

Standardy, wytyczne i procedury audytowania i kontrolowania systemów informatycznych

- Kodeks Etyki Zawodowej
- Standardy, wytyczne i procedury audytowania SI
- Standardy kontrolowania SI



Obowiązujące od 1 czerwca 2002

Information Systems Audit and Control Association

2001-2002 ASSOCIATION BOARD

Robert S. Roussey, CPA	University of Southern California, USA
Marios Damianides, CISA, CA, CPA	Ernst & Young, LLP, USA
Stephen W. Head, CISA, CPA, CPCU, CMA, CFE, CISSP	Royal & SunAlliance, USA
Dean R.E. Kingsley, CISA, CA	Deloitte Touche Tohmatsu, Australia
Lynn C. Lawton, CISA, BA, FCA, FIIA, PIIA	KPMG, Wielka Brytania
Jae Woo Lee, Ph.D.	Dongguk University, IAI, Korea
Johann Tello Meryk	Banco del Istmo, S.A., Panama
Ronald Saull, CSP	The Great-West Life Assurance Company/London Life/Investors Group, Kanada
Paul A. Williams, FCA, MBCS	Paul Williams Consulting, Wielka Brytania
Patrick Stachtchenko, CISA, CA	Deloitte & Touche, Francja

2001-2002 STANDARDS BOARD

Chair, Claudio Cilli, CISA, Ph.D.	KPMG, Włochy
Claude Carter, CISA, CA	Nova Scotia Auditor General's Office, Kanada
Sergio Fleginsky, CISA	PricewaterhouseCoopers, Urugwaj
Alonso Hernandez Garcia, CISA, ROAC	Colegio Economistas, Hiszpania
Marcelo Hector Gonzalez, CISA	Central Bank of Argentina Republic, Argentyna
Andrew J. MacLeod, CISA, FCPA, MACS, PCP	Brisbane City Council, Australia
Peter Niblett, CISA, CA, CIA, FCPA	Day Neilson, Australia
Venkatakrishnan Vatsaraman, CISA, ACA, AICWA, CISSP	Emirates Airlines, Zjednoczone Emiraty Arabskie
Sander S. Wechsler, CISA, CPA	Ernst & Young, USA

Zastrzeżenie o zrzeczeniu się odpowiedzialności "Standardów Audytowania SI"

Niniejsza publikacja wydana przez The Information Systems Audit and Control Association (ISACA) nie stwierdza, że standardy audytowania SI dają pewność pozytywnych rezultatów. Nie należy zakładać, że standardy stanowią zbiór wszelkich wytycznych, norm i procedur, ani że mogą być wykorzystane z pominięciem innych (obowiązujących) wytycznych, norm i procedur, stosowanie się do których daje możliwość osiągnięcia takich samych wyników.

Decydując o stosowności poszczególnych standardów, wytycznych i procedur, audytor powinien kierować się własnym profesjonalnym osądem wobec specyficznych warunków kontroli, związanych z danym systemem czy środowiskiem.

Warunki upowszechniania i Prawa Autorskie "Standardów Audytowania SI"

© 2002 by the Information System Audit and Control Association. Wszelkie prawa zastrzeżone. Standardy mogą być reprodukowane i wykorzystywane tylko i wyłącznie w celach niekomercyjnych. Reprodukowanie w celach komercyjnych jest zabronione bez wcześniejszej pisemnej zgody stowarzyszenia ISACA. Wszelkie wykorzystanie (wszelkie formy korzystania ze) Standardów audytowania SI muszą zawierać łatwo widoczne przedstawienie następującej notki i potwierdzenia praw autorskich: „© 2002 Information Systems Audit and Control Association. Niniejszy dokument jest reprodukowany za zgodą Information Systems Audit and Control Association.” Poza tym, co tutaj oznajmiono, żadne inne prawa czy zezwolenia nie są udzielane jeśli chodzi o standardy, odnośnie których wszelkie prawa są zastrzeżone.

© Copyright 2002
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web site: www.isaca.org

Spis treści

	Strona
KODEKS ETYKI ZAWODOWEJ	4
JAK KORZYSTAĆ Z TEJ PUBLIKACJI?	5
PRZEGLĄD STANDARDÓW AUDYTOWANIA SYSTEMÓW INFORMATYCZNYCH	6
INDEKS STANDARDÓW I WYTYCZNYCH AUDYTOWANIA SI	7
INDEKS PROCEDUR AUDYTOWANIA SI	7
STANDARDY AUDYTOWANIA SYSTEMÓW INFORMATYCZNYCH	8
WYTYCZNE AUDYTOWANIA SI	9
PROCEDURY AUDYTOWANIA SI	65
BIBLIOGRAFIA	79
STANDARDY KONTROLI SYSTEMÓW INFORMATYCZNYCH	80
HISTORIA	82
DODATEK-SŁOWNIK/INDEKS	83
FORMULARZ UWAG DO STANDARDÓW ISACA	93

Kodeks etyki zawodowej

ISACA™ - stowarzyszenie do spraw audytu i kontroli systemów informatycznych ustanawia niniejszy kodeks etyki zawodowej w celu ukierunkowania zawodowego i osobistego postępowania członków Stowarzyszenia oraz osób posiadających tytuł Certyfikowanego Audytora Systemów Informatycznych (CISA®) i Certyfikowanego Managera Bezpieczeństwa Informatycznego (CISM®)

Członkowie Stowarzyszenia, CISA oraz CISM powinni:

- Wspomagać wdrażanie właściwych standardów, procedur i mechanizmów kontrolnych systemów informatycznych oraz wspierać działania mające na celu zachowanie zgodności z nimi.
- Służyć pilnie, lojalnie i uczciwie, w interesie właściwych stron oraz nie uczestniczyć świadomie w żadnych nielegalnych lub niewłaściwych działaniach.
- Zachowywać prywatność i poufność informacji pozyskanych w czasie pełnienia obowiązków, chyba, że ich ujawnienie wymagane jest przez prawo. Informacje te nie mogą być używane ani w celu osiągnięcia własnych korzyści ani wydawane niewłaściwym stronom.
- Wypełniać swoje obowiązki w sposób niezależny i obiektywny i unikać działań grożących utratą niezależności lub obiektywności, lub mogących do niej prowadzić.
- Zachowywać kompetentność w obszarach związanych z audytem i kontrolą systemów informatycznych.
- Wyrażać zgodę na podejmowanie tylko takich działań, które całkowicie będą mogły być przeprowadzone w ramach zawodowych kompetencji.
- Wypełniać swoje obowiązki z należytą starannością zawodową.
- O rezultatach wykonanych audytów i/lub prac kontrolnych informować odpowiednie strony, ujawniając wszystkie poznane istotne fakty, które, jeśli nie zostałyby ujawnione, mogłyby zafałszować raporty dotyczące operacji lub ukryć niezgodne z prawem praktyki.
- Wspierać działania edukacyjne kierowane do użytkowników, środowiska zawodowego, społeczności szeroko rozumianych odbiorców, kadr kierowniczych, zarządów, w celu poszerzania ich rozumienia audytu i kontroli systemów informatycznych.
- Utrzymywać wysokie standardy zachowania i charakteru i nie angażować się w działania dyskredytujące dla zawodu.

Niestosowanie się do powyższego Kodeksu Etyki Zawodowej może doprowadzić do szczegółowego zbadania postępowania (członka stowarzyszenia lub Certyfikowanego Audytora) i w rezultacie spowodować podjęcie kroków dyscyplinarnych.

Jak korzystać z tej publikacji?

Powiązanie Standardów z Wytycznymi i Procedurami

Istnieje osiem kategorii Standardów Audytowania SI. Standardy Audytowania SI są krótkimi i obowiązkowymi wymaganiami wobec raportów audytowych tworzonych przez członków stowarzyszenia ISACA lub Certyfikowanych Audytorów SI (CISA). Wytyczne Audytowania SI oraz procedury stanowią szczegółową pomoc w tym, jak stosować owe standardy. Wytyczne Audytowania SI są wskazówkami, zgodnie z którymi audytor zwykle będzie postępował, dopuszczając wystąpienie sytuacji w których audytor do nich się nie zastosuje. W takich przypadkach, na audytorze spoczywa odpowiedzialność za uzasadnienie sposobu, w jaki prace zostały przeprowadzone. Przykłady procedur pokazują, jakie kroki podejmuje audytor SI i mają charakter w większym stopniu informacyjny od Wytycznych. Przykłady procedur są tak zbudowane, aby ściśle nawiązywać do Standardów i Wytycznych Audytowania SI oraz dostarczać wskazówek jak się stosować do Standardów. W pewnym stopniu, ustanawiają one również tzw. "dobre praktyki", z którymi procedury powinny być zgodne.

