Zeszyty Naukowe Uniwersytet Ekonomiczny w Krakowie
Finanse

913

ISSN 1898-6447
Zesz. Nauk. UEK, 2013; 913: 5–20

Ewa Wiktoria Babuśka
Katedra Rachunkowości Finansowej
Uniwersytet Ekonomiczny w Krakowie

Kontrola wewnętrzna w środowisku informatycznym według modelu COSO

1. Wprowadzenie

Kontrola wewnętrzna jest jednym z powszechnie uznanych narzędzi pomagających przedsiębiorstwom utrzymać się na rynku i kontynuować działalność w warunkach zaostrzającej się konkurencji. Wzrastająca konkurencja jest m.in. wynikiem szybkiego rozwoju cyfrowej technologii przepływu informacji i standaryzacji technicznej w skali ogólnoświatowej, które w dążeniu do dostarczania informacji w czasie rzeczywistym radykalnie zmieniają sposoby komunikacji i działalności przedsiębiorstw.

Prezentacja kontroli wewnętrznej w środowisku informatycznym musi nawiązywać do znanych modeli tej kontroli, takich jak np. opracowany w USA model COSO, który odegrał dominującą rolę w zidentyfikowaniu i opisaniu pięciu elementów struktury kontroli wewnętrznej[1]. Komponenty tego modelu przyjęte zostały w standardach kontroli wewnętrznej Generalnego Biura Rachunkowości Kongresu Amerykańskiego (*General Accounting Office* – GAO), w których wymienia się pięć powiązanych, głównych elementów kontroli wewnętrznej

[1] Komponenty te, obejmujące środowisko kontroli, oszacowanie ryzyka, działania kontrolne, informację i jej przekazywanie, monitorowanie, przedstawiono w publikacji zamieszczonej w Zeszytach Naukowych Uniwersytetu Ekonomicznego w Krakowie, nr 883, Kraków 2012, tytuł artykułu: *Model kontroli wewnętrznej COSO*, s. 5–18, wraz z czynnikami kształtującymi i opisującymi każdy z nich z osobna.

tworzących jej strukturę, a wywodzących się ze sposobu, w jaki zarząd kieruje przedsiębiorstwem. Będą one rozważane ze względu na technologię informacji (IT)[2]. Elementy modelu COSO stanowią podstawę oceny skuteczności i wydajności każdego systemu kontroli wewnętrznej. Współdziałają one ze sobą dla osiągnięcia ustanowionych celów jednostki. Celem artykułu jest ukazanie aspektów IT w modelu COSO oraz podkreślenie znaczenia kontroli informatycznych w systemach kontroli wewnętrznej współczesnych przedsiębiorstw, w których coraz więcej kontroli przejmowanych jest przez urządzenia techniczne.

2. Elementy kontroli wewnętrznej w modelu COSO z wykorzystaniem IT

Tabela 1 zawiera zbiorcze zestawienie podstawowych elementów tworzących ramy kontroli wewnętrznej w modelu COSO, z opisem ich charakterystycznych cech oraz głównych czynników odnoszących się do poszczególnych komponentów, w tym też ważnych czynników dotyczących IT. Rozważając wpływ IT na elementy i procedury kontroli wewnętrznej, należy stwierdzić, że wprowadzenie systemów informacji (*information systems* – IS) pociąga za sobą poważne skutki dla jej funkcjonowania.

Kontrole IT mają wspierać osiąganie celów jednostki, przeciwdziałać oszustwom, błędom i zagrożeniom rozumianym jako okoliczności i zdarzenia mogące przynieść jednostce szkody. Aby zadanie to było wykonalne, zarząd ustala wiele zasad i procedur kontroli przewidzianych do realizacji ręcznej przez personel obsługujący system IT lub z nim współpracujący, bądź użytkowników systemu, albo do realizacji automatycznej spełnianej samoczynnie przez aplikacyjne oprogramowanie komputera. Na tradycyjne (ręczne) i automatyczne (komputerowe) procedury kontroli składają się kontrole ogólne, obejmujące nadzór nad stosowaniem technologii informacji i warunkujące poprawne działanie systemu informacyjnego jako całości oraz kontrole zastosowania, tj. szczegółowe kontrole programów w systemach informacji i procesów przetwarzania w poszczególnych aplikacjach [Boynton, Johnson i Kell 2001, s. 337–338; Moeller, 2006, s. 461–494 i 513–556]. Ważniejsze kontrole komputerowe przedstawiono na rys. 1.

Kontrole ogólne i kontrole zastosowania wchodzą w skład kontroli przetwarzania danych skierowanych na ryzyko związane z autoryzacją, kompletnością i dokładnością transakcji, a szczególnie z audytem sprawozdań finansowych.

[2] Technologia informacji (*information technology* – IT) – zautomatyzowane środki służące tworzeniu, przetwarzaniu, przechowywaniu i przekazywaniu informacji. Obejmuje ona urządzenia do nagrywania, systemy komunikacyjne, systemy komputerowe (w tym sprzęt i oprogramowanie oraz dane), jak też inne urządzenia elektroniczne [MSRF 315 2005, s. 370].

