

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<sup>®</sup> 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<sup>®</sup> (CISA<sup>®</sup>) 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<sup>™</sup> 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<sup>®</sup> 5

Słownik pojęć stosowanych w ITAF dostępny jest online pod adresem: [www.isaca.org/glossary](http://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](mailto: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**

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

## Norma audytu i zapewnienia SI 1201 Planowanie realizacji zlecenia

### Wymagania

- 1201.1 Specjaliści ds. audytu i zapewnienia kontroli SI powinni planować każdą usługę audytu i zapewnień SI, w celu określenia:**
- Celu/ów, zakresu, ram czasowych i efektów prac
  - Zgodności z odnośnymi przepisami prawa i profesjonalnymi standardami realizacji audytu
  - W razie potrzeby zastosowania podejścia opartego na analizie ryzyka
  - Kwestii charakterystycznych dla danego zlecenia
  - Wymogów dot. dokumentowania i raportowania
- 1201.2 Specjaliści ds. audytu i zapewnienia kontroli SI powinni opracować i udokumentować plan realizacji projektu audytu lub zapewnienia kontroli SI, który to plan powinien obejmować:**
- Charakter zlecenia, cele, ramy czasowe i wymagane zasoby
  - Czas trwania i zakres procedur audytu wymagane w celu realizacji zlecenia
- 

### Kluczowe aspekty

- Specjaliści ds. audytu i zapewnienia kontroli SI powinni:
- Zrozumieć działalność poddawaną audytowi. Zakres wymaganej wiedzy należy ustalić w kontekście profilu przedsiębiorstwa, jego środowiska, obszarów ryzyka i celów zlecenia.
  - Uwzględnić wytyczne bądź instrukcje w przedmiotowym zakresie, według ustawodawstwa, regulacji, reguł, dyrektyw i wytycznych wydanych przez rząd lub instytucje branżowe.
  - Przeprowadzić ocenę ryzyka, by zapewnić odpowiednie objęcie wszystkich istotnych elementów w trakcie realizacji zlecenia. Następnie należy opracować strategię audytu, poziomy istotności i wymogi dot. zasobów.
  - Plan realizacji zlecenia należy opracować z wykorzystaniem odpowiednich metodologii zarządzania projektem, w celu zapewnienia, że czynności projektowe nie będą wykraczały poza zakres i budżet.
  - W planie uwzględnić kwestie bezpośrednio związane z zadaniem, takie jak:
    - Dostępność osób z odpowiednią wiedzą, umiejętnościami i doświadczeniem
    - Identyfikacja narzędzi potrzebnych przy zbieraniu materiałów, realizacji testów i przygotowywanie/podsumowanie informacji na potrzeby raportowania
    - Kryteria oceny, które będą miały zastosowanie
    - Wymogi raportowania i udostępniania
  - Udokumentować plan projektu przeprowadzenia audytu lub zapewnienia kontroli SI, aby jednoznacznie wskazać:
    - Cel/e, zakres i ramy czasowe
    - Zasoby
    - Role i odpowiedzialności
    - Zidentyfikowane obszary ryzyka i ich wpływ na plan realizacji zlecenia
    - Narzędzia i technik, które będą miały zastosowanie
    - Rozmowy ustalające stan faktyczny, które powinny zostać przeprowadzone
    - Istotne informacje, które należy uzyskać
    - Procedury do weryfikacji lub potwierdzenia uzyskanych informacji i wykorzystanie ich jako materiału dowodowego
    - Założenia dotyczące sposobu postępowania, metodologii, procedur, przewidywanych wyników i wniosków

## Norma audytu i zapewnienia SI 1201 Planowanie realizacji zlecenia

Kluczowe  
aspkety  
Ciąg dalszy

- Rozplanować realizację zlecenia w czasie, biorąc pod uwagę czas, dostępność oraz inne zobowiązania, a także wymogi kierownictwa podmiotu audytowanego, w możliwym zakresie.
- Dostosować plan projektu podczas realizacji audytu lub zapewnienia kontroli SI w celu określenia kwestii, które wynikną w trakcie realizacji zlecenia, takie jak nowe ryzyka, niewłaściwe założenia lub wnioski z procedur już zakończonych.
- Przy zleceniu audytu wewnętrznego:
  - Udostępnić kartę audytu audytowanemu; gdzie to konieczne zastosować zlecenie audytowe lub jego ekwiwalent w celu dalszego wyjaśnienia lub potwierdzenia zaangażowania do konkretnego zlecenia
  - Udostępnić plan audytowanemu, by miał do dyspozycji całość informacji, i by mógł w razie potrzeby zapewnić odpowiedni dostęp do osób, dokumentów i innych zasobów
- Przy usłudze zleceń zewnętrznych:
  - Sporządzić osobne zlecenie audytowe dla każdej zewnętrznej usługi audytu i zapewnienia kontroli SI
  - Sporządzić plan projektu dla każdej zewnętrznej usługi audytu i zapewnienia kontroli SI. Plan powinien przynajmniej dokumentować cel/e i zakres zlecenia.

Powiązanie  
z wytycznymi

Typ	Tytuł
Wytyczna	2201; Planowanie realizacji zlecenia

Data  
obowiązująca

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