1. Standardy kontroli zarządczej dotyczące systemów informatycznych i rachunkowości

W jednostce sektora finansów publicznych funkcjonowanie systemu kontroli zarządczej w obszarze rachunkowości i systemów informatycznych wspomagających jej prowadzenie sprowadza się zasadniczo do realizowania przez kierownictwo czynności nadzoru oraz wykonywania przez pracowników codziennych czynności kontrolnych w tym obszarze. Zarówno system rachunkowości, jak i system kontroli zarządczej w jednostce musi obejmować zespół czynności wykonywanych przez kierownictwo i pracowników w postaci procedur kontrolnych, które uwzględniają określone przepisy prawa i wewnętrzne regulacje. Wszystkie procedury kontrolne rachunkowości, w tym **procedury kontroli finansowo-księgowej i dotyczące środowiska informatycznego**, są ściśle ze sobą powiązane i zawierają się w elementach kontroli zarządczej.

Z komunikatu nr 23 Ministra Finansów z 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych wynika bezpośrednio **konieczność opracowania, wdrożenia, oceny i doskonalenia procedur kontroli w środowisku informatycznym**, które powinny funkcjonować w ramach systemu kontroli zarządczej w jednostce sektora finansów publicznych. A zatem zarówno system rachunkowości, jak i procedury kontroli w środowisku informatycznym w ramach systemu kontroli zarządczej w jednostce powinny być oparte co najmniej na:

- dostosowanej do realizowanych zadań publicznych i potrzeb jednostki strukturze organizacyjnej z podziałem uprawnień, obowiązków i odpowiedzialności,
- prawidłowo działających i wydajnych systemach przetwarzania danych finansowych,
- skutecznej kontroli przyjmowania i wydawania posiadanych zasobów,
- funkcjonującej kontroli wszystkich czynności mających wpływ na zmiany majątkowe w jednostce.

Przy czym **procedury kontrolne** w systemie rachunkowości wspomaganym systemami informatycznymi w jednostce powinny zapewniać co najmniej:

- właściwe wykonanie operacji księgowych zgodnie z przepisami prawa, przyjętymi zasadami (polityką) rachunkowości w jednostce oraz obowiązującym systemem upoważnień, uprawnień w systemie informatycznym rachunkowości i zatwierdzeń,
- niezawodność i bezpieczne przetwarzanie danych księgowych w taki sposób, aby komputerowe księgi rachunkowe i sprawozdawczość były prawidłowe i rzetelne,
- ochronę zasobów informatycznych zarówno w postaci rzeczowej, jak i elektronicznej.

O wdrożeniu w jednostce i funkcjonowaniu systemu kontroli zarządczej związanego z obszarem rachunkowości będzie świadczyło wiele **działań i mechanizmów kontrolnych.**

Działania i mechanizmy kontrolne

1. Przyjęte limity, uchwały, zarządzenia, regulaminy, plany (w tym plany zapewnienia ciągłości działania, plany awaryjne), polityki (w tym polityka ochrony informacji), procedury i instrukcje.
2. Hierarchizacja struktury organizacyjnej i uprawnienia nadzoru (kontrola kierownicza).
3. Ustalona siatka zastępstw i upoważnień.
4. Spisane zakresy czynności, uprawnień i obowiązków (lub karty stanowisk pracy).

5. Uprawnienia użytkowników w podsystemach informatycznych rachunkowości dostosowane do zajmowanego stanowiska i kompetencji.
6. Stosowanie fizycznych, organizacyjno-administracyjnych środków ochrony zasobów, w tym programowych środków ochrony zasobów informatycznych.
7. Wyspecyfikowane wymagania prowadzenia czynności kontroli na stanowiskach pracy, w tym czynności samokontroli, oraz obowiązek kontroli poziomej w kontaktach między stanowiskami pracy, komórkami organizacyjnymi.
8. Ograniczenia i zakazy wstępu do określonych pomieszczeń albo użytkowania określonych zasobów rzeczowych.
9. Obowiązek obecności dwóch i więcej osób przy określonych czynnościach (np. czynności inwentaryzacyjne) lub autoryzacji czynności przez drugą osobę.
10. Wprowadzone formalne ograniczenia uprawnień wewnętrznych i zewnętrznych (udzielania informacji, reprezentowania jednostki wobec osób trzecich, mediów itp.).
11. Inne ustalenia i sformalizowania wynikające ze specyfiki jednostki i szczególnych zasad rachunkowości, np. w zakładach budżetowych, oraz specyfiki systemów informatycznych stosowanych w tych podmiotach.