Tabela 1. Elementy kontroli wewnętrznej według modelu COSO z uwzględnieniem aspektów IT

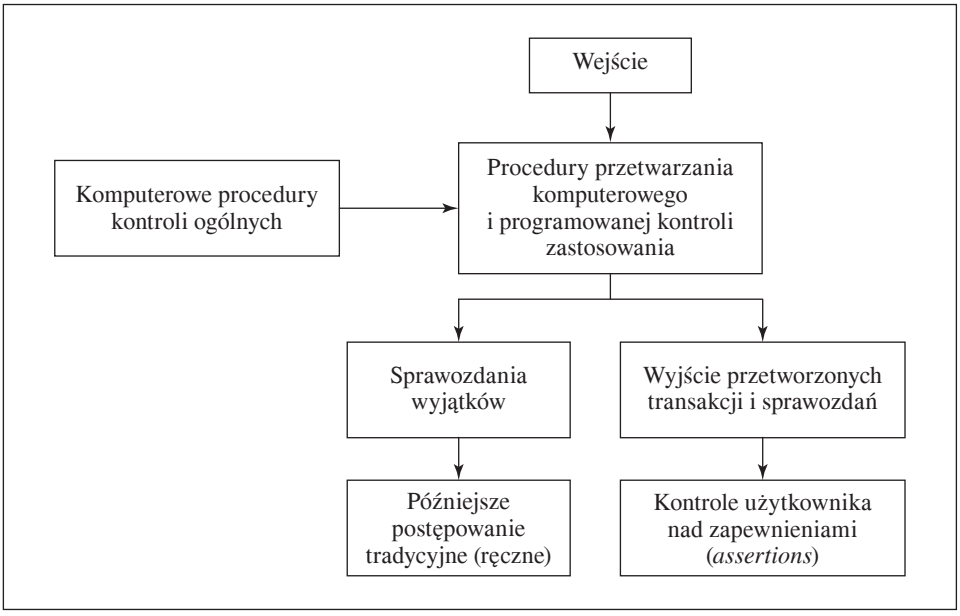
Komponent kontroli wewnętrznej	Opis odpowiedni do sprawozdawczości finansowej	Kluczowe czynniki	Ważne czynniki IT
Środowisko kontroli	Nadaje ton organizacji; wpływa na świadomość kontroli ludzi, jest podstawą wszystkich innych komponentów kontroli wewnętrznej	Czynniki środowiska kontroli: – uczciwość i wartości etyczne – odniesienie się do kompetencji – rada dyrektorów i komitet audytu – filozofia zarządu i styl działania – struktura organizacyjna – przydział uprawnień i odpowiedzialności – polityka zasobami ludzkimi i procedury	Zaangażowanie zarządu w ustanawianie zasad rozwoju, modyfikacji i stosowania programów komputerowych i danych, i w zrozumienie ryzyka IT Forma struktury organizacyjnej przetwarzanych danych (pionu IT i rachunkowości informatycznej) Metody przyznawania uprawnień i odpowiedzialności nad dokumentacją systemów komputerowych, łącznie z procedurami dla autoryzowania transakcji i zatwierdzania zmian systemów
Oszacowanie ryzyka	Identyfikacja jednostki, analiza i zarządzanie ryzykiem odpowiednio do przygotowania sprawozdań finansowych, które są rzetelnie prezentowane z dostosowaniem do GAAP	Proces szacowania ryzyka: – realacje ryzyka w stosunku do specyficznych ustaleń sprawozdań fianansowych i powiązanych czynności zapisu, przetwarzania, streszczania i raportowania danych finansowych – wewnętrzne i zewnętrzne wydarzenia i okoliczności – specjalne rozważenie zmian w okolicznościach, podobnie do audytorskiego oszacowania ryzyka nieodłącznego	Oszacowanie ryzyka: – ślad transakcji może być dostępny tylko częściowo i przez krótki okres (utrata ścieżki rewizyjnej) – zredukowana ewidencja dokumentująca dokonania kontroli – pliki i zapisy zwykle nie mogą być odczytane bez komputera – zmniejszona ingerencja ludzka w przetwarzaniu komputerowym może przysłaniać błędy możliwe do zaobserwowania w systemach ręcznych – podatność systemu IT na katastrofy fizyczne, nieupoważnione manipulacje oraz mechaniczne dysfunkcje – systemy IT mogą redukować tradycyjny podział obowiązków – zmiany w systemach są trudniejsze do wdrożenia i kontroli

