

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 postępowania, 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).

Komisja Standardów Zawodowych i Zarządzania Karierą ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Przewodniczący	Teksańska Komisja Zdrowia i Opieki Społecznej, USA
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, Wielka Brytania
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, USA
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, Malezja
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, Nowa Zelandia
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japonia
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgia
Timothy Smith, CISA, CISSP, CPA	LPL Financial, USA
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentyna

Norma audytu i zapewnienia SI 1007 Oświadczenia

Wymagania

1007.1 Specjaliści ds. audytu i zapewnienia SI winni przejrzeć oświadczenia, na podstawie których oceniany będzie przedmiotowy zakres, aby stwierdzić, czy te oświadczenia można poddać audytowi oraz czy są one wystarczające, rzetelne i dotyczą przedmiotowego zakresu.

Kluczowe aspekty

Specjaliści ds. audytu i zapewnienia SI winni:

- Dokonać ewaluacji kryteriów oceny przedmiotowego zakresu, aby zapewnić, że są zgodne z Oświadczenie.
 - Ustalić, czy oświadczenia mogą być poddane audytowi i są wsparte potwierdzającymi informacjami.
 - Ustalić, czy oświadczenia są oparte na kryteriach, które są właściwie określone i poddają się obiektywnej i wymiernej analizie.
 - Tam, gdzie oświadczenia zostały sporządzone przez kierownictwo, upewnić się, że w porównaniu z innymi normami dot. autorytatywnych oświadczeń, oświadczenia te są wystarczające w zakresie tego, czego mógłby oczekiwać zorientowany w przedmiocie czytelnik lub użytkownik.
 - Tam, gdzie oświadczenia zostały sporządzone przez strony trzecie, które obsługują mechanizmy kontroli w imieniu przedsiębiorstwa, upewnić się, że oświadczenia są zweryfikowane i zatwierdzone przez kierownictwo.
 - Raportować bezpośrednio w odniesieniu do przedmiotowego zakresu (raport bezpośredni) bądź w odniesieniu do oświadczenia na temat przedmiotowego zakresu (raport pośredni).
 - Formułować wnioski dotyczące każdego oświadczenia w oparciu o całość wyników, kryteria oraz profesjonalny osąd.
-

Terminy

Termin	Definicja
Oświadczenie	Każda formalna deklaracja lub zestaw deklaracji na temat przedmiotowego zakresu, sformułowanych przez kierownictwo. Zwykle oświadczenia powinny mieć formę pisemną i zawierać listę konkretnych atrybutów przedmiotowego zakresu lub procesu obejmującego przedmiotowy zakres.

Powiązanie z wytycznymi

Typ	Tytuł
Wytyczna	2007 Oświadczenia

Data obowiązywania

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