Norma audytu i zapewnienia SI 1008 Kryteria

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 1008 Kryteria

Wymagania

1008.1 Specjaliści ds. audytu i zapewnienia SI winni wybierać kryteria oceny przedmiotowego zakresu , które są obiektywne, kompletne, relewantne, wymierne, jasne, powszechnie uznane, miarodajne i zrozumiałe przez lub dostępne dla wszystkich czytelników i użytkowników raportu.

1008.2 Specjaliści ds. audytu i zapewnienia SI winni wziąć pod uwagę źródło kryteriów i skupić się na tych, które zostały ustanowione przez ważne uprawnione instytucje przed akceptacją mniej znanych kryteriów.

Kluczowe aspekty

Specjaliści ds. audytu i zapewnienia SI winni:

- Starannie rozważyć wybór Kryteriów i móc ten wybór uzasadnić.
- Kierować się zawodowym osądem by zapewnić, że zastosowanie kryteriów umożliwi przygotowanie rzetelnej i obiektywnej opinii lub wniosku, który nie wprowadzi czytelnika bądź użytkownika w błąd. Przyjmuje się, że kierownictwo może zaproponować kryteria, które nie spełniają wszystkich wymogów.
- Wziąć pod uwagę stosowność i dostępność kryteriów podczas ustalania wymogów realizacji zadania.
- W przypadku gdy kryteria nie są łatwo dostępne, są niekompletne lub są zależne od interpretacji zamieścić opis i wszelkie inne informacje niezbędne by zapewnić, że raport jest rzetelny, obiektywny i zrozumiały oraz że kontekst, w którym te kryteria są stosowane jest zawarty w raporcie.

Stosowność i odpowiedniość kryteriów oceny przedmiotowego zakresu należy ocenić w oparciu o pięć poniższych kryteriów stosowności:

- **Obiektywność** — Kryteria winny być wolne od stronniczości, która mogłaby niekorzystnie wpłynąć na wyniki i wnioski specjalisty, wskutek czego mogłaby wprowadzić w błąd użytkownika raportu.
- **Kompletność** — Kryteria winny być wystarczająco kompletne, aby wszystkie kryteria mogące wpłynąć na wnioski specjalisty w przedmiotowym zakresie były określone i wykorzystane w toku realizacji zadania audytowego lub zapewniającego SI.
- **Relewancja** — Kryteria winny mieć związek z przedmiotowym zakresem i przyczynić się do uzyskania wyników i wniosków, które spełniają cele zadania audytowego lub zapewniającego SI.
- **Wymierność** — Kryteria winny umożliwić spójny pomiar przedmiotowego zakresu oraz wypracowanie spójnych wniosków gdy zostaną zastosowane przez różnych specjalistów w podobnych okolicznościach.
- **Zrozumiałość** — Kryteria winny być przedstawione jasno i nie podlegać znacząco odmiennym interpretacjom docelowych użytkowników.

Na dopuszczalność kryteriów ma wpływ ich dostępność dla użytkowników raportu specjalisty, by użytkownicy rozumieli podstawy czynności zapewniających i znaczenie wyników i wniosków. Źródła mogą obejmować takie, które są:

- **Uznane** — Kryteria winny być uznane w wystarczającym stopniu tak, by ich stosowanie nie było kwestionowane przez docelowych użytkowników.
- **Miarodajne** — Należy wyszukiwać takie kryteria, które odzwierciedlają autorytatywne oświadczenia w danej dziedzinie i są odpowiednie dla

Aspekty kluczowe Ciąg dalszy

przedmiotowego zakresu. Dla przykładu autorytatywne oświadczenia mogą pochodzić od profesjonalnych instytucji, grup branżowych, władz i organów nadzorczych.

- **Publicznie dostępne** — Kryteria winny być dostępne dla użytkowników raportu specjalisty. Przykłady obejmują normy opracowane przez specjalistyczne podmioty zajmujące się rachunkowością i audytami, jak ISACA, Międzynarodowa Federacja Księgowych (IFAC) oraz inne uznane organizacje rządowe lub zawodowe.
- **Dostępne dla wszystkich użytkowników** —Gdy kryteria nie są publicznie dostępne, należy je przedstawić wszystkim użytkownikom w oświadczeniach, które stanowią część raportu specjalisty. Oświadczenia składają się ze stwierdzeń dot. przedmiotowego zakresu, które spełniają wymogi stosowności kryteriów by mogły być poddane audytowi.

