PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1073 2005
Dostosowanie rachunkowości i rewizji finansowej do dyrektyw Unii Europejskiej

Marianna Kowalska, Marcin Kowalski

AUDYT SYSTEMU INFORMATYCZNEGO RACHUNKOWOŚCI

1. Pojęcie audytu i przesłanki jego stosowania

W literaturze przedmiotu nie została w sposób jednoznaczny sprecyzowana definicja audytu systemów informatycznych (w opracowaniu używa się zamiennie pojęć: „system informacyjny" i „system informatyczny"). Jedni autorzy uważają, że audyt jest przeglądem istniejącej kontroli i wykrywania bezprawnych działań [3], z kolei inni traktują audyt jako ocenę niezależną i obiektywną tych czynników, które wpływają na wiarygodność i rzetelność systemów informacyjnych [4]. Ocena ta nie ogranicza się jednak tylko do samych systemów, jej elementami bowiem według [3] są też:

- procedury operacyjne, opierające się na wykorzystaniu systemów,
- zasady wdrożenia, eksploatacji i rozwoju systemów,
- sposób organizacji pracy służb informatycznych i dostawców [3].

Audyt zajmuje się przede wszystkim badaniem, oceną sprawności i skuteczności systemu kontroli wewnętrznej różnych procesów występujących w firmie. Celem tego działania jest usprawnienie funkcjonowania firmy.

Jak wynika z wybranych przykładowo definicji, audyt może być rozmaicie definiowany i w różnym stopniu odnoszony do zróżnicowanego zakresu przedmiotowego działań. Audyt informatyczny może być traktowany jako samodzielne przedsięwzięcie lub jako element pomocniczy projektu związanego z badaniem sprawozdania finansowego.

W przypadku gdy audyt informatyczny jest samodzielnym przedsięwzięciem, obejmuje on szeroki zakres – od oceny zarządzania bezpieczeństwem systemu autonomicznego do oceny zarządzania bezpieczeństwem systemów informatycznych w skali całej firmy.

W zasięgu tego audytu do zasobów badanych należą w szczególności: dane,

oprogramowanie, procedury, technika informatyczna, personel działu informatyki oraz pozostała dokumentacja. Po zdefiniowaniu pojęcia audytu przedstawia się jego zadania.

Zadania audytu systemów informatycznych zarządzania, a więc także systemów informatycznych rachunkowości (SIR), można ująć w cztery następujące grupy:

1. Weryfikacja zgodności systemów z wymogami prawa, pozwalająca na uzyskanie niezależnej oceny odnośnie do kryteriów określonych w przepisach prawa.
2. Weryfikacja stanu bezpieczeństwa systemu, pozwalająca na uzyskanie niezależnej oceny stopnia zabezpieczenia przed zewnętrznymi i wewnętrznymi zagrożeniami systemu.
3. Weryfikacja stanu zasobów systemów informacyjnych, pozwalająca na uzyskanie wyczerpujących i aktualnych informacji o zainstalowanym oprogramowaniu, posiadanych licencjach, zasobach danych oraz środkach technicznych.
4. Weryfikacja stanu zasobów sieciowych, pozwalająca na uzyskanie niezależnej oceny prawidłowości funkcjonowania sieci, połączeń sieciowych oraz stanu bezpieczeństwa sieci. Zadanie to występuje jedynie wtedy, kiedy system informatyczny jest zorganizowany jako sieciowy lokalny bądź sieciowy rozległy [5].