Funkcjonowanie kontroli zarządczej w obszarze systemów informatycznych w jednostce należy odpowiednio **udokumentować**. Podstawowymi dokumentami są m.in.:

- polityka i procedury zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości,
- plan awaryjny,
- plan zapewnienia ciągłości działania systemów informatycznych,
- dokumentacja ewidencyjna systemu informatycznego rachunkowości zgodnie z art. 10 ustawy z 29 września 1994 r. o rachunkowości (dalej: uor),
- procedury kontroli ogólnych w środowisku informatycznym,
- procedury kontroli aplikacyjnych dotyczące podsystemów informatycznych rachunkowości.

Silne powiązanie między etapami realizacji kontroli zarządczej w całej jednostce a zadaniami kontroli w systemie rachunkowości, w tym procedurami kontroli finansowo-księgowej, ma duży wpływ na wyznaczenie szczegółowych zadań na poszczególnych etapach kontroli, którymi jest objęty obszar funkcjonowania systemu informatycznego rachunkowości. Przy czym szczegółowe zadania kontroli, które są istotne dla prawidłowego funkcjonowania informatycznego rachunkowości w jednostce, wynikają:

1) ze specyfiki przyjętych rozwiązań i organizacji środowiska informatycznego w danej jednostce,
2) z celów i zadań systemu kontroli finansowo-księgowej i kontroli zarządczej w danej jednostce,
3) z obowiązku zapewnienia stosowania się do przepisów i przyjętych reguł prowadzenia rachunkowości w jednostce, które ujęto w zasadach (polityce) rachunkowości.

Zatem przy opracowywaniu systemu kontroli zarządczej w jednostce należy mieć na uwadze **cele kontroli finansowo-księgowej**, które mają być realizowane nie tylko w odniesieniu do systemu rachunkowości, ale i do elementów samego środowiska informatycznego rachunkowości.

Zdaniem autorki, **kontrola zarządcza w środowisku informatycznym rachunkowości w jednostce sektora finansów publicznych powinna być realizowana na dwóch poziomach:**

- **poziom I – cała jednostka** (tzw. kontrole ogólne) – dotyczy zapewnienia realizacji i egzekwowania zasad użytkowania wszystkich podsystemów rachunkowości w środowisku informatycznym,
- **poziom II – pojedynczy system użytkowy** (tzw. kontrole aplikacyjne) – dotyczy np. systemu finansowo-księgowego, kadrowo-płacowego itd.

Należy jednak pamiętać, że żaden nawet najlepiej zorganizowany system kontroli zarządczej nie jest doskonały i w stu procentach nie ochroni jednostki przed wszystkimi ryzykami i zjawiskami patologicznymi. System kontroli może jedynie ograniczyć ryzyko i skutki zmaterializowania się ryzyka do określonego akceptowalnego poziomu, ale nie jest w stanie całkowicie go wykluczyć, ponieważ po zastosowaniu nawet najlepszych obecnie dostępnych metod i środków ochrony zawsze pozostaje **ryzyko rezydualne.**

W jednostce sektora finansów publicznych ryzyko to ma szczególnie znaczenie w przypadku ochrony informacji w środowisku informatycznym. Można zastosować w jednostce najnowsze i najdroższe dostępne środki ochrony zasobów informatycznych na poziomie organizacyjno-administracyjnym, technicznym, fizycznym, sprzętowym, programowym, ale i tak nie wykluczy się w stu procentach sytuacji zaistnienia jednocześnie kilku zdarzeń, które mogą spowodować utratę tych zasobów. Nie można również wykluczyć niedbalstwa ze strony pracowników. Zazwyczaj to człowiek stanowi najsłabsze ogniwo systemu ochrony zasobów informatycznych. Należy również pamiętać, że szczególnie groźne jest ryzyko zmowy na różnych poziomach organizacyjnych zarówno na poziomie kierownika jednostki, jak i niższych szczeblach kierowniczych lub stanowiskach operacyjnych. W praktyce zdarzają się również przypadki zmowy członka kierownictwa z kontrahentem, w tym z kluczowym dostawcą usług i robót, np. wykonawcą projektu informatycznego.

