej oraz systemami o wysokiej dostępności. Występował w swojej pierwotnej postaci jako ocena prawidłowości, przy czym prawidłowość rozumiana była jako kontrola zgodności z założeniami wyrażanymi w dokumentach normatywnych, tworzonych przez kierowników jednostek. Audyt informatyczny w swej pierwotnej postaci wzorowany był na audycie finansowym. O znaczeniu audytu finansowego, wadze jego rzetelności i obiektywności przekonały się przedsiębiorstwa zainteresowane akcjami ENRON-u, i jego spektakularnego bankructwa w bieżącym roku.

Wraz ze wzrostem znaczenia systemów informatycznych w funkcjonowaniu przedsiębiorstw audyt informatyczny nabierał coraz większego znaczenia jako element komórek kontroli wewnętrznej. Gałęzie gospodarki które najwcześniej doceniły znaczenie audytu systemów informatycznych to duże instytucje finansowe, banki, sektor ubezpieczeń, telekomunikacji itp. Rozwój audytu systemów informatycznych był ściśle skorelowany z rozwojem w przedsiębiorstwach mechanizmów związanych z szeroko rozumianymi zagadnieniami kontroli wewnętrznej instytucjonalnej.

Audyt informatyczny był do niedawna rozumiany jako kontrola poprawności funkcjonowania mechanizmów jakości czy bezpieczeństwa, procedur dostępu, autoryzacji i wielu innych aspektów związanych z eksploatacja systemów oraz elektronicznym przetwarzaniem dokumentów (EDI). Samo pojecie było przedmiotem ciągłej ewolucji trwającej zresztą do dziś.

U podstaw podejścia do audytu systemów informatycznych leży sposób funkcjonowania organizacji w jakiej funkcjonuje system. Metody zarządzania, struktury i funkcjonowania samej organizacji determinują metodologię audytu systemów w niej funkcjonujących.

Obecnie możemy wyróżnić co najmniej dwa podejścia do audytu:

Pierwszy ukierunkowany na jakość kontroli. Standardami w tym podejściu są COSO, COCO, CADBURY, KING REPORT. Drugie podejście jest audytem ukierunkowanym na ryzyko. Standardem tutaj jest "rozszerzony COSO".

Obydwa zaprezentowane typy audytu są zupełnie odmiennymi kierunkami. W trakcie ewolucji samego pojęcia nastąpiło przesuniecie oczekiwań wobec audytu z funkcji kontrolnych w kierunku wspierania bieżącego zarządzania organizacją i związanego z tym nierozerwalnie zarządzania ryzykiem.

Pojecie audytu ewoluowało wraz z dojrzewaniem sposobów organizacji i zarządzania przedsiębiorstwami. Globalizacja i wszystkie jej następstwa postawiły organizacjom nowe wymagania którym nie sposób było sprostać bez zasadniczej zmiany filozofii zarządzania organizacją. Krytycznym elementem funkcjonowania dużych organizacji w kontekście zmian globalizacyjnych była ich mała mobilność, "bezwładność", hierarchiczny model przedsiębiorstwa wg. teorii Taylora, a przede wszystkim niski stopień informatyzacji.

Wraz ze wzrostem znaczenia nowych technologii i możliwości jakie dostarczyły one w zakresie globalnej komunikacji (internet), konieczna stała się weryfikacja podejścia do zarządzania organizacją. W przedsiębiorstwach z mniejszym lub większym skutkiem następuje transformacja w kierunku procesowego modelu zarządzania organizacją. Określa on organizację w kontekście współprzenikających się procesów, powiązanych ściśle określonymi zależnościami. Organizacja funkcjonuje jako system, a językiem jej opisu jest język analizy systemowej. Biorąc pod uwagę zanikanie barier geograficznych i informatyzację można zaobserwować ich ewolucję w kierunku organizacji wirtualnych.

Procesowa organizacja przedsiębiorstw jest modelem który z trudem przebija się przez stereotypy i prymitywne metody zarządzania. Większość organizacji nadal funkcjonuje wg. modelu Taylora, co powoduje nadmierne „obciążenie" i wysokie koszty funkcjonowania.