2. Unormowania prawne w zakresie audytu

W Polsce obecnie są prowadzone liczne prace, których celem jest opracowanie jednoznacznych przepisów nakładających obowiązek prowadzenia audytu systemów informacyjnych, w tym także systemów sieciowych. Do tych przepisów należą m.in.:

- Ustawa z dnia 29 września 1994 r. o rachunkowości (DzU 2002 nr 86 – tekst jednolity). Ustawa ta nakłada obowiązek wydawania opinii przez biegłego rewidenta o audytowanym sprawozdaniu finansowym, a więc także o księgach rachunkowych,
- Ustawa z dnia 27 lipca 2001 o zmianie Ustawy o finansach publicznych (DzU 2002 nr 77),
- Ustawa o biegłych rewidentach i ich samorządzie (DzU 2001 nr 31).
- „Międzynarodowe standardy rewizji finansowej" [6, s. 25].

Ustawa o rachunkowości określa m.in. wymogi, którym powinny sprostać „księgi rachunkowe prowadzone za pomocą komputera". Ze względu na to, iż księgi rachunkowe stanowią podstawę sporządzania sprawozdania finansowego, audytor (biegły rewident), aby wydać opinię o sporządzonym sprawozdaniu finansowym, musi ocenić prawidłowość działania systemów informatycznych rachunkowości (SIR). Prace związane z przeglądem środowiska informatycznego stają się integralną częścią badania sprawozdania finansowego. Audytor sprawozdań finansowych powinien określić swój poziom zaufania do procesów przetwarzania danych w badanej organizacji. W tym celu może wykorzystać specjalne procedury,

takie jak: test na istnienie, ustalenie ryzyka ogólnego, ryzyka kontroli czy ryzyka przeoczenia.

O audycie systemu informacyjnego mówią m.in. rekomendacje GINB, ale dotyczą one jedynie sektora bankowego i nie mają charakteru obligatoryjnego.

Warto zaznaczyć, iż nie należy łączyć wymagań określanych w innych aktach prawnych, np. w zakresie ustaw odnoszących się do bezpieczeństwa, poufności informacji, przestępstw komputerowych z wymogiem przeprowadzania audytu. Zapewnienie bezpieczeństwa to nie to samo co przeprowadzenie audytu bezpieczeństwa. Przeprowadzenie audytu bezpieczeństwa systemu informatycznego jest doskonałym narzędziem weryfikującym poziom bezpieczeństwa tych systemów [2].

W polskich aktach prawnych, tj. w Ustawie o rachunkowości i Ustawie o biegłych rewidentach, znajdują się przede wszystkim odwołania do roli biegłego rewidenta, tj. zewnętrznego audytora. W ustawie o finansach publicznych zawarte są odwołania do roli audytora wewnętrznego w jednostkach samorządowych oraz w bankach.

Nowelizacja ustawy o finansach publicznych wprowadziła do sektora finansów publicznych audyt wewnętrzny jako element systemu zarządzania. Szczegółowy sposób i tryb prowadzenia audytu wewnętrznego określa Rozporządzenie Ministra Finansów z dnia 5 lipca 2002 r. (DzU nr 111, poz. 973), wydane na podstawie art. 35j ust. 1 Ustawy o finansach publicznych.

Audytem wewnętrznym jest ogół działań, przez które kierownik jednostki uzyskuje obiektywną i niezależną ocenę funkcjonowania jednostki w zakresie gospodarki finansowej pod względem legalności, gospodarności, celowości, rzetelności, a także przejrzystości i jawności. Jeśli jednostka wykorzystuje w swojej działalności system informatyczny, to audytor powinien sprawdzić jego działanie.

Jak wynika z powyższych rozważań, o audycie samych systemów informatycznych mówi się niewiele. Jest on zazwyczaj przeprowadzany w razie nieprawidłowego funkcjonowania systemu lub sporu z dostawcą rozwiązań informatycznych. Taka sytuacja oznacza jednak, że firma poniosła już niekontrolowane straty, czyli nie zabezpieczyła się właściwie przed ryzykiem informatycznym.