cd. tabeli 1

Komponent kontroli wewnętrznej	Opis odpowiedni do sprawozdawczości finansowej	Kluczowe czynniki	Ważne czynniki IT
Informacja i komunikacja	System informacyjny obejmuje system rachunkowosci i składa się z metod i zapisów ustalonych do identyfikacji, gromadzenia, analizy, klasyfikacji, zapisu i sprawozdawczości jednostki oraz utrzymuje zdolność do rozliczeń dla powiązanych aktywów i zobowiązań; komunikacja zakłada zapewnienie jasnego zrozumienia indywidualnych ról i odpowiedzialności odnoszących się do kontroli wewnętrznej nad sprawozdawczością finansową	System rachunkowości powinien zapewniać: – sposób prowadzenia transakcji, który zapobiegałby niewłaściwym stwierdzeniom w sprawozdaniach finansowych zarządu – kompletny ślad audytu lub transakcji Zawiera podręczniki zasad postępowania, wykresy kont i memoranda	Transakcje mogą być inicjowane przez komputer Ślad audytu może być w formie elektronicznej W jaki sposób dane są przekazywane z dokumentów źródłowych na formę sensowną dla maszyny W jaki sposób pliki komputerowe są udostępniane i uaktualniane Zaangażowanie przetwarzania komputerowego od rozpoczęcia transakcji do włączenia w sprawozdania finansowe Zaangażowanie komputera w procesie sprawozdawczym używane do przygotowania sprawozdań finansowych
Czynności kontrolne	Zasady postępowania i procedury, które pomagają zapewnić, że dyrektywy zarządu są przekazywane i że podejmowane są konieczne działania, aby przeciwstawić się ryzyku przy osiąganiu celów jednostki; mają zróżnicowane cele i są stosowane na różnorodnych szczeblach organizacyjnych i funkcjonalnych	Kategorie: – podział obowiązków – kontrole przetwarzania informacji: kontrole ogólne, kontrole zastosowania – kontrole fizyczne – przeglądy działalności	Kontrole ogólne: – kontrola organizacyjna i operacyjna – kontrola rozwoju systemów i dokumentacji – kontrole hardware i software – kontrole dostępu – kontrole danych i proceduralne Kontrole zastosowania: – wejścia – przetwarzania – wyjścia

Komponent kontroli wewnętrznej	Opis odpowiedni do sprawozdawczości finansowej	Kluczowe czynniki	Ważne czynniki IT
Monitorowanie	Procesy prowadzone przez odpowiedni personel, który ocenia jakość kontroli wewnętrznej w czasie; zawiera oszacowanie i projektowanie, czy działa zgodnie z zamierzeniami oraz czy była modyfikowana odpowiednio do zmienionych warunków	Może przejawiać się przez: – bieżące czynności – oddzielne oceny okresowe Może obejmować dane wejściowe ze: – źródeł wewnętrznych, takich jak zarząd oraz audytorzy wewnętrzni – źródeł zewnętrznych, jak klienci, dostawcy, regulatorzy i zewnętrzni audytorzy	IT może być monitorowane w podobny sposób, jak inne kontrole wewnętrzne

Źródło: [Boynton, Johnson i Kell 2001, s. 349–350].



Rys. 1. Przegląd kontroli komputerowych
Źródło: [Boynton, Johnson i Kell 2001, s. 372].

Kontrole ogólne (*general controls*) ustanawiane są na poziomie jednostki w odniesieniu do wszystkich eksploatowanych w niej systemów użytkowych (aplikacji). Kontrole zastosowania (*application controls*) odnoszone są do poszczególnych systemów użytkowych, w tym do IS rachunkowości [Boynton, Johnson i Kell 2001, s. 337–338]. Rys. 1 ilustruje wagę kontroli komputerowych niezależnie od metod na wejściu, organizacji danych, ich przetwarzania lub innych urządzeń na wyjściu, np. gdy zlecenie sprzedaży zostaje wprowadzone do komputera, program akceptuje dane i poddaje je wielu różnym kontrolom edycyjnym (m.in. kontroli ważności numeru pozycji, danych klienta, osiągnięcia limitu kredytowego przez klienta). Przeznaczeniem kontroli zastosowania jest dostarczanie kierownictwu racjonalnej pewności, że w technologii informacji (IT) zapisuje się, przetwarza i raportuje dane, stosownie do specyficznych zastosowań. Różne kontrole zastosowania są zazwyczaj używane do operacji sprzedaży, w tym dokumentowanej paragonami gotówkowymi, zakupów, kontroli inwentaryzacyjnych, wypłat. Rezultat przetwarzania komputerowego i kontroli aplikacji jest podwójny: 1) komputer generuje na wyjściu transakcje i sprawozdania, które w niektórych systemach po przetworzeniu będą przedmiotem kontroli ręcznych, np. przegląd nadzorczy przez użytkownika systemu, 2) system wytwarza raporty wyjątków, z których jedne mogą się ukazywać na ekranie, np. sprawdzenie edycyjne ważności numeru

klienta, inne mogą być drukowane, np. transakcje w zbiorze, w którym klienci przekroczyli limit kredytowy. W każdym z tych przypadków należy zwrócić uwagę na wyjątki odnotowane przez komputer. Skuteczność kontroli zależy od zaprogramowanych kontroli aplikacji i następujących po nich czynności manualnych. Ważne są również kontrole ogólne rozwoju i zmian w programie, operacji komputerowych, dostępu do programów i danych. Reprezentują one wyższy poziom kontroli zapewniających o konsekwentnym i skutecznym działaniu indywidualnych aplikacji komputerowych [Boynton, Johnson i Kell 2001, s. 372–373].