Kodyfikacja

Trzy pierwsze cyfry w numerze dokumentu dotyczą ośmiu kategorii standardów. Standardy audytowania SI zaczynają się od cyfry "0" a standardy dla specjalistów od systemu kontroli SI zaczynają się od cyfry "5". Numery poszczególnych standardów stanowią drugą trójkę cyfr w numerze dokumentu. Trzecia grupa cyfr w numerze dokumentu jest numerem wytycznej. Procedury są wyszczególniane osobno i numerowane zgodnie z datą wydania. Kompletna lista omawianych dokumentów zawarta jest w spisach standardów, wytycznych i procedur audytowania SI.

Kategoria standardu	Standard	Wytyczna
000	.000	.000

Na przykład, dokument 060.020.040 jest wytyczną. Dostarcza wskazówek do szóstej kategorii standardów, pt. Realizacja Prac Audytowych,. Wytyczna dotyczy drugiego standardu w tej kategorii, pt. Dowody. Jest to czwarta wytyczna wyszczególniona w pozycji Dowody.

Procedury są numerowane w kolejności zgodnie z tym jak są wydawane, zaczynając od numeru "1".

Jak stosować?

Sugeruje się, aby w ramach corocznego programu audytowego, jak również w ramach indywidualnych przeglądów w trakcie roku, audytor SI przeglądał standardy w celu zapewnienia zgodności z nimi. Szczegółowe wytłumaczenie poszczególnych zagadnień znajduje się w spisie (słowniku). Są w nim określone terminy a następnie wyszczególnione są numery dokumentów, do których się odnoszą. Audytor SI może odwoływać się do standardów w swoich raportach, stwierdzając, że przegląd został przeprowadzony zgodnie z prawem danego kraju, odpowiednimi regulacjami dotyczącymi audytu i standardami ISACA.

Kopie elektroniczne

Wszystkie Standardy, Wytyczne i Procedury ISACA umieszczone są na stronach internetowych Stowarzyszenia pod adresem www.isaca.org/standards.

Słownik/indeks

Słownik na końcu niniejszej publikacji zawiera zarówno definicje terminów, jak również listę dokumentów standardów, w których te terminy występują.

Przegląd standardów audytowania systemów informatycznych

Wydane przez stowarzyszenie ISACA

Specyficzna natura audytowania systemów informatycznych (SI), jak i umiejętności niezbędne do przeprowadzenia takich audytów, pociągają za sobą potrzebę istnienia standardów bezpośrednio odnoszących się do audytu informatycznego. Jednym z celów stowarzyszenia ISACA (Information Systems Audit and Control Association) jest rozwój międzynarodowych standardów mogących sprostać tym potrzebom. Opracowanie i upowszechnienie Standardów Audytowania SI są podstawowym wkładem Stowarzyszenia ISACA na rzecz społeczności audytorów.

Cele

Cele stawiane przed Standardami Audytowania SI ISACA to:

- Informowanie audytorów systemów informatycznych o minimalnym akceptowalnym poziomie świadczonych przez nich usług, niezbędnych do spełnienia wymagań stawianych przez Kodeks Etyki Zawodowej ISACA (ISACA Code for Professional Ethics for IS Auditors).
- Informowanie zarządów firm i innych zainteresowanych stron o poziomie oczekiwań w stosunku do pracy audytorów systemów informatycznych.

Celem Wytycznych i Procedur Audytowania SI jest dostarczenie dalszych informacji o tym, jak stosować się do Standardów Audytowania ISACA.

Zakres i moc prawna Standardów Audytowania SI

Zakres i moc prawna Standardów Audytowania SI

- **Standardy** definiują obowiązkowe wymagania wobec audytowania systemów informatycznych i sposobu raportowania.
- **Wytyczne** pomagają wdrożyć odpowiednie standardy. Audytor systemów informatycznych powinien wziąć je pod uwagę podczas wdrażania standardów, kierować się profesjonalizmem w ocenie sposobów ich wdrożenia i być gotowym do wyjaśnienia wszelkich odstępstw.
- **Procedury** dostarczają przykładów, na których może się wzorować audytor systemów informatycznych. Podczas określania czy dana procedura, grupa procedur lub test są odpowiednie, audytor SI powinien zastosować swój profesjonalny osąd do szczególnych okoliczności jakie stwarza określony system informatyczny lub środowisko technologiczne.

Słowo audyt używane jest zamiennie ze słowem przegląd.

Kodeks ISACA zobowiązuje członków ISACA i posiadaczy certyfikatów CISA, do stosowania się do standardów audytu informatycznego, zaakceptowanych przez ISACA.

Niestosowanie się do tych standardów będzie skutkowało dochodzeniami prowadzonymi przez zarząd ISACA, a w ostateczności krokami dyscyplinarnymi podejmowanymi wobec członków ISACA i posiadaczy certyfikatów CISA przez odpowiedni lokalny komitet.

Rozwój Standardów, Wytycznych i Procedur

Rada ISACA do spraw standardów jest na szeroką skalę zaangażowana w konsultacje związane z przygotowaniem standardów audytu systemów informatycznych. Przed opublikowaniem jakichkolwiek dokumentów, Rada do spraw standardów publikuje na forum międzynarodowym wyciągi z dokumentów by w ten sposób poddać je publicznej ocenie. Rada poszukuje również ludzi z odpowiednią wiedzą ekspercką, zainteresowanych udzielaniem konsultacji w zakresie definiowania standardów.

Rada ds. Standardów prowadzi ciągły program rozwojowy i zachęca do partycypowania w tego rodzaju programach członków ISACA i posiadaczy certyfikatów CISA, aby dokładniej zidentyfikować potrzeby, jakim mają sprostać standardy. Wszelkie sugestie prosimy kierować pod adres: research@isaca.org, faxem (+1.847.253.1443) lub na adres: ISACA's International Office for the attention of the Director of Research, Standards and Academic Relations, umieszczony na końcu tej broszury.

Indeks standardów i wytycznych audytowania SI

010 Statut audytu

010.010 Obowiązki, uprawnienia i odpowiedzialność

010.010.010 Prawa i powinności audytu - statut audytu
010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

020 Niezależność

020.010 Niezależność zawodowa

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

Zobacz także: 020.020.010 Powiązania organizacyjne i niezależność

020.020 Powiązania organizacyjne

020.020.010 Powiązania organizacyjne i niezależność
Zobacz także: 020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

030 Standardy i etyka zawodowa

030.010 Kodeks etyki zawodowej

030.010.010 Nieprawidłowości i akty bezprawne
Zobacz także: 030.020.020 Należyta staranność zawodowa

030.020 Należyta staranność zawodowa

030.020.010 Rozważania audytowe na temat nieprawidłowości
030.020.020 Należyta staranność zawodowa
Zobacz także: 060.020.070 Stosowanie technik komputerowego wspomaganie audytu

040 Kompetencje

040.010 Umiejętności i wiedza

040.020 Ustawiczne szkolenie zawodowe

050 Planowanie

050.010 Planowanie audytu

050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych
050.010.020 Planowanie
050.010.030 Ocena ryzyka podczas planowania audytu
050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji
Zobacz także: 030.020.010 Rozważania audytowe na temat nieprawidłowości i 060.020.070 Stosowanie technik komputerowego wspomaganie audytu

060 Wykonywanie prac audytowych

060.010 Nadzór

060.020 Dowody

060.020.010 Dokumentacja audytu
060.020.020 Przegląd systemów aplikacyjnych
060.020.030 Wymóg dowodów audytu
060.020.040 Próbkiowanie audytowe
060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)
060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI
060.020.070 Stosowanie technik komputerowego wspomaganie audytu
060.020.080 Wykorzystanie prac innych audytorów i ekspertów
Zobacz także: 030.020.010 Rozważania audytowe na temat nieprawidłowości i 050.010.030 Ocena ryzyka podczas planowania audytu

070 Raportowanie

070.010 Forma i zawartość raportu

070.010.010 Raportowanie
Zobacz także: 060.020.010 Dokumentacja audytu i 030.020.010 Rozważania audytowe na temat nieprawidłowości

080 Dalszy ciąg działań

080.010 Dalszy ciąg działań

Indeks procedur audytowania SI

1 Ocena ryzyka systemów informatycznych, obowiązuje od 1 czerwca 2002
2 Podpisy cyfrowe, obowiązuje od 1 czerwca 2002

Standardy Audytowania Systemów Informatycznych

Wydane przez Information Systems Audit and Control Association (Stowarzyszenie do spraw audytu i kontroli systemów informatycznych)

010 Statut audytu

010.010 Obowiązki, uprawnienia i odpowiedzialność

Obowiązki, uprawnienia i odpowiedzialność funkcji audytu systemów informatycznych mają być odpowiednio udokumentowane w statucie audytu lub w umowie - zleceniu na przeprowadzenie prac audytowych.