Przedsiębiorstwa, w których od sprawności funkcjonowania informatyki zależy efektywne prowadzenie biznesu, powinny zlecać przeprowadzenie audytu jednostkom, które posiadają specjalne certyfikaty w tym zakresie. Jednym z takich jest Międzynarodowe Stowarzyszenie ds. Audytu i Kontroli Systemów Informatycznych (ISACA). Stowarzyszenie to opracowało metodykę prowadzenia kontroli środowiska informatycznego, zgodnie z którą powinny być prowadzone prace audytorskie. Zlecając przeprowadzenie usługi takiemu audytorowi, firma ma pewność prawidłowości przeprowadzenia audytu.

W Polsce tego typu certyfikat posiada tylko ok. 40 osób, w związku z czym z ich usług mogą korzystać jedynie zamożne firmy. Pozostałe zaś mogą zlecać wykonanie usługi innym specjalizowanym firmom doradczym lub wiarygodnym firmom informatycznym.

3. Udokumentowanie audytu

Audytor w czasie prowadzenia audytu gromadzi informacje, które pozwalają mu uzyskać wiarygodne dowody.

Dowody te mogą obejmować [10]:

- dokumentację dotyczącą funkcjonowania systemu rachunkowości w przedsiębiorstwie,
- dokumenty prezentujące technologię przetwarzania systemu informatycznego rachunkowości,
- analizy porównawcze.

W zakresie funkcjonowania systemu informatycznego rachunkowości w przedsiębiorstwie audytor może zebrać dokumentację obejmującą :

- spis nośników i miejsc ich przechowywania,
- opis zabezpieczeń pomieszczeń, dostępu do zasobów i procesów przetwarzania danych,
- opis działania systemu w warunkach awarii i możliwości jego odtworzenia.

Dokumentacja związana z realizacją technologii systemu informatycznego rachunkowości może dotyczyć:

- zapisów transakcji,
- procedur przetwarzania,
- listingów programów,
- dokumentacji określającej tryb pracy systemu,
- dokumentacji przepływu danych aplikacji w ramach sieci (ze szczególnym uwzględnieniem metod ochrony tych danych oraz miejsc styku z siecią zewnętrzną),
- dokumentacji rozwoju systemu.

Analizy porównawcze również mogą stanowić dowody audytu. Przykładowo mogą one obejmować:

- badania porównawcze wydajności aplikacji w stosunku do innych organizacji lub okresów,
- porównanie wskaźników błędów pomiędzy aplikacjami, transakcjami i użytkownikami.

Audytor powinien posługiwać się najnowszymi technikami badania, zebrać wiarygodne dowody oraz wychwycić wszystkie nieprawidłowości w funkcjonowaniu systemu informacyjnego.

Dowody audytu zebrane przez audytora powinny być odpowiednio udokumentowane i zorganizowane. Każdy z tych dowodów powinien być prawidłowo opisany przez audytora i zawierać przynajmniej takie dane, jak (podobne wymogi stawiane są przed dokumentami roboczymi zebranymi przez biegłych rewidentów w czasie badania sprawozdań finansowych):

- nazwa jednostki, w której przeprowadzany jest audyt,
- dane identyfikujące twórców systemu,

- opis, charakterystyka elementu będącego przedmiotem audytu,
- data i podpis audytora.

Dowody te audytor gromadzi w dokumentacji rewizyjnej. Dokumentacja ta jest odpowiednio opisywana przez audytora i przechowywana przez niego lub w firmie, na zlecenie której był prowadzony audyt systemu informatycznego. Okres przechowywania dokumentacji rewizyjnej wynosi – tak jak pozostałych dokumentów – 5 lat. Dokumentacja ta może zawierać np.:

- opis przez audytora systemu informacyjnego obszaru i środowiska poddanego kontroli,
- dowody modyfikacji systemu,
- opis algorytmów przetwarzania informacji,
- opis procedur zarządzania siecią i jej zasobami (zasad zarządzania),
- odpowiedzi i wyjaśnienia osób kontrolowanych na rekomendacje audytorskie.