Model procesowy organizacji, mimo swoich niezaprzeczalnych atutów, niestety pozostaje w sferze możliwości nierealizowanych. W przedsiębiorstwach w których wprowadzono model procesowy, audyt w obecnej postaci jest głównie ukierunkowany na ryzyko. Ponieważ wynika on z procesowego modelu organizacji i zarządzania przedsiębiorstwem, jest w zasadniczej części optymalizatorem funkcjonowania i zarządzania organizacją.

2. Audyt systemów informatycznych

Głównymi czynnikami które są przedmiotem audytu informatycznego systemów są:

Dostępność,	Możliwość niezakłóconego korzystania z systemu. W skład tego pojęcia wchodzi nie tylko stabilność i komfort pracy z systemem, ale również kwestia zabezpieczeń fizycznych, hardware'owych, software'owych i orgware'owych
Poufność	Możliwość skorzystania z informacji zawartych w systemie wyłącznie przez osoby do tego upoważnione.
Integralność.	Możliwość otrzymania z systemu danych dokładnych, realistyczne i dostarczanych *just on time,* spójnych i wzajemnie niesprzecznych. Integralność zabezpiecza również przed nieautoryzowanymi modyfikacjami danych przez sam system

Tabela 1 Przedmiot audytu informatycznego (źródło własne)

Na audyt informatyczny składają się:

Typ	Opis
Audyt bezpieczeństwa fizycznego i środowiska	Dotyczy zabezpieczeń fizycznych, bezawaryjności zasilania, klimatyzacji, czynników środowiskowych
Audyt administracji systemem	Dotyczy bezpieczeństwa systemów operacyjnych, systemów zarządzania bazami danych, tworzeniem, rozwojem i administracji procedurami i zgodności z nimi (*compliance)*
Audyt aplikacji	Dotyczy aplikacji głównej i oprogramowania pomocniczego obsługujących wszystkie procesy wewnętrzne i zewnętrzne organizacji. Chodzi tu o aplikacje front i back office. Na audyt aplikacji składa się kontrola wewnętrznych mechanizmów ochrony, autoryzacji, dostępu, obsługi błędów, komplementarności tych procesów z zapisami procedur organizacyjnych, procesu zasilania w dane, przetwarzania i prezentacji wyników.
Audyt bezpieczeństwa sieci	Kontrola wszystkich połączeń zewnętrznych i wewnętrznych, parametrów bezpieczeństwa sieci, protokołów, tablic routingu, firewalli, scanning portów, wykrywanie włamań i naruszenia bezpieczeństwa w sieci
Audyt zapewnienia ciągłości procesów businessowych (*Business Continuity Planning*)	Kontrola mechanizmów zarządzania sytuacjami nietypowymi, mechanizmów zapewniających backup i redundancję, ochrony nośników zapasowych, procedur organizacji pracy systemu w sytuacji zagrożenia ciągłości procesu

Audyt integralność danych	Kontrola spójności danych, zabezpieczenia przed infiltracja systemu, modyfikacją, zagubieniem lub kradzieżą danych. Badanie adekwatności mechanizmów kontrolnych do istniejących procesów businessowych, budowa systemu powiadamiania o zaistniałych nieprawidłowościach, skutecznych mechanizmów zarządzania infrastrukturą techniczną organizacji.
Audyt projektu	Kontrola powstawania i cyklu życia rozwiązań software'owych. Kontrola poprawności założeń projektowych, doboru metodologii, prac projektowych, wdrożeń, testów wydajnościowych. Audyt cyklu życia produktu na etapie projektowania.

Tabela 2 Komponenty audytu infomatycznego (źródło własne)

3. Ryzyko

Najważniejszym z punktu widzenia audytu systemów informatycznych jest ryzyko operacyjne w organizacji. Jest to ryzyko wystąpienia straty na skutek nieadekwatności lub zawodności działania procesów wewnętrznych, ludzi i systemów, lub na skutek działania czynników zewnętrznych - taką definicję podaje Bazylejski Komitet Nadzoru Bankowego. Zarządzanie ryzykiem jest podstawowym narzędziem wspomagającym procesy ochrony informacji elektronicznej.