3. Wpływ technologii informacji na elementy kontroli wewnętrznej w modelu COSO

Przegląd kontroli komputerowych ułatwia zrozumienie aspektów IT każdego z pięciu elementów kontroli wewnętrznej rozróżnianych w modelu COSO. Środowisko kontroli jest specyficznym składnikiem tak dla ręcznego, jak i komputerowego przetwarzania danych, a jego komponenty są niezależne od technicznych środków wprowadzonych do systemu informacyjnego jednostki. Ocena ryzyka odgrywa szczególną rolę w środowisku informatycznym ze względu na liczne zagrożenia, którym należy stawić czoła. Systemy IT niosą z sobą wiele korzyści i ryzyko, a ich uświadomienie pozwala lepiej zrozumieć wagę kontroli wewnętrznej w środowisku IT. Ważniejsze rodzaje ryzyka ujęto w tabeli 1. Główne korzyści systemów IT i zarządzania nimi polegają na tym, że mogą zapewnić większą precyzję w przetwarzaniu niż systemy ręczne, gdyż jednakowo poddają wszystkie transakcje takim samym kontrolom i mogą dostarczyć kierownictwu skuteczniejszych środków do nadzoru, przeglądu i analiz działalności w postaci szybciej sporządzanych sprawozdań finansowych [Boynton, Johnson i Kell 2001, s. 370–372 oraz MSRF 315 2005, s. 381]. Wiele rodzajów ryzyka jest kontrolowanych przez nawarstwiające się procedury kontrolne, tj. takie, w których jeden zestaw jest przeznaczony do kontroli przetwarzania transakcji, podczas gdy inny do kontroli systemów i programów kontrolujących i przetwarzających te transakcje. Ocena ryzyka powinna objąć rozważenie różnych jego rodzajów powiązanych z IT. Zarząd powinien zaprojektować systemy informacji i kontroli, które złagodzą problemy związane z udziałem IT w redukowaniu tradycyjnego podziału obowiązków. Jeśli ustanowi i wdroży dobry system ogólnych kontroli, wiele rodzajów ryzyka będzie zmniejszonych do poziomu możliwego do opanowania. W oszacowaniu ryzyka zarząd powinien wykazać się specjalnym podejściem do ryzyka powstałego wskutek zmienionych okoliczności, np.: zmian w środowisku operacyjnym, nowego personelu, nowych i odnowionych systemów informacji, szybkiego wzrostu, nowych technologii, linii, wyrobów, działań,

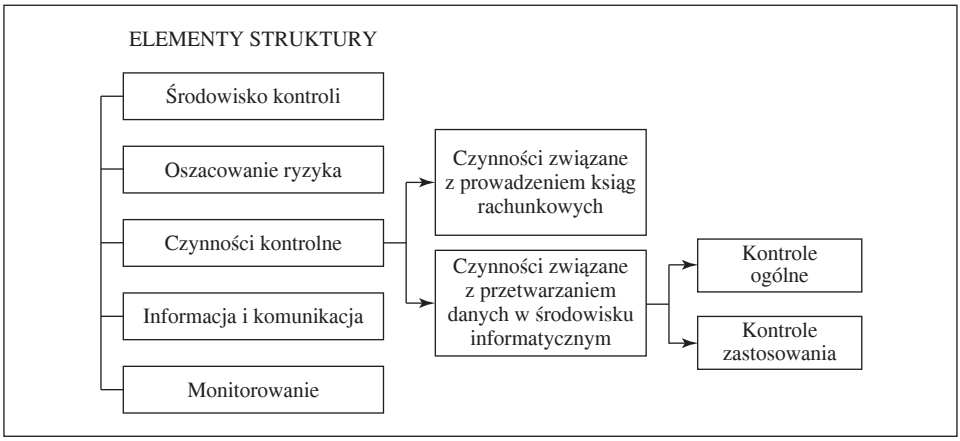
restrukturyzacji, operacji zagranicznych i sprawozdań finansowych w rachunkowości [Boynton, Johnson i Kell 2001, s. 334].

Wpływ IT na systemy informacji i komunikacji uwidocznił się w zmianie formy przechowywania i przekazywania wiedzy i danych. Przepływające przez systemy informacyjne zbiory informacji są w rzeczywistości niematerialnymi elementami tych systemów, ich materialną postacią są nośniki, na których dane są utrwalone. Należą do nich wydruki, dyski, taśmy magnetyczne. Informacje muszą być przyjęte, przetworzone i przekazywane tak, aby ich wewnętrzni i zewnętrzni użytkownicy mogli z nich w pełni skorzystać. Ważne jest zapewnienie przejrzystego śladu transakcji w systemach IT, gdzie ewidencja dokumentująca zdarzenia może być zatrzymywana przez krótki czas. Np. systemy on-line zwykle stwarzają unikalny numer transakcji, który może być użyty do ustalenia śladu transakcji[3]. Audytorzy używają go w dochodzeniu oraz zapewnianiu o istnieniu transakcji [Boynton, Johnson i Kell 2001, s. 335]. W ramach monitorowania członkowie zarządu, komitetu audytu i kierownictwa rachunkowości świadomi różnego ryzyka związanego z IT powinni na bieżąco śledzić dokonania kontroli w środowisku IT. Komitet audytu może też obciążyć audyt wewnętrzny okresowymi przeglądami ryzyka IT i obowiązkowymi ich kontrolami [Boynton, Johnson i Kell 2001, s. 348].