020 Niezależność

020.010 Niezależność zawodowa

We wszystkich sprawach związanych z prowadzeniem audytów, audytor systemów informatycznych musi być niezależny od audytowanej strony, zarówno, jeśli chodzi o postawę wewnętrzną, jak i wizerunek publiczny.

020.020 Powiązania organizacyjne

Funkcja audytu systemów informatycznych musi być wystarczająco niezależna od audytowanego obszaru, aby umożliwić obiektywne przeprowadzenie audytu.

030 Standardy i etyka zawodowa

030.010 Kodeks etyki zawodowej

Audytor systemów informatycznych jest zobowiązany do stosowania się do Kodeksu Etyki Zawodowej Stowarzyszenia do spraw audytu i kontroli systemów informatycznych (ISACA - Information Systems Audit and Control Association).

030.020 Należyta staranność zawodowa

We wszelkich aspektach pracy Audytora Systemów Informatycznych obowiązuje należyta staranność zawodowa oraz przestrzeganie odpowiednich standardów audytowania.

040 Kompetencje

040.010 Umiejętności i wiedza

Audytor systemów informatycznych ma być kompetentny w zagadnieniach technicznych, posiadając równocześnie umiejętności i wiedzę niezbędne do wykonywania pracy audytorskiej.

040.020 Ustawiczne szkolenie zawodowe

Audytor systemów informatycznych jest zobowiązany utrzymywać na odpowiednim poziomie swoje kompetencje dotyczące zagadnień technicznych poprzez właściwe i ustawiczne szkolenie zawodowe.

050 Planowanie

050.010 Planowanie audytu

Audytor systemów informatycznych ma planować prace związane z audytem systemów informatycznych pod kątem realizacji celów audytu oraz zgodnie z odpowiednimi standardami audytowania.

060 Wykonywanie prac audytowych

060.010 Nadzór

Personel zajmujący się audytem systemów informatycznych ma podlegać odpowiedniemu nadzorowi, w celu zapewnienia, że zostaną spełnione cele audytu oraz odpowiednie standardy zawodowe audytu.

060.020 Dowody

Podczas przeprowadzania audytu, audytor systemów informatycznych zobowiązany jest uzyskać wystarczające, wiarygodne, stosowne i użyteczne dowody, tak, aby skutecznie zrealizować cele audytu. Spostrzeżenia i wnioski z audytu mają być poparte odpowiednią analizą i interpretacją tychże dowodów.

070 Raportowanie

070.010 Forma i zawartość raportu

Zadaniem audytora systemów informatycznych jest dostarczenie określonym odbiorcom raportu w odpowiedniej postaci z wykonania prac audytowych. Raport z audytu ma przedstawiać zakres, cele, okres oraz rodzaj i obszar wykonanych prac audytowych. Raport ma wskazywać organizację, planowanych odbiorców raportu oraz wszelkie zastrzeżenia, co do jego obiegu. Raport ma przedstawiać spostrzeżenia, wnioski i rekomendacje oraz wszelkie zastrzeżenia lub uwarunkowania audytora względem audytu.

080 Dalszy ciąg działań

080.010 Dalszy ciąg działań

Audytor systemów informatycznych zobowiązany jest domagać się odpowiednich informacji o wcześniejszych spostrzeżeniach, wnioskach i rekomendacjach audytowych, a następnie dokonać ich oceny, w celu określenia, czy zostały na czas podjęte właściwe działania.

DATA OBOWIĄZYWANIA

Powyższe standardy obowiązują w stosunku do wszystkich audytów systemów informatycznych rozpoczynających się począwszy od dnia 25 lipca 1997r.

Wytyczne audytowania SI

Alfabetyczny spis wytycznych audytowania

060.020.020 Przegląd systemów aplikacyjnych
060.020.010 Dokumentacja audytu
060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)
030.020.020 Należyta staranność zawodowa
030.010.010 Nieprawidłowości i akty bezprawne
050.010.030 Ocena ryzyka podczas planowania audytu
010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji
050.010.020 Planowanie
050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych
020.020.010 Powiązania organizacyjne i niezależność
010.010.010 Prawa i powinności audytu - statut audytu
060.020.040 Próbkowanie audytowe
070.010.010 Raportowanie
030.020.010 Rozważania audytowe na temat nieprawidłowości
060.020.070 Stosowanie technik komputerowego wspomaganie audytu
060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI
020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI
050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji
060.020.080 Wykorzystanie prac innych audytorów i ekspertów
060.020.030 Wymóg dowodów audytu

Spis wytycznych audytowania według daty wydania

060.020.080 Wykorzystanie prac innych audytorów i ekspertów	1 lutego 1998
060.020.030 Wymóg dowodów audytu	19 czerwca 1998
070.010.010 Raportowanie	19 czerwca 1998
060.020.070 Stosowanie technik komputerowego wspomaganie audytu	19 czerwca 1998
010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji	1 maja 1999
010.010.010 Prawa i powinności audytu - statut audytu	1 maja 1999
050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych	1 maja 1999
030.020.020 Należyta staranność zawodowa	1 maja 1999
060.020.010 Dokumentacja audytu	1 maja 1999
030.020.010 Rozważania audytowe na temat nieprawidłowości	1 listopada 1999
060.020.040 Próbkowanie audytowe	1 listopada 1999
060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI	1 listopada 1999
020.020.010 Powiązania organizacyjne i niezależność	1 września 2000
050.010.030 Ocena ryzyka podczas planowania audytu	1 września 2000
060.020.020 Przegląd systemów aplikacyjnych	1 sierpnia 2001
050.010.020 Planowanie	1 listopada 2001
050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji	1 listopada 2001
020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI	1 kwietnia 2002
060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)	1 kwietnia 2002
030.010.010 Nieprawidłowości i akty bezprawne	1 kwietnia 2002

010.010.010 Prawa i powinności audytu - statut audytu

1. PODSTAWA

1.1 Powiązanie ze standardami

1.1.1 Standard 010.010 (Obowiązki, uprawnienia i odpowiedzialność) stwierdza, że "Obowiązki, uprawnienia i odpowiedzialność funkcji audytu systemów informatycznych mają być odpowiednio udokumentowane w statucie audytu lub w umowie – zleceniu na przeprowadzenie prac audytowych."

1.2 Potrzeba Wytycznej

1.2.1 Celem poniższej Wytycznej jest pomoc Audytorowi Systemów Informatycznych (SI) w przygotowaniu statutu audytu, tak by określone zostały obowiązki, uprawnienia i odpowiedzialność obszaru funkcji związanej z audytem SI. Wytyczna ta dotyczy w pierwszej mierze Wewnętrznego Audytu SI, jednakże niektóre jej aspekty mogą być brane pod uwagę również w innych przypadkach.

1.2.2 Niniejsza Wytyczna dostarcza wskazówek, jak wdrażać standardy audytowania SI. Audytor SI powinien wziąć ją pod uwagę określając sposób wdrożenia powyższego Standardu, powinien posłużyć się swoim profesjonalnym osądem podczas jej stosowania i być gotowym uzasadnić każde od niej odstępstwo.

2. UREGULOWANIE PRAW I POWINNOŚCI AUDYTU - STATUT AUDYTU

2.1 Pełnomocnictwo

2.1.1 Audytor SI powinien posiadać wyraźne pełnomocnictwo do wykonywania funkcji audytu SI. Pełnomocnictwo to jest zwykle wyrażone w statucie audytu, który powinien być formalnie przyjęty. W przypadkach, gdy statut audytu istnieje dla całości obszaru audytu w organizacji, to w sytuacjach, gdy jest to możliwe, powinno być również dołączone pełnomocnictwo dla audytu SI.

2.2 Treść Statutu Audytu

2.2.1 Statut audytu powinien wyraźnie odnosić się do następujących trzech aspektów: obowiązków, uprawnień oraz odpowiedzialności.

2.2.2 Obowiązki:

- Misja (deklaracja misji),
- Plany (zamierzenia) i cele,
- Zakres (działania),
- Zadania,
- Niezależność,
- Relacje wzajemne z audytem zewnętrznym,
- Wymagania komórek (stron) audytowanych,
- Krytyczne czynniki sukcesu,
- Kluczowe wskaźniki wydajności,
- Inne miary wydajności.

