Norma audytu i zapewnienia SI
1207 Nieprawidłowości i czyny zabronione

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 1207 Nieprawidłowości i czyny zabronione

Wymagania

1207.1 Specjaliści z zakresu audytów i kontroli SI powinni uwzględniać ryzyko wystąpienia nieprawidłowości i czynów zabronionych podczas realizacji zlecenia.

1207.2 Specjaliści z zakresu audytów i kontroli SI winni zachowywać zawodowy sceptycyzm podczas realizacji zlecenia.

1207.3 Specjaliści z zakresu audytów i kontroli SI winni dokumentować i niezwłocznie zgłaszać wszelkie istotne nieprawidłowości lub czyny zabronione właściwym podmiotom we właściwym czasie.

Kluczowe aspekty

Specjaliści ds. audytu i kontroli SI winni:

- Zredukować ryzyka wynikające z prowadzenia audytu do akceptowalnego poziomu w fazie planowania i realizacji, poprzez:
  - Świadomość, że mogą zaistnieć istotne błędy, braki kontroli i błędne oświadczenia spowodowane nieprawidłowościami i czynami zabronionymi niezależnie od oceny ryzyka wystąpienia nieprawidłowości i czynów zabronionych
  - Zrozumienie natury przedsiębiorstwa i jego środowiska, łącznie z systemem kontroli wewnętrznej mającym na celu zapobieganie lub wykrywanie nieprawidłowości i czynów zabronionych istotnych dla przedmiotowego zakresu realizacji zlecenia i jego celów
  - Zdobycie dostatecznego i stosownego materiału dowodowego w celu ustalenia, czy kierownictwo, lub inne osoby w przedsiębiorstwie mają wiedzę na temat faktycznych, podejrzewanych lub rzekomych nieprawidłowości i czynów zabronionych
- Podczas realizacji procedur audytu uwzględnić niespotykane lub nadzwyczajne powiązania, które mogą wskazywać na ryzyko wystąpienia istotnych błędów, braków kontroli lub nieprawdziwych oświadczeń spowodowanych nieprawidłowościami i czynami zabronionymi,
- Stworzyć i wdrożyć procedury w celu zweryfikowania prawidłowości kontroli wewnętrznej oraz ryzyka, że kierownictwo może omijać procedury kontroli mające na celu zapobieganie lub wykrywanie nieprawidłowości i czynów zabronionych,
- Ocenić, czy zidentyfikowane błędy, brak kontroli lub nieprawdziwe oświadczenia mogą wskazywać na obecność Nieprawidłowość lub czynu zabronionego. Jeśli istnieją takie przesłanki, należy przeanalizować ich konsekwencje dla innych aspektów realizacji zlecenia, a w szczególności w stosunku do oświadczeń kierownictwa.
- Oświadczenia pisemne należy od kierownictwa uzyskiwać przynajmniej raz na rok lub częściej, zależnie od zlecenia, aby:
  - Potwierdzić odpowiedzialność kierownictwa za formę i wdrożenie procedur kontroli wewnętrznej w celu zapobiegania i wykrywania nieprawidłowości i czynów zabronionych.
  - Ujawnić stosowne wyniki jakichkolwiek ocen ryzyka, które wskazują, że mogą występować błędy, braki kontroli lub nieprawdziwe oświadczenia spowodowane nieprawidłowością lub czynem zabronionym.
  - Ujawnić kierownictwu i osobom pełniącym ważne funkcje w systemie

Kluczowe aspekty

ciąg dalszy

kontroli wewnętrznej wiedzę zarządczą nt. nieprawidłowości i czynów zabronionych mających wpływ na przedsiębiorstwo.
  - Ujawnić wiedzę zarządczą nt. wszelkich rzekomych bądź podejrzewanych nieprawidłowości i czynów zabronionych mających wpływ na przedsiębiorstwo, przekazaną przez pracowników, byłych pracowników, czynniki urzędowe itd.
- Niezwłocznie powiadomić:
  - Odpowiedni szczebel kierownictwa, przekazując wszelkie informacje nt. zidentyfikowanych lub otrzymanych danych wskazujących na możliwość istnienia nieprawidłowości lub czynu zabronionego
  - Osoby upoważnione o wszelkich istotnych nieprawidłowościach lub czynach zabronionych dotyczących kierownictwa lub osób piastujących ważne stanowiska w systemie kontroli wewnętrznej
- Poinformować osoby upoważnione o zidentyfikowanych podczas realizacji zlecenia wszelkich istotnych słabościach w projekcie i realizacji systemu kontroli wewnętrznej, którego celem jest zapobieganie i wykrywanie wszelkich nieprawidłowości i czynów zabronionych, nawet jeśli zidentyfikowane słabości wykraczają poza zakres zlecenia.
- Uwzględnić wszelkie wymogi prawne i związane ze sprawozdawczością mające zastosowanie w danych okolicznościach.
- Rozważyć wycofanie się z realizacji zlecenia, jeśli istotne błędy, braki kontroli, nieprawdziwe oświadczenia lub czyny zabronione mogą mieć negatywny wpływ na realizację zlecenia.
- Dokumentować wszelką komunikację, plany, wyniki, oceny i wnioski odnoszące się do istotnych nieprawidłowości i czynów zabronionych, o których poinformowane zostało kierownictwo, osoby upoważnione, ustawodawcy i inni.

Terminy

Termin	Definicja
Nieprawidłowość	Nieprzestrzeganie polityki ustalonej przez kierownictwo lub wymogów prawnych. Może obejmować celowo nieprawdziwe oświadczenia lub zatajenie informacji dotyczących zakresu audytu lub całości przedsiębiorstwa, rażące zaniedbania lub niezamierzone czyny zabronione.
Istotnie nieprawdziwe oświadczenie	Przypadkowe lub zamierzone nieprawdziwe oświadczenie, które ma wpływ na wynik audytu w wymiernym zakresie
Zawodowy sceptycyzm	Postawa, która zakłada kwestionowanie i krytyczną ocenę materiałów podlegających audytowi. Źródło: Amerykański Instytut Biegłych Rewidentów (AICPA) AU 230.07

Powiązania z normami i wytycznymi

Typ	Tytuł
Norma	Kryteria 1008
Norma	1202 Ocena ryzyka w planowaniu
Norma	1205 Dowód/dowody
Wytyczne	2206 Korzystanie z pracy innych specjalistów
Wytyczne	2207 Nieprawidłowości i czyny zabronione

Norma audytu i zapewnienia SI 1207 Nieprawidłowości i czyny zabronione

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