W najsilniejszym stopniu wpłynęła technologia informacji na czynności kontrolne wiążące się z przetwarzaniem danych w tym środowisku. Czynności te składają się z zasad i procedur dostarczających określonych zapewnień odnośnie do wykonywania dyrektyw zarządu. Wpływ IT jest na tyle duży, że uzasadnia rozpatrywanie struktury kontroli wewnętrznej w środowisku informatycznym, szczególnie rachunkowości, tylko pod kątem tego jednego elementu, co może prowadzić do pewnej modyfikacji struktury, efektem której jest podział na kontrole ogólne i zastosowań jako pochodnych działań związanych z przetwarzaniem danych w środowisku IT. Działania te, obok czynności związanych z prowadzeniem ksiąg rachunkowych, stanowią jeden z dwóch rodzajów działań kontrolnych wyróżnianych w środowisku IT. Czynności kontrolne dotyczące prowadzenia ksiąg odnoszą się do zasad i procedur powiązanych z systemem rachunkowości i jej podstawowym celem, tj. sporządzaniem sprawozdań finansowych. Należą do nich znane w systemach ręcznych praktyki, np.: opracowanie i właściwe prowadzenie dokumentacji i ksiąg, rozdzielenie funkcji niezgodnych, stosowanie upoważnień do przeprowadzania i zatwierdzania operacji, odpowiednie zabezpieczenie zasobów, prawidłowa wycena pozycji sprawozdań finansowych [Idzi-

[3] „Ślad rewizyjny (*audit trail*) jest to zdolność prześledzenia, na podstawie dokumentacji, wszystkich zapisów dotyczących danej transakcji, aż do jej początkowego salda lub źródła; umożliwiająca stwierdzenie, w jaki sposób powstały obecne salda, ścieżka rewizyjna stanowi podstawowy element kontroli wewnętrznej" [Patterson 2002, s. 433].

kowska 2002, s. 112–113]. Zastosowanie technologii informacji w rachunkowości narzuca konieczność wprowadzenia radykalnych zmian w powiązanym z nią systemie kontroli wewnętrznej, o czym przesądzają ilościowe i jakościowe zwiększenia elementów informacyjnych i proceduralnych rachunkowości, co oznacza wzrost stopnia złożoności nie tylko samych elementów systemu kontroli, ale też związków i zależności występujących między nimi. Zmodyfikowany schemat kontroli wewnętrznej w środowisku IT, z wyeksponowaniem czynności kontrolnych jako głównego elementu, i dalszym ich podziałem na czynności związane z prowadzeniem ksiąg rachunkowych i przetwarzaniem danych w środowisku IT wraz z końcowym podziałem tych ostatnich na kontrole ogólne i zastosowania przedstawia rys. 2.



Rys. 2. Struktura systemu kontroli wewnętrznej w środowisku informatycznym rachunkowości

Źródło: opracowanie własne na podstawie: [Idzikowska 2002, s. 113].

Ukazana zmiana struktury kontroli wewnętrznej w środowisku informatycznym rachunkowości jest konsekwencją specyficznych cech tego środowiska i szczególnego zagrożenia wiarygodności danych wymagających znaczącego rozbudowania czynności kontrolnych, a w ślad za tym zastosowanych rodzajów i metod kontroli. Czynności kontroli w środowisku IT powinny być poprzedzone właściwym podziałem obowiązków uważanym za krytyczny aspekt kontroli ogólnych. Kontrole ogólne prezentuje tabela 2.

Wśród kontroli ogólnych wyróżnia się zazwyczaj: kontrole organizacyjne i operacyjne (w nich mieści się podział obowiązków), kontrole rozwoju systemów i dokumentacji, kontrole *hardware* (sprzętu) i systemów *software* (oprogramowania), kontrole dostępu, kontrole danych i kontrole procedur. Podział