2.2.3 Uprawnienia:

- Analiza ryzyka,
- Prawo dostępu do informacji, personelu, pomieszczeń oraz systemów, właściwych w celu przeprowadzania audytów,
- Zakres uprawnień oraz jego ograniczenia,
- Obszary (funkcjonowania organizacji), które mają być audytowane,
- Oczekiwania stron (komórek) audytowanych,
- Struktura organizacyjna, włączając w to ścieżki raportowania do Zarządu i wyższego kierownictwa,
- Struktura i hierarchia personelu audytu SI.

2.2.4 Odpowiedzialność (rozliczanie prac):

- Ścieżka raportowania do wyższego kierownictwa,
- Ocena realizacji zadań,
- Ocena wydajności personelu,
- Obsadzanie stanowisk/ możliwości rozwoju zawodowego i awansu,
- Prawa stron (komórek) audytowanych,
- Niezależne przeglądy jakości,
- Ocena zgodności ze standardami,
- Wydajność i rola badań porównawczych,
- Ocena wykonania planu audytu,
- Porównanie budżetu w stosunku do kosztów rzeczywistych,
- Uzgodnione działania, np. kary, w przypadku, gdy którakolwiek ze stron nie wykona swoich obowiązków.

2.3 Komunikacja (komunikowanie się) z audytowanymi stronami (komórkami)

2.3.1 Efektywna komunikacja ze stronami audytowanymi obejmuje wzięcie pod uwagę następujących kwestii:

- Opisanie usług, ich zakresu, dostępności oraz zgodności z terminarzem (ich dostarczania),
- Dostarczenie kosztorysów lub budżetów, jeśli są dostępne,
- Opisanie problemów oraz ich możliwych rozwiązań,
- Zapewnienie odpowiednich i natychmiast dostępnych sposobów i narzędzi dla skutecznej komunikacji,

- Określenie powiązania (korelacji) między oferowaną usługą a potrzebami audytowanych stron (komórek).

2.3.1 Statut audytu stwarza solidne podstawy dla komunikacji z komórkami (stronami) audytowanymi i powinien obejmować odwołania do umów dotyczących poziomu usług w sprawach takich, jak:

- Dostępność dla niezaplanowanych prac,
- Dostarczanie raportów,
- Koszty,
- Reagowanie na reklamacje komórek (stron) audytowanych,
- Jakość usług,
- Badanie wydajności,
- Komunikacja z komórkami (stronami) audytowanymi,
- Szacowanie potrzeb,
- Samoocena ryzyka kontrolnego,
- Porozumienie odnośnie zakresów działań (zasięgów) audytów,
- Proces raportowania,
- Uzgadnianie i potwierdzanie wykryć.

2.4 Proces zapewnienia jakości

2.4.1 Audytor SI powinien rozważyć ustanowienie procesu zapewnienia jakości (np. wywiady, badanie zadowolenia klientów, badanie wykonania zadań, itp.) w celu zrozumienia potrzeb i oczekiwań stron (komórek) audytowanych wobec audytu SI. Potrzeby te powinny podlegać ocenie w porównaniu do statutu, mając na względzie poprawę świadczonych usług, ewentualnie zmianę dostarczania usług lub statutu audytu, jeśli byłoby to uznane za konieczne..

3. UMOWA – ZLECENIE (NA PRZEPROWADZENIE AUDYTU)

3.1 Cel umowy - zlecenia

3.1.1 Umowy – zlecenia na przeprowadzenie audytu są często stosowane w przypadku zleceń jednorazowych lub dla ustalenia zakresu oraz celów relacji wzajemnych między zewnętrznym Audytem SI a daną organizacją..

3.2 Treść umowy - zlecenia

3.2.1 Umowa – zlecenie na realizację powinna jasno odnosić się do poniższych trzech aspektów : obowiązków, uprawnień oraz odpowiedzialności (rozliczania). Aspekty te nakreślone są w dalszych punktach..

3.2.2 Obowiązki:

- Zakres,
- Zadania,
- Niezależność,
- Szacowanie ryzyka,
- Szczególne wymagania komórek (stron) audytowanych,
- Raporty i inne produkty, składniki, które mają być dostarczone.

3.2.3 Uprawnienia:

- Prawo dostępu do informacji, personelu, pomieszczeń (lokalizacji) oraz systemów, właściwych, aby móc wykonać zleczone zadania,
- Zakres uprawnień i dowolne ograniczenia zakresu,
- Dowody potwierdzające uzgodnienie warunków i zapisów umowy

3.2.4 Odpowiedzialność (rozliczanie wykonania prac):

- Planowani odbiorcy raportów,
- Prawa stron (komórek) audytowanych,
- Badania (przeeglądy) jakości,
- Uzgodnione daty ukończenia prac,
- Uzgodnione budżety/ honoraria, jeśli są dostępne.

4. DATA OBOWIĄZYWANIA

4.1 Powyższa Wytyczna obowiązuje wszystkie audyty systemów informatycznych rozpoczynające się w dniu 1 sierpnia 1999 lub później.

010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

- 1.1.1** Standard 010.010 (Obowiązki, Uprawnienia i Odpowiedzialność) stanowi, że „Obowiązki, uprawnienia i odpowiedzialność obszaru działalności związanego z audytem systemów informatycznych mają być odpowiednio udokumentowane w regulacjach (statucie) dotyczących audytu lub w umowie na jego realizację”.
- 1.1.2** Standard 050.010 (Planowanie Audytu) stanowi, że „Audytor Systemów Informatycznych ma tak zaplanować prace podczas audytu systemów informatycznych, aby uwzględnić cele audytu i zastosować się do odpowiednich profesjonalnych standardów audytu”.
- 1.1.3** Standard 060.020 (Dowody) stanowi, że "Podczas przeprowadzania audytu Audytor Systemów Informatycznych (Audytor SI) zobowiązany jest uzyskać wystarczające, wiarygodne, odpowiednie (relevantne) i użyteczne dowody, aby efektywnie zrealizować cele audytu. Wyniki (stwierdzenia) i wnioski z audytu mają być poparte odpowiednią analizą i interpretacją tych dowodów”.

1.2 Potrzeba Wytycznej

- 1.2.1** Dana organizacja (użytkownik usług) może częściowo lub w pełni delegować (przekazać) fragment lub całość swoich operacji związanych z systemami informatycznymi zewnętrznemu dostawcy tego typu usług (usługodawcy). Operacje informatyczne, które mogą podlegać outsourcingowi obejmują takie funkcje obszaru IT jak: eksploatacja centrum przetwarzania danych, zapewnienie bezpieczeństwa oraz rozwój i utrzymanie systemów użytkowych (aplikacji)..
- 1.2.2** Odpowiedzialność za potwierdzenie zgodności z umowami, porozumieniami i przepisami pozostaje po stronie użytkownika usług.
- 1.2.3** Prawo do przeprowadzania audytu często jest niejasne. Odpowiedzialność za zgodność audytowania (z umowami i regulacjami) jest również często niejasna. Celem tej Wytycznej jest wyznaczenie, jak w tego typu sytuacjach Audytor SI powinien przestrzegać Standardów 010.010, 050.010 oraz 060.020..
- 1.2.4** Prezentowana Wytyczna dostarcza wskazówek, w jaki sposób stosować standardy audytowania systemów informatycznych. Audytor SI powinien uwzględnić ją podczas określania sposobu wdrożenia wyżej wymienionych Standardów, powinien posłużyć się profesjonalnym osądem w czasie jej wdrażania oraz być przygotowanym do uzasadnienia każdego od niej odstępstwa.

2. REGULACJE (STATUT) DOTYCZĄCE AUDYTU

2.1 Obowiązki, Uprawnienia i Odpowiedzialność

- 2.1.1** Tam gdzie jakikolwiek aspekt obszaru funkcjonalnego IT (systemów informatycznych) został przekazany usługodawcy zewnętrznemu, usługi te powinny być objęte regulacjami audytu..
- 2.1.2** Regulacje dotyczące audytu powinny explicitie określać prawo Audytora SI do:
 - Przeglądu porozumień między użytkownikiem usług a usługodawcą (przed wejściem w życie i po wejściu w życie),
 - Prowadzenia takich prac audytowych, jakie zostaną uznane za konieczne wobec przekazanych na zewnątrz usług obszaru IT,
 - Raportowania wyników, wniosków i rekomendacji kierownictwu użytkownika usług.