Zapotrzebowanie na zarządzanie ryzykiem spowodowane jest poprzez:

1. Coraz szybsze tempo zmian
2. Nowe struktury organizacyjne i procesy zarządzania
3. Naglośniane porażki
4. Redukcje, fuzje, przejęcia – szybka zmienność
5. Globalizacja
6. Zmieniające się oczekiwania grup interesu
7. Zadania organów ustawodawczych

Ryzyko jest czymś innym niż niepewność. Niepewności nie potrafimy określić. Jest nieszacowalna i niezarzadzalna. Ryzyko jest szacowalne, można je mierzyć, zarządzać nim, zabezpieczać, ubezpieczać, łączyć, dywersyfikować, transferować.

Każde działanie prowadzone przez instytucje jest narażone na ryzyko operacyjne, dlatego też nazywane jest ono ryzykiem fundamentalnym (z

uwzględnieniem charakterystyki dla danego działania i instytucji). Rośnie ono wraz ze złożonością procesów wewnątrzorganizacyjnych

Najczęściej występuje ono na skutek braku lub słabości nadzoru przez właścicieli procesów oraz błędnych mechanizmów kontroli lub ich braku.

W procesie zarządzania ryzykiem główną rolę odgrywa zarząd który jest pierwszym i nadrzędnym właścicielem całego ryzyka na jakie narażona jest organizacja.

Udział oraz akceptacja zarządu są także jednym z kluczowych wymagań sukcesu skutecznego wdrożenia polityki zarządzania ryzykiem, ponieważ zarząd ma wpływ na kształt misji instytucji oraz cele biznesowe i cele IT. Cele biznesowe i cele IT nie tyle przenikają się wzajemnie, ile cele IT podlegają celom businesowym. Wartość informacji systematycznie rośnie stad tez rośnie tez ryzyko związane z jej bezpieczeństwem i ochroną.

Rysunek 1. Rodzaje ryzyk w organizacji (Information System Control, 2001)

System identyfikacji i pomiaru ryzyka prowadzi do zdefiniowania miary ryzyka jako iloczynu prawdopodobieństwa wystąpienia zagrożenia i wartości zagrożonej. Wartość zagrożona (*Value at Risk*) może być traktowana zarówno jako strata, jak i zagrożenie zysku, koszt związany z zagrożeniem. Przeciwieństwem VaR jest EaR (*Earn at Risk*), którą można określić jako wartość przychodu przy ryzyku.

R=Lv*p

R - ryzyko
Lv –wartość potencjalnej straty *(loss value)*
p – prawdopodobieństwo

Problemem przed którym staja audytorzy jest jednostronność metodologiczna. Z jednej strony podchodzi się do ryzyka wyłącznie dedukcyjnie - zaniedbując wiedzę wynikającą z obserwacji empirycznych, z drugiej strony wyłącznie redukcyjnie a wiec hipersubiektywnie. Zarządzanie ryzykiem w obszarze audytu systemów informatycznych podlega nie tylko metodom analizy ilościowej np. wyliczania VaR ale tez analiz jakościowych, których podstawą stają się w znacznej mierze analizy metodologii i procesów.

Prawda jest ze matematycznie mierząc elementy opisujące ryzyko (*risk factors*) otrzymujemy dane intersubiektywnie porównywalne. Analiza systemowa pokazuje, że ryzyko trzeba nie tylko matematycznie mierzyć, ale także jakościowo analizować. W wymiarze metody redukcyjnej ryzyko jawi na się jako wiele subiektywnych ocen, przypuszczeń, sugestii, przemyśleń i przewidywań. Zarządzanie ryzykiem to także system ocen, schematów reagowania, ocena adekwatności mechanizmów kontroli. Można wiec zaryzykować stwierdzenie ryzyko jest też kategorią psychologiczną i komplementarne funkcjonowanie dedukcyjnej i redukcyjnej metodologii analizy ryzyka przyniesie efekty optymalne. Docelowym językiem raportowania o ryzyku wydaje się być XBRL (eXtensible Bussines Report Language).