Tabela 2. Ogólne kontrole nad komputerowymi systemami informacyjnymi

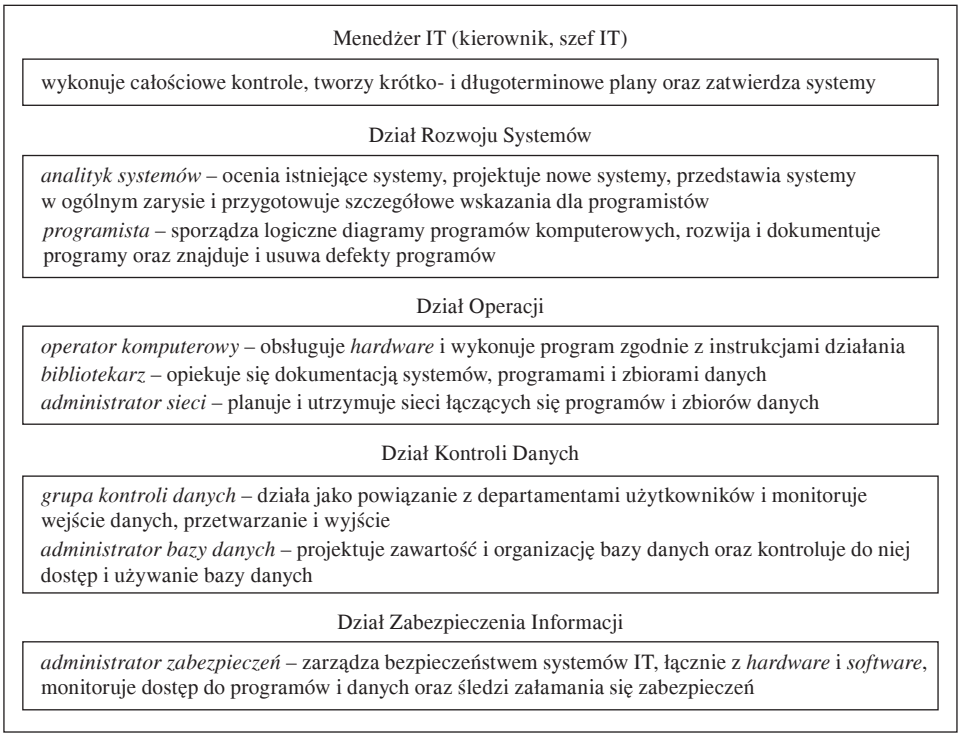
Rodzaj kontroli	Cel (przeznaczenie) kontroli	Zakres kontroli (obszary zagadnień)
Kontrole organizacyjne i operacyjne (zarządcze)	określenie organizacyjnych ram działania systemów informacyjnych (IS), tj. zorganizowanie i zarządzanie tymi systemami	– zasady i procedury wykonywania funkcji kontrolnych – odpowiedni podział niekompatybilnych funkcji (np. sporządzanie danych wejściowych dotyczących transakcji, programowanie oraz operacje komputerowe)
Kontrole rozwoju systemów i dokumentacji	dostarczenie wystarczającej pewności, że: – oprogramowanie systemowe jest opracowywane lub używane za odpowiednią zgodą i następuje to w sposób efektywny – systemy użytkowe są opracowywane i serwisowane pod nadzorem i działają wydajnie	– autoryzowanie, zatwierdzanie, testowanie, wdrażanie, dokumentowanie nowego oprogramowania systemowego oraz jego modyfikacji – testowanie, konwersja, wdrażanie, dokumentowanie nowych lub zaktualizowanych systemów użytkowych – zmiany programowe (użytkowe) – zakup systemów użytkowych od stron trzecich
Kontrole *hardware* i systemów *software* programów (eksploatacji systemów)	dostarczenie wystarczającej pewności, że: – wykrywa się błędy w działaniu urządzeń (aparatury) – programy są wykorzystywane wyłącznie do zatwierdzonych celów – używa się tylko zatwierdzonych programów	– podwójny odczyt (*dual read*) – sprawdzenie częściowe (*partity check*) – sprawdzenie echowe (*echo check*) – czytanie po pisaniu (*read after write*) – autoryzowanie celów i programów
Kontrole dostępu	dostarczenie wystarczającej pewności, że: – dostęp do danych i programów mają wyłącznie upoważnieni pracownicy – dostęp do operacji komputerowych mają wyłącznie upoważnieni pracownicy	– dostęp do sprzętu komputerowego – dostęp do oprogramowania systemowego – dostęp do dokumentacji systemów – dostęp do danych i programów – dostęp do operacji komputerowych
Kontrole wprowadzania danych i operacji komputerowych	dostarczenie wystarczającej pewności, że: – do systemu wprowadza się wyłącznie autoryzowane transakcje – wykrywa się i koryguje błędy w przetwarzaniu – zapewnia się ciągłość operacji w przypadku fizycznej katastrofy lub uszkodzenia (zepsucia się) komputera	– autoryzowanie transakcji – operacje komputerowe (obsługa komputerów), otrzymywanie i wyświetlanie wszystkich danych, które mają być przetworzone, księgowanie wszystkich danych wejściowych, wyśledzenie błędów przetwarzania, weryfikowanie odpowiedniej dystrybucji na wyjściu – kontynuacja operacji komputera przez: użycie pamięci *off-premise* dla ważnych plików, programów i dokumentacji, fizyczne zabezpieczenia przeciwko zagrożeniom środowiskowym, plany

cd. tabeli 2

Rodzaj kontroli	Cel (przeznaczenie) kontroli	Zakres kontroli (obszary zagadnień)
		zatrzymywania formalnego zapisu i odzyskiwania danych, użycia urządzeń wspomagających zlokalizowanych w innym miejscu; zabezpieczenia ciągłości przetwarzania polegają m.in. na przechowywaniu poza siedzibą kopii zapasowych danych i programów, możliwości przetwarzania poza siedzibą na wypadek zdarzeń losowych

Źródło: opracowanie własne na podstawie: [Boynton, Johnson i Kell 2001, s. 338–342].

obowiązków w organizacji IT powinien zapewniać wyraźne linie głównych uprawnień i odpowiedzialności dla każdego stanowiska, co ukazuje rys. 3.



Rys. 3. Główne odpowiedzialności dla każdego stanowiska w ramach departamentu (działu) IT

Źródło: opracowanie własne na podstawie: [Boynton, Johnson i Kell 2001, s. 339].

Tabela 3. Kontrole zastosowania (aplikacyjne)

