

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 wymagania 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 (**wytluszczonym 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 jej 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
Ailsdair 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 1203 Wykonawstwo i nadzór

Wymagania

- 1203.1** Aby zaadresować wszystkie zidentyfikowane ryzyka, specjaliści ds. audytu i kontroli SI winni prowadzić prace zgodnie z zatwierdzonym planem audytu SI. Prace winny być prowadzone zgodnie z ustalonym harmonogramem.
- 1203.2** Specjaliści ds. audytów i kontroli SI winni zapewnić nadzór nad personelem wykonującym audyt SI, za który to personel są odpowiedzialni. Ich odpowiedzialnością jest osiągnięcie celów audytu w zgodności ze standardami zawodowymi.
- 1203.3** Specjaliści ds. audytów i kontroli SI winni przyjmować tylko takie zlecenia, których realizacja leży w zakresie ich wiedzy i umiejętności lub co do których można się w sposób uzasadniony spodziewać, że nabeżdą oni umiejętności w trakcie realizacji zlecenia, lub zrealizują zadanie pod nadzorem.
- 1203.4** Specjaliści ds. audytów i kontroli SI winni uzyskać dostateczne i stosowne dowody, aby zrealizować cel audytu. Obserwacje i wnioski należy poprzeć właściwą analizą i interpretacją dowodów audytowych.
- 1203.5** Specjaliści ds. audytów i kontroli SI winni są udokumentować proces audytu, opisując wykonane prace i zebrane dowody, które potwierdzają zidentyfikowane obserwacje i wnioski.
- 1203.6** Specjaliści ds. audytów i kontroli SI winni przeanalizować zebrane materiały i na ich podstawie sformułować wnioski.
-

Kluczowe aspekty

Specjaliści ds. audytu i zapewnienia kontroli SI winni:

- Przydzielać członków zespołu do zadań odpowiadających ich umiejętnościom i doświadczeniu, zgodnie z potrzebami realizowanego zlecenia.
- W razie potrzeby uzupełnić zespół audytowy o zewnętrzne zasoby, jak i zapewnić właściwy nadzór nad ich pracą.
- Zarządzać rolami i zakresem obowiązków poszczególnych członków zespołu audytowego w trakcie trwania zlecenia audytowego. Minimalne wymagania w tym obszarze to:
 - Odpowiedzialność za realizację i weryfikację zlecenia
 - Odpowiedzialność za opracowanie metodologii i podejścia
 - Tworzenie programu audytu i **zapewnienia kontroli**
 - Prowadzenie prac
 - Adresowanie problemów, wątpliwości i trudności w miarę powstawania
 - Dokumentowanie i porządkowanie obserwacji
 - Pisanie raportu
- Zapewnić, aby każde zlecenie wykonane przez członka/ów zespołu było zweryfikowane przez innego kompetentnego członka zespołu.
- Wykorzystywać najlepsze dostępne dowody i materiały audytowe. Dowody te powinny odpowiadać istotności celu audytu oraz czasowi i wysiłkowi koniecznym w celu ich pozyskania.
- Pozyskać dodatkowe dowody, jeśli zgodnie z profesjonalnym osądem pozyskane dane nie są wystarczające i właściwe, aby możliwe było sformułowanie opinii czy

Norma audytu i zapewnienia SI 1203 Wykonawstwo i nadzór

Kluczowe aspekty ciągu dalszy

- wniosków.
- Zorganizować i udokumentować realizowane zlecenie - zgodnie z wcześniej zdefiniowanymi, udokumentowanymi i zatwierdzonymi procedurami.
 - Zawrzeć w dokumentacji:
 - Cele audytu, zakres prac, program audytu, wykonane czynności kontrolne, zebrane dowody i materiały, wnioski i rekomendacje
 - Szczegóły wystarczające, by osoba niezaangażowana w realizację zlecenia była w stanie powtórzyć zadania wykonane podczas jego realizacji i dojść do takich samych wniosków
 - Informacje pozwalające na identyfikację osób, które realizowały poszczególne zadania, jak i role tych osób w przygotowywaniu i weryfikacji dokumentacji
 - Datę sporządzenia i weryfikacji dokumentacji
 - Uzyskać odpowiednie pisemne oświadczenie od audytowanego, potwierdzające kluczowe obszary realizowanego zlecenia, zidentyfikowane obserwacje, w jaki sposób zostały zaadresowane oraz zapewnienie ich realizacji przez audytowanego.
 - Zadbać o to, by oświadczenia audytowanego zostały podpisane i opatrzone datą w celu potwierdzenia jego odpowiedzialności związanej z realizacją zlecenia.
 - Dokumentować i przechowywać w archiwum wszelkie upoważnienia otrzymane w trakcie realizacji zlecenia, niezależnie od tego, czy były wyrażone w formie ustnej, czy pisemnej.
-

Powiązania z normami i wytycznymi

Typ	Tytuł
Norma	1005 Należyta staranność zawodowa
Norma	1205 Dowód/dowody
Norma	1401 Sprawozdawczość
Wytyczna	2202 Ocena ryzyka w planowaniu

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