Po zebraniu dokumentacji rewizyjnej i ukończeniu audytu audytor powinien opracować w formie pisemnej odpowiednią dokumentację, zwaną raportem z przeprowadzonego badania. Dokumentacja ta zawiera stanowi zapis przeprowadzonej przez audytora pracy oraz jego wnioski. Obecnie nie ma jednoznacznego standardu, który by określał zawartość raportu dotyczącego systemu informatycznego funkcjonującego w przedsiębiorstwie. Niektóre wytyczne co do treści raportu są zawarte w normach wykonywania zawodu biegłego rewidenta oraz we wskazówkach zawartych w sprawie sporządzania raportu [7; 9].

W raporcie sporządzonym przez audytora z przeprowadzonego audytu informatycznego systemu rachunkowości powinny się znaleźć m.in. takie informacje, jak:

- charakterystyka systemu informatycznego,
- przedstawienie zakresu systemu, w którym audytor zastosował standardy audytu,
- ocena przez audytora programu zabezpieczenia jakości, dotycząca funkcjonowania systemu informacyjnego,
- ocena zbiorów danych, prawidłowości ich zabezpieczania oraz archiwowania,
- ocena wyposażenia informatycznego systemu sieciowego,

Warto zaznaczyć, że zakres dokumentacji rewizyjnej zgromadzonej przez audytora, a następnie opracowanie raportu zależą od potrzeb określonego audytu, czyli od zleceniodawcy, na rzecz którego przeprowadzany jest audyt. Jeśli audyt systemu informatycznego rachunkowości przeprowadzany jest w ramach badania sprawozdania finansowego, to dokumentacja rewizyjna z tego audytu musi być zgodna z zakresem rzeczowym dokumentacji dotyczącej badania sprawozdania finansowego.

Zakres rzeczowy dokumentacji rewizyjnej określają [6, s. 9]:

- art. 65 ust. 6 Ustawy z dnia 29 września 1994 r. o rachunkowości,
- norma nr 1, rozdz. V „Planowanie badania" i rozdz. XII „Dokumentacja rewizyjna",
- norma nr 5, rozdz. VI „Dokumentacja rewizyjna i jej archiwowanie",
- „Międzynarodowe standardy rewizji finansowej" nr 230 „Dokumentacja".

Dokumentacja z audytu pozostałych systemów informatycznych powinna zawierać informacje kontrolne wymagane przez prawo, regulacje rządowe lub stosowane standardy jakości. Zakłada się, że będzie ona czytelna, kompletna i zrozumiała dla korzystających z niej osób. Należy ją przechowywać, podobnie jak pozostałą dokumentację, zgodnie z przepisami prawa.

4. Podsumowanie

Celem artykułu było przedstawienie ogólnych ram projektu dotyczącego realizacji procesu audytu systemu informatycznego rachunkowości w firmie. Audyt jako forma kontroli jest jednym z elementów zarządzania ryzykiem gospodarczym. Może być realizowany jako odrębne przedsięwzięcie lub zostać wykonany w ramach audytu sprawozdań finansowych. W przypadku gdy jest realizowany w ramach audytu sprawozdań finansowych przez biegłych rewidentów, należy go przeprowadzić zgodnie z wymogami dotyczącymi audytu sprawozdań finansowych. Powinien on dać odpowiedź m.in. na pytania dotyczące zagrożeń systemu, częstotliwości występowania tych zagrożeń, wpływu zagrożeń na zbiory danych. Dodatkowo powinien udzielić odpowiedzi na pytanie, czy wykorzystywane w firmie systemy są wiarygodne, rzetelne i bezpieczne.

Usługa audytu systemu informatycznego, w tym także sieciowego, nie jest jeszcze zbyt popularna w Polsce; na ogół jest stosowana wówczas, gdy użytkownik stwierdzi nieprawidłowości w funkcjonowaniu systemu i chce uzyskać opinię eksperta o nieprawidłowościach działania systemu.