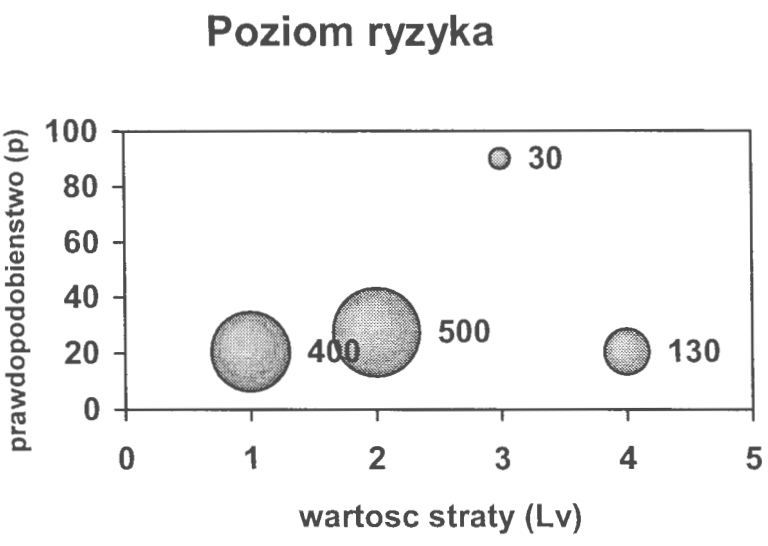
Zarządzanie ryzykiem opiera się na wiedzy o nim. Wiedza ta pozwala podjąć decyzje co do dalszych działań. Działania te można podzielić na trzy podstawowe kategorie:

- Akceptacja
- Minimalizacja
- Transfer

W pierwszym przypadku instytucja zdaje sobie sprawę z możliwości wystąpienia ryzyka, jednak koszty jego minimalizacji są zbyt duże w porównaniu z potencjalnymi zyskami.

W drugim przypadku ryzyko jest na tyle istotne, że instytucja podejmuje działania, które minimalizują szansę zaistnienia zdarzenia oraz potencjalne straty na skutek jego wystąpienia. Koszt tych działań nie przewyższa zysków. Należy jednak pamiętać, że istnieje grupa zagrożeń,

których nie można całkowicie wykluczyć. Dlatego stosowany jest termin minimalizacja, a nie likwidacja ryzyka.



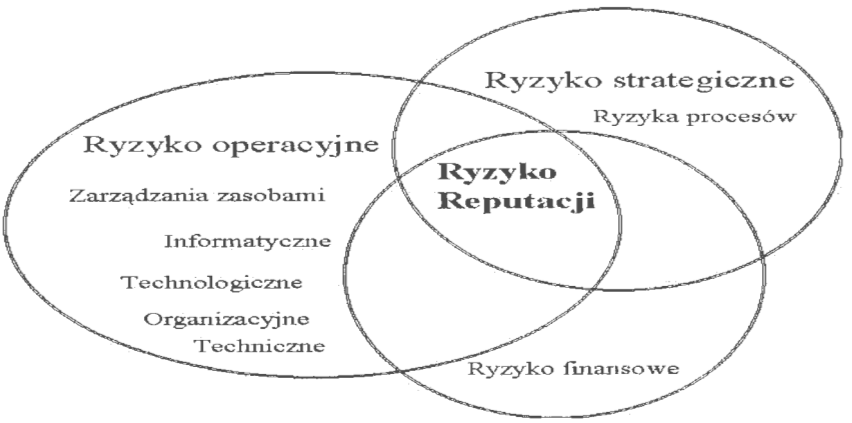
Wykres 1 Określenie poziomu ryzka (źródło własne)

W niektórych przypadkach dysponujemy możliwością transferu, czyli przeniesienia ryzyka. Dzieje się tak na przykład w przypadku wykupienia ubezpieczenia. W rzeczywistości jednak instytucja nie chroni się przed ryzykiem, ma tylko zapewnioną pewną (finansową) rekompensatę w przypadku wystąpienia zdarzenia.