Poza stosownością i dostępnością, wybór kryteriów zapewnienia SI winien uwzględniać także źródło —w odniesieniu do użycia i potencjalnego odbiorcy. Na przykład zajmując się regulacjami rządowymi, najbardziej odpowiednimi mogą być kryteria oparte na oświadczeniach powstałych z przepisów prawa i regulacji, które odnoszą się do przedmiotowego zakresu. W innych przypadkach relewantne mogą być kryteria stowarzyszeń branżowych lub handlowych. Możliwe źródła kryteriów, ułożone w kolejności znaczenia to:

- **Kryteria ustanowione przez ISACA**—Są to publicznie dostępne kryteria i normy, które zostały poddane ocenie branżowej i szczegółowemu procesowi zachowania należytej staranności przez uznanych międzynarodowych ekspertów w zakresie ładu informatycznego, kontroli, bezpieczeństwa i zapewnienia.
- **Kryteria ustanowione przez inne organizacje —** Podobne do norm i kryteriów ISACA, są relewantne do przedmiotowego zakresu, zostały opracowane, poddane ocenie branżowej i szczegółowemu procesowi zachowania należytej staranności przez ekspertów z wielu dziedzin.
- **Kryteria ustanowione przez przepisy i regulacje** — Choć przepisy i regulacje mogą stanowić podstawę kryteriów, należy stosować je ostrożnie. Często sformułowania są złożone i mają określony sens prawny. W wielu przypadkach może być konieczne przeformułowanie wymogów na oświadczenia. Ponadto opiniowanie przepisów prawa jest zazwyczaj zarezerwowane dla prawników.
- **Kryteria ustanowione przez przedsiębiorstwa, które nie przestrzegają należytego procesu** —Obejmują relewantne kryteria opracowane przez inne przedsiębiorstwa, które nie przestrzegały należytego procesu i nie będące przedmiotem publicznej konsultacji i debaty.
- **Kryteria opracowane specjalnie do zadania audytowego lub zapewniającego SI** — Choć kryteria opracowane specjalnie do zadania audytowego lub zapewniającego SI mogą być odpowiednie, należy zachować szczególną staranność upewnając się, że spełniają kryteria stosowności, zwłaszcza kompletność, wymierność i obiektywność. Kryteria opracowane specjalnie do zadania audytowego lub zapewniającego SI występują w formie oświadczeń.

Kryteria wyboru należy starannie rozważyć. Podczas gdy przestrzeganie miejscowych przepisów i regulacji jest ważne i należy je przyjąć jako wymóg obowiązkowy, uznaje się, że wiele zadań audytowych i zapewniających SI obejmuje obszary nie ujęte w przepisach prawa i regulacjach, takie jak zarządzanie zmianami, ogólne kontrole IT i kontrole dostępu. Ponadto niektóre branże, takie jak sektor kart płatniczych, ustanowiły

obowiązkowe wymogi, które muszą być spełnione. Tam, gdzie wymogi ustawodawcy opierają się na zasadach, specjalista powinien upewnić się, że wybrane kryteria odpowiadają celomzadania.

W miarę postępu zadania, dodatkowe informacje mogą sprawić, że niektóre kryteria nie będą potrzebne do osiągnięcia celów. W takich okolicznościach dalsza praca nad kryteriami nie będzie potrzebna.

Terminy

Termin	Definicja
Kryteria	Normy i wzorce stosowane do mierzenia i prezentacji przedmiotowego zakresu, w oparciu o które audytor SI ocenia przedmiotowy zakres. Kryteria winny być: • Obiektywne - wolne od stronniczości • Kompletne - obejmować wszystkie istotne elementy niezbędne do sformułowania wniosku • Relewantne - mieć związek z przedmiotowym zakresem • Mierzalne- umożliwiać spójny pomiar W zadaniu atestacyjnym stanowią wzorce, w oparciu o które może być ocenione pisemne oświadczenie kierownictwa nt. przedmiotowego zakresu. Specjalista formułuje wniosek dotyczący przedmiotowego zakresu, korzystając ze stosownych kryteriów.

Powiązanie z wytycznymi

Typ	Tytuł
Wytyczna	Kryteria 2008

Data obowiązywania

Niniejsza norma ISACA ma zastosowanie do wszystkich zadań audytowych i zapewniających SI od dnia 1 listopada 2013.