Wiele firm (głównie spółek publicznych lub przedsiębiorstw z kapitałem zagranicznym) nawiązuje długofalową współpracę także z firmami audytorskimi, które badając ich sprawozdania, oceniają również stan infrastruktury systemów informatycznych. Ze względu na to, że wyposażenie techniczne systemu jest jedną z podstaw funkcjonowania współczesnej firmy, audyt systemu informatycznego stanowi istotną część badania sprawności tej firmy.

Specyfika systemu informatycznego powoduje, że prowadzenie audytu systemu informatycznego wymaga istnienia jasno określonych standardów (procedur). Procedury te są określane m.in. przez Międzynarodowe Stowarzyszenie ds. Audytu i Kontroli Systemów Informatycznych – ISACA [10]. Organizacja ta jest największą, najważniejszą, a przy tym niezależną organizacją zajmującą się problemami audytu, kontroli i zarządzania w środowisku informatycznym. W ISACA, mającym prawie 200 oddziałów na całym świecie, zrzeszonych jest ponad 35 000 osób.

Stowarzyszenie to dość szczegółowo reguluje kwestie organizacji i przebiegu procesu audytowania systemów informatycznych.

Najbardziej znane produkty ISACA to:

- COBIT – standard zarządzania i kontroli SI. Jest on podstawowym zbiorem standardów i wytycznych dla audytorów. Jest to również metodologia, która konsoliduje i harmonizuje ogólne wytyczne w zakresie audytu,

- CONeCT – standard audytu środowiska sieciowego.

Coraz większego znaczenia nabiera też certyfikat CISA (*certified information systems audito*), który jest jedynym, globalnym i powszechnie uznawanym programem certyfikacji audytorów systemów informacyjnych. Uzyskanie przez audytorów certyfikatu CISA nie jest warunkiem prowadzenia audytu, tylko wiarygodnym potwierdzeniem posiadanej wiedzy.

Literatura

[1] Aforystek M., *Cobit dla (nie) opornych audytorów – ogólna procedura audytu*, Warszawa 2003.

[2] Bojanowski J., *Systemy informatyczne z perspektywy audytora – bariera czy wezwanie*, „Monitor" 2001 nr 3.

[3] Bojanowski J., *Wykorzystanie standardów audytu informatycznego ISACA na przykładzie audytu sieci*, Warszawa 2003.

[4] Kisielnicki J., Sroka H., *Systemy informacyjne biznesu*, Warszawa 1999.

[5] Korytowski J., *Podstawy audytu aplikacji*, www.isaca.org.pl

[6] Kurzawski R., Mierzejewski S., *Dokumentacja rewizyjna badania sprawozdania finansowego*, SKwP, Warszawa 2004.

[7] *Normy wykonywania zawodu biegłego rewidenta*, Biuletyn KIBR nr 53, Warszawa 2002.

[8] Piattini M., *Audyting Information Systems*, Wyd. Idea Group Publishing, Herschey 2000.

[9] *Wskazówki w sprawie sporządzania opinii, raportu i udziału biegłego rewidenta w inwentaryzacji*, Biuletyn KIBR nr 57, Warszawa 2002.

[10] *Wytyczna audytowania systemów informatycznych. Forma i zawartość raportów*, www.isaca.org.pl

AUDIT OF ACCOUNTING INFORMATION SYSTEM

Summary

In the paper some chosen problems from the range of audits of accounting information systems has been presented. Having the core business of the information system illustrated, the authors focus on the legal requirements concerning the audit. An appropriate documentation is a very significant element of performing such an audit. The auditor's documentation has been deeply described in the publication.

Dr Marianna Kowalska jest starszym wykładowcą w Katedrze Informatyki Ekonomicznej Akademii Ekonomicznej we Wrocławiu.

Mgr Marcin Kowalski jest doktorantem w Katedrze Zarządzania Procesami Gospodarczymi Akademii Ekonomicznej we Wrocławiu.