Uzyskanie w jednostce efektywnego i adekwatnego systemu kontroli wymaga – oprócz posiadania, oceny i doskonalenia mechanizmów kontrolnych, będących reakcją na zidentyfikowane ryzyko – również innych elementów organizacyjnych, które utworzą ten system, czyli:

- właściwie kształtowanego środowiska funkcjonowania kontroli w jednostce,
- skutecznego i efektywnego systemu przepływu informacji i komunikacji w jednostce,
- sprawnie funkcjonującego systemu bieżącego monitorowania i okresowej oceny realizacji kontroli zarządczej.

Zatem należy mieć na uwadze, że system kontroli zarządczej w danej jednostce może być także nieefektywny z powodu niewłaściwie funkcjonujących ww. elementów organizacyjnych.

Kierownik jednostki i księgowi projektujący oraz wdrażający zasady i procedury kontroli zarządczej w środowisku informatycznym rachunkowości powinni także brać pod uwagę różne **dodatkowe przepisy prawa i normy ISO dotyczące bezpieczeństwa zasobów informatycznych**, które mogą mieć zastosowanie w danej jednostce. Uwzględnienie tych regulacji na etapie projektowania kontroli zarządczej może mieć istotny wpływ na jakość tego systemu w jednostce. Wśród tych regulacji są zarówno te, które bezpośrednio, jak i te, które pośrednio są związane ze środowiskiem informatycznym rachunkowości.

Do przepisów prawa w tym obszarze należy zaliczyć następujące **ustawy:**

- z 29 sierpnia 1997 r. o ochronie danych osobowych,
- z 27 lipca 2001 r. o ochronie baz danych,
- z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,

- z 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej,
- z 22 sierpnia 1997 r. o ochronie osób i mienia,
- z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Do ustaw tych wydano wiele aktów wykonawczych w tym zakresie.

Należy podkreślić, że w jednostkach sektora finansów publicznych w celu zapewnienia bezpieczeństwa zasobów informatycznych w ostatnich latach **stosowało się również wiele krajowych norm ISO**, są to np.:

- PN-ISO/IEC 17799/2007. Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji,
- PN-ISO/IEC 2382-8:2001. Technika informatyczna. Terminologia. Część 8: Bezpieczeństwo,
- PN-I-02000:2002. Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia,
- PN-ISO/IEC 27001:2007. Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania,
- PN-ISO/IEC 27005:2014-01. Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji,
- PN-ISO/IEC 24762:2010. Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie,
- PN-ISO/IEC 20000-2:2007. Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania,
- PN-ISO/IEC 20000-1:2014-01. Technika informatyczna – Zarządzanie usługami – Część 1: Wymagania dla systemu zarządzania usługami.

Z punktu widzenia organizacji kontroli zarządczej w środowisku informatycznym rachunkowości w jednostce istota i zakresy działania systemu kontroli zarządczej oraz systemu informatycznego rachunkowości wskazują na konieczność wspólnego ich rozpatrywania jako wspomagających się systemów w realizacji celów informacyjnych i kontrolnych rachunkowości oraz przyjętych celów jednostki.

2. Samoocena kontroli zarządczej dotycząca środowiska informatycznego rachunkowości

Wykorzystanie systemów informatycznych rachunkowości w jednostce sektora finansów publicznych skutkuje różnego typu wewnętrznymi i zewnętrznymi zagrożeniami. Dlatego bezpieczne wykorzystanie systemu informatycznego rachunkowości w jednostce powinno wiązać się z zapewnieniem określonych warunków ochrony zasobów informatycznych oraz prowadzenia dokumentacji systemów informatycznych rachunkowości zgodnie z uor.

2.1. Samoocena kontroli zarządczej w obszarze ochrony zasobów informatycznych rachunkowości

Warunki prawidłowej eksploatacji i ochrony zasobów informatycznych rachunkowości muszą sprostać wymogom, które są stawiane jednostkom przez uor (art. 71 ust. 1). Na jednostki sektora