3. PLANOWANIE

3.1 Stwierdzanie Stanu Rzeczy

- 3.1.1** Audytor SI powinien posiadać zrozumienie natury, terminarza, oraz zakresu przekazanych na zewnątrz usług.
- 3.1.2** Audytor SI powinien ustalić jakie mechanizmy kontrolne użytkownik usług wdrożył, aby uwzględnić wymagania biznesowe „w celu zapewnienia, że role i obowiązki stron trzecich są jasno określone, dotrzymywane i nie przestają spełniać wymagań (COBIT, Ogólny Cel Kontrolny DS2).
- 3.1.3** Ryzyko związane z przekazanymi na zewnątrz usługami powinno być zidentyfikowane i oszacowane.
- 3.1.4** Audytor SI powinien oszacować stopień do jakiego mechanizmy kontrolne użytkownika usług dostarczają rozsądnego zapewnienia, że cele biznesowe będą osiągnięte, oraz że zapobiegnie się niepożądanym sytuacjom lub że będą one wykrywane i korygowane.
- 3.1.5** Audytor SI powinien ustalić stopień w jakim porozumienie o outsourcingu zapewnia przeprowadzanie audytu usługodawcy, oraz powinien rozważyć, czy to zapewnienie jest wystarczające. Obejmuje to ocenę możliwości polegania na audytach przeprowadzanych przez audytorów wewnętrznych usługodawcy albo przez niezależną stronę trzecią na podstawie umowy zawartej przez usługodawcę..

3.2 Planowanie

- 3.2.1** Audytor SI powinien wziąć pod uwagę uzyskanie odpowiednich porad prawnych od ekspertów..
- 3.2.2** Audytor SI powinien ocenić przygotowane dla usługodawcy raporty z uprzednio przeprowadzonych audytów, i tak zaplanować audyt systemów informatycznych, aby objąć cele audytu związane ze środowiskiem usługodawcy, biorąc pod uwagę

- informacje uzyskane podczas planowania.
- 3.2.3** Cele audytu powinny być uzgodnione z kierownictwem użytkownika usług zanim zostaną zakomunikowane usługodawcy. Dowolne zmiany jakich zażyczy sobie usługodawca powinny zostać uzgodnione z kierownictwem użytkownika usług..
- 3.2.4** Audytor SI powinien tak planować prace audytowe systemów informatycznych, aby uczynić zadość stosownym standardom profesjonalnego audytu, tak samo, jak gdyby audyt miał być przeprowadzony we własnym środowisku użytkownika usług..
- 4. PRZEPROWADZANIE PRAC AUDYTOWYCH**
- 4.1 Wymóg dowodów audytu**
- 4.1.1** Audyt powinien być przeprowadzony tak samo, jak gdyby usługi świadczone były we własnym środowisku użytkownika usług..
- 4.2 Umowa z usługodawcą**
- 4.2.1** Audytor SI powinien wziąć pod uwagę takie kwestie jak:
- Istnienie formalnego porozumienia pomiędzy usługodawcą a użytkownikiem usług,
 - Włączenie do umowy outsourcingowej klauzuli, która będzie wyraźnie stanowiła, że usługodawca jest zobowiązany do spełnienia wszystkich wymagań prawnych, mających zastosowanie do jego działalności, oraz do stosowania się do aktów prawnych i przepisów dotyczących działań (funkcji), które powinien podjąć w imieniu użytkownika usług,
 - Zastrzeżenie w umowie outsourcingowej, że działalność prowadzona przez usługodawcę podlega kontroli i audytom tak samo, jak byłaby ona prowadzona samodzielnie przez użytkownika usług,
 - Uwzględnienie w porozumieniu z usługodawcą praw dostępu niezbędnych podczas audytów,
 - Istnienie Umów dotyczących Poziomu Usług (ang. skrót SLAs) wraz z procedurami monitorowania wydajności,
 - Stosowanie się do polityk bezpieczeństwa użytkownika usług,
 - Adekwatność kroków podejmowanych w celu ubezpieczenia się na wypadek nieojalności usługodawcy,
 - Adekwatność polityk i procedur usługodawcy dotyczących personelu.
- 4.3 Zarządzanie usługami przekazanymi na zewnątrz**
- 4.3.1** Audytor SI powinien zweryfikować, że:
- Procesy biznesowe mające tworzyć informacje wykorzystywane do monitorowania zgodności z Umowami dotyczącymi Poziomu Usług (ang. skrót SLAs) są odpowiednio kontrolowane,
 - W tych przypadkach, gdy Umowy dotyczące Poziomu Usług (ang. skrót SLAs) nie są spełniane, użytkownik usług poszukuje środków zapobiegawczych i rozpatruje działania korygujące w celu osiągnięcia uzgodnionego poziomu usług,
 - Użytkownik usług posiada zdolność i możliwość do ciągłego przeglądania i oceniania dostarczanych usług.
- 4.4 Ograniczenia co do Zakresu**
- 4.4.1** W tych przypadkach, kiedy usługodawca nie wykazuje chęci do współpracy z Audytorem SI, Audytor powinien zaraportować ten fakt kierownictwu użytkownika usług..
- 5. RAPORTOWANIE**
- 5.1 Publikowanie i Uzgodnienie Raportu**
- 5.1.1** Po zakończeniu prac audytowych Audytor SI powinien dostarczyć raport w odpowiedniej formie zamierzonym odbiorcom po stronie użytkownika usług..
- 5.1.2** Audytor SI powinien rozważyć przedyskutowanie raportu z usługodawcą przed jego opublikowaniem, ale Audytor SI nie powinien być odpowiedzialny za udostępnienie usługodawcy raportu końcowego. Jeśli usługodawca ma otrzymać kopię, zwykle powinno to wynikać z inicjatywy kierownictwa użytkownika usług..
- 5.1.3** Raport powinien dokładnie określać wszelkie ograniczenia, co do dystrybucji, jakie Audytor SI i kierownictwo użytkownika usług zgodzili się nałożyć. Na przykład, usługodawca nie powinien móc dostarczać kopii raportu innym użytkownikom swoich usług bez zezwolenia macierzystej organizacji Audytora SI, i tam gdzie to właściwe, bez zezwolenia użytkownika usług. Audytor SI powinien również rozważyć uwzględnienie klauzuli o wyłączeniu odpowiedzialności wobec stron trzecich..
- 5.2 Ograniczenia co do Zakresu**
- 5.2.1** Raport z audytu powinien jasno identyfikować ograniczenia dotyczące zakresu (audytu), w tych przypadkach, gdy podczas audytu odmówione zostało prawo dostępu oraz powinien wyjaśnić wpływ tych ograniczeń na audyt..
- 6. DALSZE DZIAŁANIA**
- 6.1 Wyniki Poprzednich Audytów**
- 6.1.1** Tak samo, jak w przypadku, gdyby audyt przeprowadzany był w środowisku własnym użytkownika usług, Audytor SI powinien poprosić o odpowiednie informacje, zarówno od użytkownika usług jak i usługodawcy, dotyczące uprzednich, odpowiednio powiązanych wyników (audytów) : stwierdzeń, wniosków i rekomendacji. Audytor SI powinien określić, czy zostały przez usługodawcę wdrożone we właściwym czasie odpowiednie działania korygujące..
- 7. OBOWIĄZYWANIE**

7.1 Powyższa wytyczna obowiązuje wszystkie audyty systemów informatycznych rozpoczynające się począwszy od 1 września 1999.

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

1. INFORMACJE OGÓLNE

1.1 Powiązania ze standardami

1.1.1 Standard 020.010 (Niezależność zawodowa) stwierdza, "We wszystkich sprawach związanych z prowadzeniem audytów, audytor systemów informatycznych musi być niezależny od audytowanej strony, zarówno jeśli chodzi o postawę wewnętrzną, jak i wizerunek publiczny."

1.1.2 Standard 020.020 (Powiązania organizacyjne) stwierdza, "Funkcja audytu systemów informatycznych musi być wystarczająco niezależna od audytowanego obszaru, aby umożliwić obiektywne przeprowadzenie audytu."

