

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 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 1205 Dowody

Wymagania

- 1205.1 Specjaliści w zakresie audytów i zapewnienia kontroli SI powinni uzyskać właściwy i wystarczający materiał dowodowy, pozwalający na wyciągnięcie uzasadnionych wniosków, na których opierają się wyniki realizowanych zleceń.**
- 1205.2 Specjaliści w zakresie audytów i zapewnienia kontroli SI powinni ocenić czy uzyskali wystarczającą ilość dowodów do poparcia wniosków i osiągnięcia celów realizowanego zlecenia.**
-

Kluczowe aspekty

Podczas realizacji usługi, specjaliści w zakresie audytu i zapewnienia kontroli SI powinni:

- Uzyskać wystarczającą ilość Właściwych dowodów, w tym:
 - Wykonane procedury
 - Wyniki wykonanych procedur
 - Dokumenty źródłowe (w formacie papierowym lub elektronicznym), zapisy i informacje potwierdzające wykorzystane dla wsparcia realizacji zlecenia
 - Ustalenia i wyniki realizacji zlecenia
 - Dokumentację potwierdzającą, że prace zostały wykonane zgodnie z odnośnym prawem, przepisami i politykami
- Przygotować dokumentację, która powinna być:
 - Zachowana i dostępna przez okres czasu i w formacie zgodnymi z politykami organizacji w zakresie audytów lub zapewnienia kontroli oraz z odnośnymi standardami zawodowymi, prawem i przepisami
 - Zabezpieczona przed dostępem osób nieupoważnionych i modyfikacjami podczas sporządzania i przechowywania
 - Odpowiednio zniszczona po zakończeniu okresu przechowywania
- Ocenic czy ilość dowodów zebranych podczas testów mechanizmów kontrolnych jest wystarczająca dla potwierdzenia oszacowanego poziomu ryzyka tych mechanizmów.
- Odpowiednio zidentyfikować, skorelować i skatalogować zebrane dowody.
- Uwzględnić właściwości, takie jak źródło, charakter (np. pisemne, ustne, wizualne, elektroniczne) i autentyczność (np. podpisy elektroniczne i ręczne, pieczęcie) dowodów podczas oceny ich wiarygodności.
- Rozważyć najbardziej ekonomiczne i korzystne czasowo metody zbierania niezbędnych dowodów, aby zapewnić realizację celów zlecenia i zminimalizować ryzyka jej wykonania. Jednakże trudności i koszty nie mogą stanowić podstawy do pominięcia niezbędnej procedury.
- Wybrać najbardziej stosowną procedurę zbierania dowodów, zależną od przedmiotu audytu (tj. jego charakteru, czasu trwania, profesjonalnego osądu). Procedury uzyskiwania dowodów obejmują:
 - Zapytania i potwierdzenia
 - Powtórzenie procedury
 - Ponowne wyliczenia
 - Obliczenia
 - Procedury analityczne
 - Kontrole
 - Obserwacje
 - Inne ogólnie przyjęte metody

Norma audytu i zapewnienia SI 1205 Dowody

- Aspekty
kluczowe
ciąg dalszy
- Przeanalizować źródła i charakter wszelkich otrzymanych informacji, aby ocenić ich wiarygodność i określić wymagania ewentualnej dalszej weryfikacji. Generalnie, wiarygodność dowodów jest większa, gdy są one:
 - w formie pisemnej, a nie ustnej
 - uzyskane z niezależnych źródeł
 - uzyskane przez specjalistę, a nie przez audytowany podmiot
 - poświadczane przez niezależny podmiot
 - w posiadaniu niezależnego podmiotu
 - wynikami kontroli
 - wynikami obserwacji
 - Uzyskać obiektywne dowody wystarczające do tego, by niezależny kwalifikowany podmiot mógł ponownie przeprowadzić testy i uzyskać takie same rezultaty i wnioski.
 - Uzyskać dowody współmierne do istotności mechanizmu kontrolnego i związanego z nim ryzyka.
 - Położyć odpowiedni nacisk na dokładność i kompletność informacji, gdy informacje uzyskane od przedsiębiorstwa są wykorzystywane przez specjalistę ds. audytów lub zapewnienia kontroli SI w procedurach audytu.
 - Ujawniać wszystkie sytuacje, w których Dostateczna ilość dowodów była niemożliwa do uzyskania w sposób zgodny z zasadami przekazywania wyników realizacji zleceń audytu lub zapewnienia kontroli SI.
 - Zabezpieczyć dowody przed dostępem osób nieupoważnionych i modyfikacją.
 - Po zakończeniu prac związanych z usługą audytu lub zapewnienia kontroli SI zachować materiały tak długo, jak to będzie konieczne, by spełnić wymagania stosownego prawa, przepisów i polityk.

Terminy

Termin	Definicja
Właściwe dowody	Miara jakości materiału dowodowego
Dostateczna ilość dowodów	Miara ilości materiałów; pomaga sformułować wszystkie pytania związane z istotnością i zakresem audytu. Patrz Dowody

Powiązanie
z wytycznymi

Typ	Tytuł
Wytyczna	2205 Dowody

Data obowiązywania

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