Norma audytu i zapewnienia SI 1401 Sprawozdawczość

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 1401 Sprawozdawczość

Wymagania

1401.1 Specjaliści ds. audytów i zapewnienia kontroli SI winni po zakończeniu zlecenia sporządzić raport zawierający wyniki ich pracy, zawierający:

- **Identyfikację przedsiębiorstwa, adresatów raportu oraz wszelkie ograniczenia co do jego treści i udostępniania**
- **Zakres, cele zlecenia, analizowany okres oraz charakter, czas trwania oraz prace wykonane w ramach zlecenia**
- **Ustalenia, wnioski i zalecenia**
- **Wszelkie kwalifikacje lub ograniczenia zakresu, które specjalista ds. audytów i zapewnienia kontroli SI ustalił w odniesieniu do danego zlecenia**
- **Podpis, datę i zakres rozpowszechniania zgodnie z kartą audytu lub zleceniem audytowym**

1401.2 Specjaliści ds. audytów i zapewnienia kontroli SI winni zadbać o to, by wnioski zawarte w raporcie były poparte dostatecznymi i odpowiednimi dowodami.

Kluczowe aspekty

Specjaliści ds. audytu i zapewnienia kontroli SI winni:

- Uzyskać odpowiednie pisemne oświadczenie od podmiotu polegającemu audytowi, szczegółowo określające kluczowe obszary zlecenia, kwestie, które wynikły w trakcie jego realizacji, sposoby ich rozwiązania oraz oświadczenia poczynione przez podmiot audytowany.
- Zadbać o to, by oświadczenia podmiotu audytowanego zostały przezeń podpisane i opatrzone datą w celu potwierdzenia znajomości zakresu obowiązków związanych ze zleceniem
- Ewidencjonować i przechowywać w dokumentacji wszelkie oświadczenia, pisemne i ustne, otrzymane w toku realizacji zlecenia. Przy zleceniach związanych z atestacją w celu zmniejszenia możliwości nieporozumienia, należy uzyskać pisemne oświadczenia ze strony podmiotu audytowanego.
- Dostosować formę i treść raportu do rodzaju zlecenia, czyli:
  - Audyt (bezpośredni lub z atestowaniem)
  - Weryfikacja (bezpośrednia lub z atestowaniem)
  - Uzgodnione procedury
- Opisać w raporcie istotne lub znaczące niedociągnięcia i ich konsekwencje dla osiągnięcia celów zlecenia.
- Przedyskutować z kierownictwem merytoryczną treść raportu wstępnego przed jego finalizacją i publikacją. W zależności od potrzeb opisać w raporcie końcowym reakcję kierownictwa na ustalenia, wnioski i zalecenia.
- Powiadomić osoby upoważnione, a w miarę potrzeby odnośne władze, o znaczących niedociągnięciach i istotnych słabościach systemu kontroli; informacje o tych powiadomieniach zamieścić w raporcie.
- W raporcie końcowym wymienić także wszystkie inne raporty.
- Poinformować kierownictwo podmiotu objętego audytem o takich niedociągnięciach w wewnętrznym systemie kontroli, które niekoniecznie są znaczące, ale nie pozostają bez wpływu na jakość systemu kontroli. W takich wypadkach należy powiadomić osoby upoważnione lub odnośne władze o fakcie poinformowania kierownictwa o powyższych niedociągnięciach w systemie kontroli.
- Określić normy przestrzegane podczas zlecenia i poinformować w razie potrzeby o wszelkich niezgodnościach z tymi normami.

Terminy

Termin	Definicja
Informacje istotne	W odniesieniu do mechanizmów kontrolnych, informują oceniającego o ważnych kwestiach związanych z działaniem tych mechanizmów lub ich składowych. Informacje, które bezpośrednio potwierdzają działanie mechanizmów kontrolnych są najważniejsze. Informacje odnoszące się pośrednio do działania mechanizmów kontrolnych mogą również być ważne, ale mają mniejsze znaczenie niż informacje bezpośrednie. Pojęcie powiązane z celami jakości informacji w COBIT 5
Informacje wiarygodne	Informacje, które są dokładne, weryfikowalne i pochodzą z obiektywnego źródła. Pojęcie powiązane z celami jakości informacji w COBIT 5
Informacje wystarczające	Informacje są wystarczające, gdy oceniający zbiorą dostateczną ich ilość, by móc sformułować sensowny wniosek. Aby informacje były wystarczające, muszą być też odpowiednie. Pojęcie powiązane z celami jakości informacji w COBIT 5
Informacje odpowiednie	Aktualne (tj. odpowiadające założonemu celowi), wiarygodne (tj. dokładne, weryfikowalne, pochodzące z obiektywnego źródła) i dostarczone na czas (tj. sporządzone i wykorzystane w odpowiednim czasie). Pojęcie powiązane z celami jakości informacji w COBIT 5
Informacje dostarczone na czas	Sporządzone i wykorzystane w takim czasie, by możliwe było zapobieżenie lub wykrycie braków kontroli, zanim staną się one istotne dla przedsiębiorstwa. Pojęcie powiązane z celami jakości informacji w COBIT 5

Powiązania z normami i wytycznymi

Typ	Tytuł
Wytyczna	2401 Sprawozdawczość

Data obowiązywania

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