Etapy zarządzania ryzykiem to:

- Zrozumienie funkcjonowania organizacji, celów strategicznych i operacyjnych
- Kategoryzacja ryzyka (słownik ryzyka)
- Definicja i kategoryzacja procesów w organizacji
- Określenie czynników ryzyka (risk factors) wbudowanego w procesy (inherent risk) oraz stopnia ich istotności na cykl życia procesu - ryzyka rezydualne.
- Gromadzenie danych dotyczących wysokości potencjalnej straty spowodowanej zaburzeniem lub zatrzymaniem procesu
- Określenie prawdopodobieństwa wystąpienia zaburzenia lub zatrzymaniem procesu

- Konstrukcja zagregowanej mapa ryzyka dla organizacji jako wynik audytu



Rysunek 2 Klasyfikacja ryzyka (źródło własne)

Dla każdego z wymienionych elementów można odnaleźć analogiczny odpowiednik w audycie systemów informatycznych. Posługujemy się wtedy w audycie informatycznym słownikiem ryzyka. Język ryzyka w przeciwieństwie do języka analizy systemowej jest bliższy managerom średniego i wyższego szczebla, stad tez audytor staje się zrozumiały w wydawaniu opinii i formułowaniu wniosków.

4 Korelaty audytu systemów informatycznych i elementów zarządzania ryzykiem

Odpowiednikami dla analizy ryzyka w audycie informatycznym ukierunkowanym na ryzyko są:

Zarządzanie ryzykiem	Działania w obszarze IT
Zrozumienie funkcjonowania organizacji, celów strategicznych i operacyjnych	Inwentaryzacja systemów informatycznych używanych w organizacja i ich kategoryzacja
Wyodrębnienie procesów i kategoryzacja ryzyk na jakie są narażone	Określenie które z nich zawierają funkcje krytyczne dla działalności organizacji.
Określenie czynników ryzyka (risk factors) wbudowanego w procesy (inherent risk) oraz stopnia ich istotności na cykl życia procesu - ryzyko rezydualne.	Określenie kategorii ryzyk i zagrożeń i oszacowanie istotności w sferze zasobów materiałowych, technicznych ludzkich, kapitałowych, podejmowania decyzji.

Gromadzenie danych dotyczących wysokości potencjalnej straty spowodowanej zaburzeniem lub zatrzymaniem procesu	Określenie w jakim realnym czasie opisane ryzyka mogą zagrozić funkcjonowaniu organizacji, wielkości strat materialnych i niematerialnych. Określenie metod obrony przed nimi (*Business Continuity Plannig*)
Określenie prawdopodobieństwa wystąpienia zaburzenia lub zatrzymaniem procesu	Określenie prawdopodobieństwa wystąpienia zaburzenia funkcjonowania poszczególnych elementów infrastruktury, potencjalnej częstotliwosci występowania zaburzeń.
Zagregowana mapa ryzyka dla organizacji w zakresie IT	Stworzenie wielowymiarowych rankingów systemów IT pozwalających na stałą ich kategoryzacje pod względem wrażliwości na ryzyko. Ustalenie priorytetów wykonywania audytu. Zmniejszenie wrażliwości systemów na ryzyko. Określenie możliwości wytransferowania ryzyka poza system. Stworzenie i analiza mapy ryzyka dla systemów IT

U podstaw modelu audytu zorientowanego na zarządzanie ryzykiem leży głęboka znajomość procesów, zrozumienie celów strategicznych i operacyjnych organizacji. Ryzyko zakłóca proces osiągania celów stad tez dopiero w kontekście pełnego zrozumienia zasad, celów, struktur, procesów organizacji, a zwłaszcza współzależności miedzy nimi, można mówić o zarządzaniu ryzykiem. Można założyć, ze istnieje istotna dodatnia korelacja ryzyka operacyjnego z ryzykiem strategicznym i finansowym organizacji.

