Norma audytu i zapewnienia SI 1202 Ocena ryzyka w planowaniu

Szczególny charakter audytu i zapewnienia systemów informacyjnych (SI) oraz umiejętności niezbędne do wykonywania tych zadań wymagają norm, które ściśle odnoszą się do audytu i zapewnienia SI. Opracowanie i rozpowszechnianie norm audytu i zapewnienia SI to fundamentalny element profesjonalnego wkładu ISACA® dla społeczności audytorów.

Normy audytu i zapewnienia SI określają wymogi w zakresie audytu SI i sprawozdawczości oraz informują:

- Specjalistów w zakresie audytu i zapewnienia SI o minimalnym dopuszczalnym poziomie wykonawstwa w celu spełnienia wymogów odpowiedzialności zawodowej określonych w Kodeksie Etyki Zawodowej ISACA
- Zarząd oraz inne zainteresowane strony o oczekiwaniach branżowych dotyczących praktyki zawodowej
- Posiadaczy certyfikatu audytora systemów informacyjnych ® (CISA®) o wymogach. Nieprzestrzeganie powyższych norm może spowodować wszczęcie dochodzenia w sprawie postępowania posiadacza certyfikatu CISA przez Zarząd ISACA, lub odpowiednią komisję, oraz w ostateczności działania dyscyplinarne.

Specjaliści w zakresie audytu i zapewnienia SI winni dołączyć w swej pracy, tam gdzie należy, oświadczenie, że zadania zostały wykonane zgodnie z normami audytu i zapewnienia SI ISACA, a także z innymi, mającymi zastosowanie normami zawodowymi.

Ramowe zasady *ITAF*™ dla specjalistów w zakresie audytu i zapewnienia SI określają normy postępowania na wielu poziomach:

- **Normy**, podzielone na trzy kategorie:
  - Normy ogólne (seria 1000) — Są to podstawowe normy postępowania, zgodnie z którymi działa branża audytu i zapewnienia SI. Stosuje się je do wszystkich zadań, które dotyczą etyki zawodowej, niezależności, obiektywizmu, należytej staranności, a także wiedzy, kompetencji i umiejętności specjalisty ds. audytu i zapewnienia SI. Wymagania norm (**wytłuszczonym drukiem**) są obowiązkowe.
  - Normy wykonawcze (seria 1200) —dotyczą realizacji zadań takich jak planowanie i nadzór, określanie zakresu, ryzyko i istotność, organizowanie zasobów, nadzór i zarządzanie zadaniami , dokumentacja audytu i zapewnienia SI oraz zachowania profesjonalnego osądu i należytej staranności
  - Normy sprawozdawczości (seria 1400) — odnoszą się do typów raportów, sposobów komunikacji oraz przekazywanych informacji
- **Wytyczne,** wspierające normy i również podzielone na trzy kategorie:
  - Wytyczne ogólne (seria 2000)
  - Wytyczne wykonawcze (seria 2200)
  - Wytyczne sprawozdawczości (seria 2400)
- **Narzędzia i techniki**, dostarczające specjalistom ds. audytu i zapewnienia SI dodatkowe normy postępowania, np. białe księgi, programy audytu/zapewnienia SI, produkty z rodziny COBIT® 5

Słownik pojęć stosowanych w ITAF dostępny jest online pod adresem: *www.isaca.org/glossary*.

Zastrzeżenie: ISACA sporządziła te normy postępowań, jako minimalny dopuszczalny poziom wykonawstwa, w celu spełnienia wymogów odpowiedzialności zawodowej określonych w Kodeksie Etyki Zawodowej ISACA. ISACA nie gwarantuje, że wykorzystanie tego produktu zapewni osiągnięcie pomyślnych rezultatów. Nie należy traktować tej publikacji, jej procedur i testów w sposób wyłączny lub wykluczający inne procedury lub testy, które odpowiednio ukierunkowane przyniosłyby takie same rezultaty. Aby określić adekwatność konkretnej procedury czy testu, specjaliści ds. kontroli powinni kierować się własną oceną zawodową konkretnych okoliczności kontroli występujących w poszczególnych systemach lub środowiskach SI.