1.2 Potrzeba wytycznej

1.2.1 W wielu organizacjach, oczekiwaniem kierownictwa, zespołu SI oraz wewnętrznego audytu jest by audytorzy SI mogli zostać zaangażowani w zadania nieaudytowe takie jak:

- Definiowanie strategii SI odnośnie takich obszarów jak technologia, aplikacje i zasoby
- Ocena, wybór i wdrożenie technologii
- Ocena, wybór, dopasowanie do oczekiwań klienta oraz wdrożenie aplikacji i rozwiązań SI pochodzących od strony trzeciej
- Projektowanie, rozwój i wdrożenie aplikacji i rozwiązań SI zbudowanych na zamówienie klienta
- Ustanowienie najlepszych praktyk, polityk i procedur odnoszących się do różnych funkcji SI
- Projektowanie, rozwój i wdrożenie środków bezpieczeństwa i kontroli

1.2.2 Zadanie nieaudytowe, generalnie rzecz biorąc, wymaga udziału w inicjatywach SI i zespołach projektowych SI, w charakterze roboczym i/ lub w charakterze doradcy/konsultanta na całym etapie lub na części etatu. Przykładowo:

- Tymczasowe przydzielenie lub wypożyczenie na pełny etat pracowników audytu SI do zespołu projektu SI
- Przydzielenie na część etatu pracowników audytu SI do różnych struktur projektowych takich jak grupa sterująca projektem, grupa robocza projektu, zespół oceniający, zespół umów i negocjacji, zespół wdrożeniowy, zespół ds. zapewnienia jakości oraz zespół zajmujący się problemami
- Działania jako niezależny doradca lub dokonujący przeglądu na zasadzie ad hoc

1.2.3 Takie nieaudytowe zadania stanowią ważną część wkładu audytora SI w edukację i szkolenie pozostałych członków organizacji. Umożliwiają audytorom SI wykorzystanie specjalistycznych umiejętności i wiedzy o organizacji, dostarczają wyjątkowy i cenny wkład w efektywność i skuteczność inwestycji SI. Wpływają również na wzrost rangi audytu SI i dają pracownikom audytu SI cenne praktyczne doświadczenie.

1.2.4 Tam, gdzie audytor został zaangażowany w zadanie nieaudytowe w pewną inicjatywę SI, a prowadzony jest później/lub w tym samym czasie audyt tej inicjatywy lub związanych z nią funkcji SI, rekomendacje i wnioski powstałe w wyniku tego audytu mogą być postrzegane przez odbiorców jako nieobiektywne.

1.2.5 Celem tej wytycznej jest dostarczyć strukturę ramową by audytor był w stanie:

- Ustalić kiedy wymagana niezależność może być lub może wydawać się być osłabiona
- Rozważyć potencjalne, alternatywne podejścia do procesu audytowego, gdy wymagana niezależność jest lub może wydawać się być osłabiona
- Określić ujawnione wymagania

2. CHARAKTER AUDYTU

2.1 Warunki nieaudytowego zaangażowania audytorów SI

2.1.1 Charakter audytu powinien ustalić mandat dla audytora SI, który ma być zaangażowany w zadania nieaudytowe oraz ogólną istotę, harmonogram i zasięg tych zadań. Pozwoli to na uniknięcie potrzeby uzyskiwania określonego mandatu za każdym razem.

2.1.2 Audytor SI powinien dostarczyć rozsądnych gwarancji, że specyfikacja warunków (TOR = Terms of Reference), określonych nieaudytowych zadań, jest dostosowana do charakteru audytu. Tam, gdzie występują jakieś odstępstwa/ odchylenia, takie same powinny zostać wyraźnie oznaczone/ opisane w TOR.

3. NIEZALEŻNOŚĆ

3.1 Znaczenie niezależności w zadaniach nieaudytowych

3.1.1 Standard audytu 020.010 wymaga, aby auditor SI był niezależny “we wszystkich sprawach odnoszących się do audytu...” O ile nie zabraniają tego inne zewnętrzne standardy, nie istnieje żadne wymaganie dla audytora SI zarówno by być lub być postrzeganym, że się jest niezależnym tam gdzie istota zaangażowania w inicjatywę SI jest jednym z nieaudytowych zadań jak powyżej w punkcie 1.2.1.

3.1.2 Chociaż nie ma potrzeby, aby auditor SI był niezależny podczas prowadzenia powyższych zadań obiektywizm jest wciąż jeszcze profesjonalnym wymogiem. Auditor SI powinien odnoszących się do nieaudytowej roli w przedmiocie/celu i racjonalnym zachowaniu bez uprzedzeń.

3.1.3 Pomimo że nie istnieje wymóg by auditor SI był niezależny podczas wykonywania zadania nieaudytowego w inicjatywie SI, powinien rozważyć, czy jeśli taka rola mogłaby być uznana za osłabienie niezależności, powinien zostać przydzielony do danej inicjatywy SI lub do powiązanej z nią funkcji. Tam, gdzie jest przewidywalny taki konflikt – na przykład tam gdzie później będzie potrzebny niezależny audyt oraz tam gdzie jest tylko jeden audytor z wymaganymi umiejętnościami do prowadzenia zarówno zadania nieaudytowego oraz późniejszego audytu – audytor SI powinien przedyskutować tę kwestię z komitetem audytowym lub ekwiwalentnym ciałem zarządczym przed podjęciem nieaudytowego zadania.

3.1.4 Rozważenie kompromisu pomiędzy zadaniem nieaudytowym w inicjatywie SI i niezależnym audytem tejże inicjatywy lub powiązanych z nią funkcji powinna być decyzją komitetu audytowego lub ekwiwalentnego ciała zarządczego. Aspekty, które prawdopodobnie wpływają na tę decyzję zawierają:

- Potencjalne alternatywne zasoby dla obu zadań
- Zrozumienie względnej wartości dodanej przez sprzeczne działania
- Potencjał kształcenia zespołu SI, aby przyszłe inicjatywy mogły przynieść korzyść
- Możliwości rozwoju kariery i planowania następców dla audytora SI
- Poziom ryzyka związanego z zdaniem nieaudytowym
- Skutek dla wizerunku, obrazu, image'u itp. funkcji audytu SI
- Skutek decyzji na wymagania audytorów zewnętrznych lub organów nadzorczych jeśli takie są
- Warunki wynajęcia audytora SI

3.2 Skutek nieaudytowych zadań na późniejsze audyty

3.2.1 Gdy inicjatywa SI lub funkcja jest audytowana według wymagań regulacyjnych lub kierownictwa, audytor SI powinien być niezależny od zespołu SI i jego kierownictwa i tak być postrzegany.

3.2.2 Nieaudytowe zaangażowanie audytora w inicjatywę SI może potencjalnie osłabić niezależność audytora SI w odniesieniu do audytu inicjatywy SI lub powiązanych funkcji. Auditor SI powinien stwierdzić czy w jego/jej opinii niezależność podczas prowadzenia audytu jest osłabiona przez jego/jej nieaudytową rolę. Komitet Audytu lub ekwiwalentnego ciała zarządczego powinien być poproszony o zgodzenie się w formie pisemnej z tą opinią.

3.2.3 Krytyczne czynniki, które mogłyby pomóc w określeniu, czy niezależność audytora w odniesieniu do audytu mogłaby być osłabiona przez jego nieaudytową rolę obejmuje takie aspekty jak:

- Istota, harmonogram i zakres nieaudytowego zadania audytora SI w inicjatywie lub w funkcji SI, której audyt jest rozważany
- Istnienie faktów, które mogą być widziane jako zachwianie niezależności. Są to takie aspekty jak: dodatkowe korzyści materialne (bonusy) lub kary związane z zadaniem nieaudytowym
- Umiejętności jak również zobowiązanie audytora SI, że pozostanie bezstronnym podczas przeprowadzenia audytu i raportowania o słabościach lub błędach pomimo zaangażowania w zadanie nieaudytowe
- Swoboda audytora SI w określeniu zakresu i prowadzeniu audytu pomimo zaangażowania w zadanie nieaudytowe
- Ujawnienie przez audytora SI swojej nieaudytowej roli, poziomu zaangażowania oraz istotnych faktów z tym związanych

4. PLANOWANIE

4.1 Wpływ na niezależność

4.1.1 Potencjalny wpływ zadania nieaudytowego na niezależność w nawiązaniu do prawdopodobnego przyszłego/jednocześnie prowadzonego audytu tej samej inicjatywy SI lub związanych z nią funkcji powinien być ocenione podczas planowania nieaudytowego zadania.

4.1.2 Potencjalny wpływ jakiegokolwiek wcześniejszego lub toczącego się nieaudytowego zadania w każdej inicjatywie SI na niezależność powinna być oceniana podczas planowania audytów każdej z takich inicjatyw i lub powiązanych z nimi funkcji.