Grupy kontroli	Cele (przeznaczenie) kontroli	Zakres (obszar) kontroli i szczegółowe rodzaje kontroli
Kontrole wejścia (wprowadzania danych) *input controls*	Dostarczanie wystarczającej pewności, że są wykrywane i zgłaszane błędy w danych wejściowych wprowadzanych do komputera; tj. że dane są zatwierdzane, przekształcane i zapisywane w plikach, nie są pomijane, dodawane jako fikcyjne, dwukrotnie wprowadzane, zmieniane oraz że niewłaściwe dane są odrzucane, poprawiane, a w razie potrzeby na nowo niezwłocznie wprowadzane do systemu	Kontrole poprawnej autoryzacji (*authorization*) generalnej i szczególnej przy przetwarzaniu bezpośrednim i wsadowym (*on-line data processing, batch processing*) Kontrole nad przekształceniem danych wejściowych (*conversion of input data*) obejmujące: 1) kontrole weryfikacyjne (*verification controls*) 2) edycję komputerową (*computer editing*) w tym: – sprawdzenie braku danych (*missing data check*) – sprawdzenie ważności charakteru zapisu (*valid charakter check*) – sprawdzenie (wystarczalności) limitu (*limit* [*reasonableness*] *check*) – sprawdzenie ważności znaku (*valid sign check*) – sprawdzenie ważności kodu (*valid code check*) – cyfra sprawdzająca (*check digit*), 3) poprawa błędu (*error correction*)
Kontrole przetwarzania (i zbiorów danych) *processing controls*	Dostarczanie wystarczającej pewności, że przetwarzanie komputerowe zostało dokonane zgodnie z intencją dla poszczególnych aplikacji, tj. że dane są chronione przed zagubieniem, przeoczeniem, dodawaniem czegoś do nich, duplikowaniem i zmianą podczas przetwarzania	Kontrole programowane włączone w *software* indywidualnych zastosowań obejmujące: – liczby kontrolne (*control totals*) – etykietki identyfikacyjne plików (*file identification labels*) – sprawdzenie limitu i racjonalności (*limit and resonableness check*) – raport przed-i-po (*before-and-after report*) – testy następstwa (sekwencji) (*sequence tests*) – dane przedstawiające ślad procesu przetwarzania (*process tracing data*)
Kontrole wyjścia (informacji wynikowych) *output controls*	Dostarczanie wystarczającej pewności, że rezultaty przetwarzania są poprawne i że tylko upoważnieni pracownicy otrzymują dane wyjściowe w ustalonych terminach; kontrole dotyczą adekwatności uzyskanych informacji względem danych wejściowych i weryfikacji uprawnień do odczytu i korzystania z informacji	Dokładność rezultatu przetwarzania dotyczy uaktualnionych plików czytelnych komputerowo i wydruków wyjścia; cel ten spełniany jest poprzez: – uzgodnienie liczb (kwot, sum) (*reconciliation of totals*) – porównanie z dokumentami źródłowymi (*comparison to source documents*) – wizualne skanowanie (*visual scanning*), osoby kontrolujące zazwyczaj utrzymują kontrole nad udostępnianiem danych wyjściowych; aby ułatwić kontrolę nad dysponowaniem danymi wyjściowymi dokumentacja systemów powinna zawierać sprawozdawczą kartę dystrybucji

Źródło: opracowanie własne na podstawie: [Boynton, Johnson i Kell 2001, s. 344–346].

Podział obowiązków w ramach komórki IT oraz pomiędzy nią a komórkami użytkującymi powinien być poprawny. Wiele funkcji, jak: rozwój systemów, operacje, kontrole danych, administracja zabezpieczeń, powinno być podzielonych. Dział IT nie może poprawiać danych przekazanych przez działy użytkujące i musi być od nich organizacyjnie niezależny. Słabości ogólnych kontroli organizacyjnych i operacyjnych zazwyczaj wpływają na wszystkie zastosowania (aplikacje) IT. Kontrole zastosowania odnoszą się do programów działających w komputerowych systemach informacyjnych lub do przebiegu aplikacyjnych procesów przetwarzania, w tym również zastosowanych w środowisku informatycznym rachunkowości. Kontrola wewnętrzna ma w tym wypadku posłużyć się metodami i procedurami kontrolnymi w odniesieniu do przebiegu procesów „wejścia", „przetwarzania" i „wyjścia". Odpowiednio do tego wśród kontroli zastosowania wyróżnia się trzy grupy znanych kontroli ukazanych w tabeli 3.

Można również wskazać, że ustalenie zasad i procedur związanych z kontrolami na poziomie jednostki (ogólnymi) i z kontrolami systemów użytkowych (aplikacyjnymi) oraz z bezpieczeństwem zasobów informatycznych jest zdeterminowane możliwymi do wyodrębnienia funkcjami, celami i zadaniami kontroli w środowisku IT.

4. Funkcje, cele i zadania kontroli w środowisku IT

Funkcje, cele i zdania kontroli w środowisku IT są uwzględniane we wszystkich mniej lub bardziej rozbudowanych klasyfikacjach kontroli dokonywanych w tym środowisku (tabela 4).

Wyszczególnione w tabeli 4 funkcje, cele i zadania kontroli rozstrzygają o ustalaniu zasad i procedur odnoszących się do kontroli ogólnych realizowanych na poziomie jednostki oraz do kontroli zastosowania dotyczących systemu użytkowego. Można też wskazać, wynikające z innych sposobów klasyfikacji, różne typy i rodzaje kontroli możliwe i warte wprowadzenia w ramach kontroli wewnętrznej systemów informatycznych, jak np. podział: według celów – na kontrole finansowe i niefinansowe, według relacji do zagrożeń – na prewencyjne, detekcyjne i korekcyjne, a według architektury systemu – na kontrole przetwarzania wsadowego, przetwarzania bezpośredniego, baz danych, sieci komputerowych i stanowisk autonomicznych. Jednak podział na kontrole ogólne i kontrole zastosowania, dokonany z punktu widzenia usytuowania w jednostce procedur kontrolno-rewizyjnych, jest dominujący. Jest to podział dwupoziomowy obejmujący kontrole ustanawiane na poziomie jednostki gospodarczej oraz kontrole występujące na poziomie systemu informatycznego rachunkowości. Podział ten umożliwia charakterystykę obu rodzajów kontroli i dobrze odzwierciedla istotę