Komisja Standardów Zawodowych i Zarządzania Karierą ISACA (PSCMC) jest zobowiązana do szerokich konsultacji podczas przygotowywania norm i wytycznych. Przed wydaniem każdego dokumentu na całym świecie rozpowszechniona jest jego wersja wstępna, którą można publicznie skomentować. Komentarze mogą ponadto być przedstawione do wglądu dyrektorowi ds. opracowania standardów zawodowych za pośrednictwem poczty elektronicznej (*standards@isaca.org*), faksu (+1.847. 253.1443) lub tradycyjnej poczty (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

Norma audytu i zapewnienia SI 1202 Ocena ryzyka w planowaniu

Wymagania

1202.1 Funkcja audytu i zapewnienia kontroli SI powinna wykorzystywać odpowiednie podejście do oceny ryzyka, a także pomocniczą metodologię w celu opracowania całościowego planu audytu SI, oraz wytyczyć priorytety dla efektywnej alokacji środków dla audytu SI.

1202.2 Specjaliści z zakresu audytów i zapewnienia kontroli SI winni określać i oceniać ryzyko związane z analizowanym obszarem na etapie planowania realizacji poszczególnych prac.

1202.3 Specjaliści z zakresu audytów i zapewnienia kontroli SI winni uwzględniać ryzyko w przedmiotowym zakresie, w tym ryzyko związane z audytem, jak i ryzyka powiązane dla przedsiębiorstwa.

Kluczowe aspekty

Podczas planowania czynności w ramach funkcji audytu i zapewnienia kontroli SI należy:

- W celu ułatwienia sporządzenia planu audytu IS, przeprowadzić i udokumentować, przynajmniej raz na rok, formalną ocenę ryzyka (Ocena ryzyka).
- W ramach procesu oceny ryzyka załączyć plany i cele strategiczne organizacji, a także określić strukturę ramową zarządzania ryzykiem w przedsiębiorstwie oraz związane z nią inicjatywy.
- Podczas każdej realizacji audytu i zapewnienia kontroli SI określić ilościowo i uzasadnić wielkość zasobów potrzebnych do przeprowadzenia audytu SI zgodnie z wymogami.
- Stosować ocenę ryzyka przy wyborze obszarów i elementów będących przedmiotem audytu, a także do decyzji dotyczących planowania i realizacji poszczególnych audytów i działań kontrolnych SI.
- Dążyć do uzyskania zatwierdzenia oceny ryzyka od interesariuszy oraz innych zainteresowanych stron.
- Nadać priorytety i stworzyć harmonogram czynności audytu i zapewnienia kontroli SI w oparciu o ocenę ryzyka.
- W oparciu o ocenę ryzyka opracować plan, który:
  - Będzie działać jako struktura ramowa dla czynności audytu i zapewnienia kontroli SI
  - Uwzględni wymogi i czynności spoza obszaru audytu i zapewnienia kontroli SI
  - Będzie aktualizowany przynajmniej raz do roku i zatwierdzany przez osoby upoważnione
  - Określi zakres obowiązków ustalonych w karcie audytu (Karta audytu)

Podczas planowania realizacji konkretnego zlecenia (działania kontrolnego), specjaliści ds. audytu i zapewnienia kontroli SI powinni:

- Określić i ocenić ryzyko związane z kontrolowanym obszarem.
- Przeprowadzić wstępną ocenę ryzyka związanego z kontrolowanym obszarem przy każdym zleceniu. Cele dla poszczególnych zleceń winny odzwierciedlać wyniki wstępnej oceny ryzyka.
- Podczas analizy obszarów ryzyka i planowania danego zlecenia należy uwzględnić poprzednie audyty, oceny i wnioski, łącznie z działaniami naprawczymi. Należy też uwzględnić proces oceny ryzyka z poziomu Zarządu.