4.1.3 Jak wspomniano w punktach 3.1.3 i 3.2.2 komitet audytowy albo ekwiwalentne ciało zarządzające powinno być informowane o potencjalnym osłabieniu niezależności w sytuacjach wspomnianych w punktach 4.1.1 i 4.1.2. Podczas informowania komitetu audytowego lub ekwiwalentnego ciała zarządzającego o potencjalnym osłabieniu niezależności, audytor SI powinien zalecić działania, które mogą być podjęte aby zapewnić rozsądne zabezpieczenie niezależności i obiektywności, które mogą zawierać:

- Przydzielenie dodatkowego kierownictwa oraz /lub personelu z wewnątrz funkcji SI, którzy nie pełnią żadnej nieaudytowej roli w obszarze podlegającym audytowi, by zastąpić audytora SI, który wykonuje/wykonywał zadanie nieaudytowe.
- Przydzielenie kierownictwa i personelu spoza funkcji audytu SI takie jak pożyczanie pracowników z innej funkcji, oddziału, zewnętrznej organizacji itd. w celu zastąpienia audytora SI, który wykonuje/wykonywał zadanie nieaudytowe.
- Przydzielenie niezależnych zasobów z wewnątrz funkcji audytu SI lub innych źródeł wspomnianych wyżej żeby poprowadzić równorzędny audyt i działać jako niezależny arbiter podczas planowania, pracy i raportowania.

5. REALIZACJA PRACY AUDYTOWEJ

5.1 Monitorowanie Prowadzenia Audytu

- 5.1.1** W przypadku audytu, gdzie istnieje możliwość osłabienia niezależności spowodowana nieaudytowym zaangażowaniem, kierownictwo audytu SI powinno dokładnie monitorować jego prowadzenie. Każdy materialny sygnał o naruszeniu niezależności, który wynika nieaudytowego zaangażowania powinien zostać krytycznie oceniony przez kierownictwo audytu SI i powinny zostać wprowadzone niezbędne działania naprawcze. W takich przypadkach komitet audytu lub ekwiwalentne ciało zarządzające powinno zostać powiadomione.

6. RAPORTOWANIE

6.1 Wymagania ujawnienia

- 6.1.1** Tam, gdzie niezależność kierownictwa SI oraz/ lub personelu podczas audytowania inicjatywy SI i/ lub związanej z nią funkcji może być osłabiona przez rolę nieaudytową w tym przedsięwzięciu lub może tak być postrzegana, audytor SI powinien ujawnić w raporcie audytowym, odpowiednią informację dotyczącą swojej nieaudytowej roli jak również działań podjętych w celu zagwarantowania obiektywności. Umożliwi to użytkownikom raportu audytowego zrozumieć prawdopodobny zakres osłabienia niezależności jeśli taki jest, oraz środki podjęte w celu osłabienia jego wpływu. Informacja, że audytor SI powinien rozważyć ujawnienie zawiera aspekty takie jak:

- Nazwiska i staż/starszeństwo kierownictwa audytu SI i personelu zaangażowanego w nieaudytowe zadanie inicjatywy SI
- Istota, harmonogram i zakres ich nieaudytowego zaangażowania w inicjatywę SI
- Przyczyny ich zaangażowania w zadanie nieaudytowe inicjatywy SI, jak również audyt tej inicjatywy lub powiązanych z nią funkcji
- Kroki podjęte w celu zapewnienia, że obiektywność nie została istotnie osłabiona w ciągu prac audytowych i procesu raportowania
- Fakt, że na potencjalne osłabienie niezależności została zwrócona uwaga komitetu audytowego lub ekwiwalentnego ciała zarządzającego i uzyskano ich zgodę przed podjęciem się nieaudytowego zadania

7. DATA WEJŚCIA W ŻYCIE

- 7.1** Powyższe standardy obowiązują w stosunku do wszystkich audytów systemów informatycznych rozpoczynających się począwszy od dnia 1 lipca 2002 r.

020.020.010 Powiązania organizacyjne i niezależność

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

- 1.1.1** Standard 020.010 (Zawodowa niezależność) stwierdza, że : „We wszystkich sprawach związanych z audytem, audytor systemów informatycznych musi być niezależny od poddawanych audytowi, zarówno co do stanowiska jak i postępowania”
- 1.1.2** Standard 020.020 (Powiązania organizacyjne) stanowi: „Funkcja audytu Systemów Informatycznych musi być wystarczająco niezależna od audytowanego obszaru, aby umożliwić obiektywne prowadzenie audytu”
- 1.1.3** Standard 030.010 (Kodeks Etyki Zawodowej) stanowi: „Audytor Systemów Informatycznych jest zobowiązany do stosowania się do Kodeksu Etyki Zawodowej Stowarzyszenia ds. audytu i kontroli systemów informatycznych (ISACA)”

1.2 Potrzeba wytycznej

- 1.2.1** Celem „Wytycznej” jest rozszerzenie znaczenia pojęcia "niezależność" używanego w Standardach 020.010 i 020.020 Audytu Systemów Informatycznych i odniesienie się do postawy Audytora SI oraz jego niezależności podczas audytu systemów informatycznych.
- 1.2.2** „Wytyczna” dostarcza wskazówek w stosowaniu standardów audytu SI. Audytor SI powinien ją rozważyć przy określaniu, w jaki sposób osiągnąć implementację powyższych Standardów, w jaki sposób zastosować profesjonalny osąd w jej stosowaniu oraz jak być przygotowanym na uzasadnienie odstępstw.

2. NIEZALEŻNOŚĆ

2.1 Postawa

- 2.1.1** Audytorzy SI powinni dążyć do stosowania kodeksu etyki zawodowej i standardów audytu we wszystkich aspektach swojej pracy.
- 2.1.2** Opierając się na założeniach ujętych w opracowaniu COBIT® , Statut Audytu powinien zagwarantować, że niezależność, autorytet i odpowiedzialność funkcji audytu będą zapewnione i ustalone przez odpowiednie (właściwe) kierownictwo organizacji.

3. PLANOWANIE

3.1 Dobór personelu

- 3.1.1** Audytor SI nawiązuje wiele relacji z ludźmi zaangażowanymi w czynności audytu oraz ma okazję badać najgłębsze aspekty badanego obszaru, nierazko całą organizację. Postawa audytora SI zawsze powinna być odpowiednia do tej roli. Planowanie powinno zatem uwzględniać wszystkie znane relacje (stosunki) dotyczące badanego obszaru (organizacji).
- 3.1.2** Audytorzy SI nie powinni współuczestniczyć w audycie, jeżeli ich niezależność jest naruszona (np. nie są bezstronni). Na przykład niezależność audytorów SI jest naruszona, gdy mają oni pewne oczekiwania dotyczące korzyści finansowych lub innych korzyści osobistych, które mogą spowodować wpływ na wyniki badań. Jednak niezależność audytorów SI niekoniecznie może być naruszona w wyniku przeprowadzania audytu systemów informatycznych tam, gdzie mają miejsce osobiste transakcje audytora w normalnym toku spraw..
- 3.1.3** Na początku audytu, niezależność audytora SI może być potwierdzona przez podpisanie oświadczenia o konflikcie interesów.

3.2 Uprzywilejowany plan audytu

- 3.2.1** Cel kontroli COBIT'u M-4, stanowi, że "Kierownictwo powinno utrzymywać niezależność audytu." Ażeby osiągnąć ten cel, powinien być ustalony plan audytu. Plan ten powinien zapewnić gwarancję skuteczności, wydajności i ekonomiczności bezpieczeństwa oraz właściwe wewnętrzne procedury kontrolne. W granicach tego planu kierownictwo powinno określać pierwszeństwo co do otrzymania zapewnienia niezależności.

4. WYNIKI DZIAŁALNOŚCI PRACY AUDYTU

4.1 Organizacja

- 4.1.1** Audytor SI powinien być organizacyjnie niezależny od audytowanego obszaru. Niezależność jest osłabiona jeżeli audytor SI sprawuje bezpośrednią kontrolę nad audytowanym obszarem. Niezależność audytora SI też może być osłabiana, jeśli podlega bezpośrednio osobom, które sprawują bezpośrednią kontrolę nad badanym obszarem.
- 4.1.2** Niezależność powinna być regularnie oceniana przez audytora SI i kierownictwo. Ta ocena powinna rozważać takie czynniki, jak zmiany w stosunkach osobistych, korzyści finansowe, i wcześniejsze zobowiązania. Audytor SI powinien rozważyć użycie w kontroli oceny niezależności technik samooceny.
- 4.1.3** W zależności od zadania, audytor SI może przeprowadzać wywiad z osobami, analizować procesy organizacyjne, uzyskiwać pomoc od personelu organizacji, itd. Postawa i postępowanie audytora SI powinny być zawsze adekwatne do napotkanej sytuacji. Audytorzy SI powinni być świadomi, że na ocenę ich niezależności mogą mieć wpływ ich działania lub powiązania. Sposób postrzegania niezależności audytora SI mógłby wpływać na przyjęcie wyników jego pracy .
- 4.1.4** Jeżeli audytorzy SI stają się świadomi, że sytuacja lub relacja jest widziana jako naruszenie ich niezależności, powinni powiadomić kierownictwo audytu o dostrzeżonych faktach tak szybko, jak to jest możliwe.