Tabela 4. Funkcje, cele i zadania kontroli w środowisku informatycznym

Funkcje	Cele i zadania
Odpowiedzialność za kontrolę	– wykonywanie nadzoru nad tworzeniem i dystrybucją informacji oraz zasobami systemu informacyjnego
Rozwój i reprodukcja zasobów systemu informatycznego	– zaspokajanie potrzeb jednostki przez system informatyczny – zapewnienie sprawnego wdrażania systemu informatycznego – zapewnienie sprawnego użytkowania systemu – zapewnienie sprawności procesu rozwoju i reprodukcji zasobów systemu
Przetwarzanie danych i wykorzystywanie zasobów systemu informatycznego	– zaspokajanie bieżących i przyszłych potrzeb użytkowników informacji – zapewnienie sprawnego wykorzystania zasobów systemu – zapewnienie wiarygodności systemu informatycznego
Zabezpieczenie systemu	– zapewnienie należytego podziału niekompatybilnych funkcji wewnątrz jednostki – zapewnienie wyłącznie uprawnionego dostępu do zasobów systemu informatycznego – zapewnienie fizycznego zabezpieczenia zasobów systemu informatycznego przed nieupoważnionym dostępem oraz przypadkowymi lub rozmyślnymi uszkodzeniami lub stratami – zapewnienie możliwości odzyskiwania lub odtwarzania procesów przetwarzania w przypadku ich przerwania – zapewnienie możliwości podtrzymania i odtworzenia najważniejszych dla użytkownika procesów przetwarzania, które uległy przerwaniu
Kontrola wewnętrzna w ramach systemu informatycznego	– zapewnienie właściwego przebiegu procesu wprowadzania danych, przetwarzania i generowania informacji – zapewnienie właściwego przetwarzania danych stałych i technologicznych oraz przechowywania danych

Źródło: opracowanie własne na podstawie: [Idzikowska 2002, s. 117].

funkcjonowania rachunkowości w środowisku informatycznym, a także ułatwia biegłym rewidentom badanie kontroli wewnętrznej w tym środowisku [Idzikowska 2002, s. 114–116]. Podobne zagadnienia traktowane są jako nieodzowne przy opracowywaniu planów kontroli w środowisku IT i mogą posłużyć za wzorce do ich tworzenia w danej jednostce.

5. Zakończenie

Kontrola wewnętrzna w środowisku informatycznym została przedstawiona głównie z wykorzystaniem aspektów IT wkomponowanych w elementy kontroli wewnętrznej modelu COSO, ze względu wiodącą jego rolę w tworzeniu ogól-

nych ram kontroli wewnętrznej. Zaprezentowanie ujęcia IT w modelu COSO nie wyczerpuje wielu innych projektów i propozycji podziału kontroli wewnętrznej istniejących w środowisku informatycznym, w tym specyficznych modeli odnoszących się wyłącznie do kontroli informatycznych, takich jak modele SAC i eSAC (IIA), model COBIT (ISACA), czy model SysTrust (AICPA i CICA). Przedstawiony podział kontroli w środowisku IT na kontrole ogólne i kontrole zastosowania ukazuje rangę i wzrastające znaczenie kontroli informatycznych w ramach systemów kontroli wewnętrznej każdej jednostki.

Literatura

Boynton W.C., Johnson R.N., Kell W.G. [2001], *Modern Auditing*, 7th ed., John Wiley & Sons, Inc., New York–Toronto.

Idzikowska G. [2002], *Wiarygodność danych a bezpieczeństwo zasobów w środowisku informatycznym rachunkowości*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź.

Moeller R. [2005], *Brink's Modern Internal Auditing*, 6th ed., Wiley, Inc., Hoboken, New Jersey, USA.

MSRF 315 [2005], *Poznanie jednostki i jej środowiska oraz oszacowanie ryzyka wystąpienia istotnej nieprawidłowości*, Międzynarodowe Standardy Rewizji Finansowej 2005, KIBR, SKwP, Warszawa.

Patterson R. [2002], *Kompendium terminów z zakresu rachunkowości i finansów po polsku i po angielsku*, PricewaterhouseCoopers, Fundacja Rozwoju Rachunkowości w Polsce, Warszawa.

Streszczenie

W artykule przedstawiono kontrolę wewnętrzną w środowisku informatycznym zgodnie z modelem COSO i podkreślono znaczenie tej kontroli dla systemów kontroli wewnętrznej jednostek. Kontrola ta została ukazana na podstawie aspektów IT występujących w elementach kontroli wewnętrznej. Wyjaśniono też kontrole ogólne i kontrole zastosowania jako główne kontrole przetwarzania informacji. Na końcu przedstawiono funkcje, cele i zadania kontroli w środowisku IT.

Słowa kluczowe: technologia informacyjna, systemy informacyjne, kontrola wewnętrzna, kontrole procesu przetwarzania, kontrole ogólne, kontrole zastosowania.

COSO Model-based Control of an IT Environment

The article presents internal control in an IT environment done in accordance with the COSO model and emphasises the importance of the control to an entity's internal control systems. The paper describes the key components of internal control including relevant IT aspects. It also explains general and application controls employed as the main infor-

mation processing controls. The final section characterises the functions, objectives and control tasks in the IT environment.

Keywords: information technology, information systems, internal control, information processing controls, general controls, application controls.