Cecha współczesnego produktu finansowego jest wartość oparta na wycenie ryzyka w czasie, podczas gdy w modelu doskonalej konkurencji dobro jest dostarczane w czasie rzeczywistym, a decyzje uczestników mogą być podejmowane bez uwzględniania ryzyka. Ryzyko musimy uwzględniać wszędzie tam, gdzie aktywność (np. zaopatrzenie, transmisja, płatność) nie następuje natychmiast. Ryzyko zwiększa się wraz ze zwiększeniem interwału czasowego. Dotyczy to ryzyka straty jak i nieosiagniecia przychodu („nie wejście do gry").

Potrzeby w zakresie audytu informatycznego zorientowanego na ryzyko wzrastają w miarę nasilenia rożnych czynników. Zaliczamy do niej wielkość organizacji, ilość używanego sprzętu i oprogramowania, stopień jego złożoności, integracji, stopnia wspierania procesów businessowych. W podejściu do audytu zorientowanym na ryzyko uproszczeniu ulega

częstotliwość kontroli. Można precyzyjniej określić umiejscowienie kontroli, natomiast jakość kontroli pozostaje zawsze taka sama. Dane wyjściowe audytu służą do zasilania mapy ryzyka organizacji. Analiza mapy ryzyka stanowi centralne miejsce w zarządzaniu ryzykiem całej organizacji.

Audytor kontroluje jak inni zarządzają ryzykiem - nie zarządza jednak sam ryzykiem strategicznym. Ryzykiem strategicznym zawsze zarządza właściciel procesu. Audytor zaś zarządza ryzykiem operacyjnym poprzez dokonywanie kontroli w obszarach najbardziej narażonych na ryzyko. Określa czynnik ryzyk operacyjnych i ich wpływ na wzrost zagrożenia realizacji celów strategicznych.

Pewne ryzyka są krytyczne dla organizacji - niektóre zaś nie. W systemach billingowych minuty przestoju generują straty rzędu milionów dolarów, stad tez ryzyko przestoju jest wysoko znaczące. To samo ryzyko dla systemu zarządzania łańcuchami dostaw będzie znikome. Ryzyko zawsze należy widzieć w kontekście procesu, ponieważ proces ma wbudowane faktory ryzyka. Dopóki są kontrolowane (zarzadzalne) istnieje możliwość kontroli cyklu życia procesu. W przeciwnym razie proces zaczyna być izolowany od życia organizacji.

Ze względu na postępującą informatyzację procesów businessowych audyt informatyczny staje się coraz istotniejszym elementem zainteresowania wyższej kadry zarządzającej.

Z dużą dozą prawdopodobieństwa można założyć ze w nieodległej przyszłości będzie odgrywać jeszcze większą rolę w bezpośrednim zarządzaniu organizacją.

Literatura

COSO Committee of Sponsoring Organisations of the Treadway Commission. Internal Control - Integrated Framework. 2 Vols. American Institute of Certified Accountants, New Jersey, 1994.(Cadbury in the U.K., CoCo in Canada, King Report in South Africa

COBIT 3rd Edition (*Control Objectives for Information and related Technology*), IT Governance Institute, 2000

Bhatia, Mohan, *Auditing in a Computerised Envinronment,* McGraw Hill, *2001*

Andrzej Blikle, *Procesowa Organizacja Przedsiębiorstwa*, Międzynarodowa Szkoła Jakości, III sesja – W drodze do Unii Europejskiej, Szczyrk 17-18 maja 2001

CICA *Computer Control Guidelines: Canadian Institute of Chartered Accountants*, Toronto, 1986.

Computerised Information Systems (CIS) Audit Manual: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Rolling Meadows, IL, 1992.

Weber R., EDP – *Auditing – Conceptual Foundations and Practice.* IS Control Journal vol.1/2001

Weber R. *Information Systems Control and Audit* ISACA Bookstore.

McName D., Pleier J.R. Tongren J.D., *Risk Management: Best Practicies, Case studies and related materials.* ISACA Bookstore.

Risk Management – http://www.irmi.com

Information Systems Control Journal 1/2002

Międzynarodowe Stowarzyszenie Audytorów Systemów Informatycznych – http://www.isaca.org

NSW Gowernment, *Information Management of Technology. Risk Management Guideline* Office of IT 1998.

ISBN 83-85847-74-X