- W procesie audytu i kontroli należy podejmować wysiłek w celu zmniejszenia ryzyka audytu (Ryzyko audyt) do akceptowalnego poziomu. Cele audytu należy realizować przez prawidłową ocenę przedmiotowego zakresu SI i kontroli powiązanych.
- Podczas planowania konkretnej procedury audytu SI należy pamiętać, że im niższy jest próg istotności (Istotność), tym bardziej precyzyjne są oczekiwania związane z audytem i tym wyższe ryzyko.
- Aby zmniejszyć ryzyko niewykrycia zdarzeń o wyższej istotności, można albo rozszerzyć zakres testu narzędzi kontrolnych (zmniejszenie ryzyka prawidłowości kontroli) i/lub rozszerzyć procedury badania wiarygodności (Badanie wiarygodności) (zmniejszenie ryzyka niewykrycia nieprawidłowości), aby zyskać dodatkowe mechanizmy kontroli.

Terminy

Termin	Definicja
Karta audytu	Dokument zatwierdzony przez upoważnione osoby, określający cel, nadzór i zakres obowiązków w ramach audytu wewnętrznego. Karta powinna: • Określać pozycję funkcji audytu wewnętrznego w przedsiębiorstwie • Upoważniać do dostępu do danych, pracowników i zasobów fizycznych niezbędnych dla przeprowadzenia audytu i zapewnienia kontroli SI • Określać zakres czynności w ramach audytu
Ryzyko audytu	Ryzyko sformułowania nieprawidłowych wniosków na podstawie uzyskanych informacji. Trzy elementy ryzyka audytu to: • Ryzyko związane z działaniami kontrolnymi • Ryzyko niewykrycia • Ryzyko inherentne (dziedziczone)
Ryzyko związane z przedmiotowym zakresem audytu	Ryzyko związane z kontrolowanym obszarem: • Ryzyko handlowe (zdolność płatnicza klienta, wiarygodność kredytowa, czynniki rynkowe itp.) • Ryzyko kontraktowe (zakres odpowiedzialności, cena, typ, kary umowne itp.) • Ryzyko krajowe (polityka, środowisko, poziom bezpieczeństwa ogólnego itp.) • Ryzyko projektowe (zasoby, umiejętności, metodologia, stabilność produktu itp.) • Ryzyko technologiczne (rozwiązania, architektura, sprzęt i oprogramowanie, infrastruktura sieciowa, kanały dostaw itp.) Patrz ryzyko inherentne (dziedziczone).
Ryzyko związane z kontrolą	Ryzyko, że istnieje istotny błąd, któremu nie można było zapobiec albo wykryć na czas w ramach kontroli wewnętrznej. (Patrz ryzyko inherentne (dziedziczone)..)

Ryzyko niewykrycia	Ryzyko, że podstawowe procedury stosowane przez specjalistę ds. audytów **i kontroli** nie wykryją błędu, który może być istotny, sam w sobie i/lub w połączeniu z innymi błędami. Patrz ryzyko audytu.
Ryzyko inherentne (dziedziczone)	Poziom ryzyka bez uwzględniania działań, które podjęło lub może podjąć kierownictwo (np. wdrażanie procedur kontrolnych). Patrz ryzyko związane z kontrolą.
Istotność	Koncepcja audytu dotycząca ważności informacji względem jej wpływu na bądź konsekwencji w stosunku do jednostki podlegającej audytowi. Wyrażenie względnej ważności bądź znaczenia konkretnego zagadnienia w kontekście całości przedsiębiorstwa
Ocena ryzyka	Proces stosowany do określenia i oceny ryzyka i jego potencjalnych skutków. Ocenę ryzyka wykorzystuje się do określenia takich zagadnień bądź obszarów, które stanowią najwyższe ryzyko, podatność lub zagrożenie dla przedsiębiorstwa, i które należy uwzględnić w rocznym planie audytów SI. Ocenę ryzyka wykorzystuje się także do zarządzania realizacją projektów oraz ryzykiem związanym z utratą korzyści.
Badanie wiarygodności	Zbieranie w ramach audytu dowodów na temat kompletności, dokładności i istnienia czynności lub transakcji, jakie wystąpiły w badanym okresie

Powiązanie z wytycznymi

Typ	**Tytuł**
Wytyczna	2202; ocena ryzyka w planowaniu

Data obowiązywania

Niniejsza norma ISACA ma zastosowanie dla wszystkich realizacji audytów i zapewnienia kontroli SI od dnia 1 listopada 2013.