4.2 Zbieranie informacji

4.2.1 Spośród różnych elementów istotnych do zrozumienia audytowanej organizacji, audytorzy SI, ażeby zachować swoją niezależność, powinni dokonać przeglądu:

- organizacyjnej polityki i procedur związanych z procesem zapewnienia niezależności,
- statutu audytu, deklaracji misji, polityk, procedur i standardów, wcześniejszych sprawozdań i planów audytu,
- schematu organizacyjnego.

4.3 Ocena kontroli

4.3.1 Plan audytu SI powinien definiować czynności, w których wymagana jest niezależność audytora SI. Niezależność audytora SI w tych działaniach powinna być stale monitorowana przez kierownictwo wyższego szczebla lub przez osobę, która ustala i zatwierdza plan audytu. Ten proces monitorowania powinien zawierać ocenę przypisaną każdemu audytorowi SI do określonych zadań, aby zapewnić, że ten proces zagwarantuje niezależność i wystarczające (dostateczne) umiejętności.

4.3.2 Zawsze powinna być przeprowadzana weryfikacja stosowania się audytorów SI do odpowiedniego kodeksu zachowania zawodowego. W wielu okolicznościach powinno być to wystarczające do dostarczenia dowodu niezależności. Jeżeli jednak istnieje wskazanie, że niezależność audytora SI może być narażona na szwank, powinno rozważyć się zmianę (korektę) planu audytu.

5. SKŁADANIE SPRAWOZDAŃ

5.1 Informowanie o sprawozdaniach

5.1.1 W okolicznościach, w których niezależność audytora SI jest osłabiona i audytor SI jest nadal powiązany z audytem, sprawy dotyczące kwestii niezależności Audytora IS powinny być ujawnione stosownemu kierownictwu w sprawozdaniu .

6. DATA OBOWIĄZYWANIA

6.1 **Powyższy standard obowiązuje w stosunku do wszystkich audytów systemów informatycznych rozpoczynających się począwszy od 1 września 2000.**

030.010.010 Nieprawidłowości i akty bezprawne

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami ISACA

1.1.1 Standard 030.010 (*Kodeks Etyki Zawodowej*) stanowi, "Audytor systemów informatycznych jest zobowiązany do stosowania się do Kodeksu Etyki Zawodowej Stowarzyszenia do spraw audytu i kontroli systemów informatycznych (ISACA - Information Systems Audit and Control Association)."

1.1.2 Standard 030.020 (*Należyta Staranność Zawodowa*) stanowi, "We wszelkich aspektach pracy, audytora systemów informatycznych obowiązuje należyta staranność zawodowa oraz przestrzeganie odpowiednich standardów audytowania."

1.2 Potrzeba wytycznej

1.2.1 Celem niniejszej wytycznej jest dostarczenie audytorowi SI definicji nieprawidłowości i aktów bezprawnych oraz zasad ich uwzględnienia podczas wykonywania prac.

2. DEFINICJE

2.1 Nieprawidłowości i działania niedozwolone

2.1.1 Nieprawidłowości i działania niedozwolone mogą obejmować:

- Oszustwa, które są każdym aktem oszukiwania w celu osiągnięcia niedozwolonej korzyści
- Inne akty prowadzące do niezgodności z prawem i regulacjami, włączając w to niezgodność systemów IT z odpowiednimi przepisami prawa i regulacjami
- Akty, które prowadzą do niezgodności z organizacyjnymi porozumieniami i kontraktami ze stronami trzecimi, tj. bankami dostawcami i sprzedawcami
- Manipulowanie, fałszowanie, falsyfikowanie lub zmiana zapisów lub dokumentów (zarówno w postaci elektronicznej, jak i papierowej)
- Eliminowanie lub pomijanie efektów transakcji pochodzących z zapisów lub dokumentów (zarówno w postaci elektronicznej, jak i papierowej)
- Bezpodstawne rejestrowanie transakcji z zapisach finansowych lub innych (zarówno w postaci elektronicznej, jak i papierowej) organizacji
- Nieodpowiednie lub nieumiejętne wykorzystanie majątku, w tym majątku SI
- Inne akty intencjonalne, ale nie oszukańcze, włączając w to nielegalne wykorzystanie znaków towarowych, praw autorskich, praw patentowych
- Błędy w zapisach finansowych lub innych pochodzące od nieautoryzowanego dostępu lub użycia systemów IT organizacji

2.1.2 Nieprawidłowości, które nie są zdefiniowane powyżej ale prowadzą do nieprawidłowości w stosowaniu polityk zarządczych lub nieprawidłowego kierowania organizacją podczas wypełnienia jej działań.

2.2 Uzależnienie od opinii prawnej

2.2.1 Pytanie, czy nieprawidłowości, działania niedozwolone lub błędy zostały popełnione oraz ich waga lub wpływ na organizację wykracza poza zakres odpowiedzialności audytora SI.

2.2.2 Określenie, czy konkretny akt lub akty są nielegalne powinno generalnie opierać się na ekspertyzie osoby z kwalifikacjami w zakresie prawa lub może oczekiwać na ostateczne określenie przez sąd.

2.2.3 Jednakże dla wygody, niniejsza wytyczna odnosi się do "nieprawidłowości i innych działań niedozwolonych" w obszarach praktyki audytora SI, gdzie będzie rozważane raczej podejrzenie, a nie dowód oszustwa lub innego nielegalnego działania.

3. ODPOWIEDZIALNOŚĆ KIEROWNICTWA I AUDYTORA SI

3.1 Kierownictwo

Odpowiedzialnością kierownictwa jest zapobiegać oraz wykrywać nieprawidłowości i akty bezprawne

3.1.1 Kierownictwo, aby uzyskać racjonalne zapewnienie, że zapobiega się i wykrywa na czas nieprawidłowości i akty bezprawne, zwykle używa:

- Mechanizmy kontroli wewnętrznej, włączając w to przeglądanie i aprobowanie transakcji oraz procedury zarządcze dotyczące weryfikacji
- Polityki i procedury regulujące zachowania pracowników
- Atestację zgodności i procedury monitorowania

3.1.2 Audytor SI powinien rozumieć pogląd, że mechanizmy kontrolne nie eliminują prawdopodobieństwa wystąpienia nieprawidłowości lub aktów bezprawnych.

3.2 Audytor SI

3.2.1 Audytor SI nie jest zawodowo odpowiedzialny za zapobieganie lub wykrywanie nieprawidłowości lub aktów bezprawnych.

3.2.2 W rezultacie, jeżeli nie istnieją informacje mogące wskazywać audytorowi SI, że miały miejsce nieprawidłowości lub akty bezprawne, audytor SI nie ma obowiązku wykonywania procedur zaprojektowanych dla ich wykrywania.

3.2.3 Obowiązkiem audytora SI jest badanie i raportowanie pojawiających się nieprawidłowości tylko w warunkach, gdy został zidentyfikowany dowód istnienia nieprawidłowości lub aktów bezprawnych.

3.2.4 Audytor SI powinien także informować kierownictwo i komitet audytowy (lub ekwiwalent), gdy zidentyfikuje sytuację, gdzie istnieje podwyższone ryzyko powstania nieprawidłowości lub aktów bezprawnych, nawet jeżeli żadne nie zostały wykryte.

3.2.5 Jednakże, w warunkach kiedy podjęte prace obejmują nieprawidłowości i akty bezprawne, audytor SI może otrzymać specyficzne wymaganie wykonania procedur służących do ich wykrywania.

4. PLANOWANIE I PROWADZENIE PRAC

4.1 Planowanie prac

4.1.1 Mimo, że audytor nie ponosi explicite odpowiedzialności za zapobieganie lub wykrywanie aktów bezprawnych, to jednak powinien projektować procedury do ich wykrywania opierając się na oszacowanym poziomie ryzyka możliwości ich wystąpienia.

Stąd, podczas planowania prac, audytor SI powinien zrozumieć takie rzeczy jak:

- Środowisko kontroli wewnętrznej
- Polityki i procedury regulujące zachowania pracowników
- Atestację zgodności i procedury monitorowania
- Środowisko prawne i regulacyjne, w którym operuje organizacja
- Mechanizmy wykorzystywane przez organizację do pozyskiwania, monitorowania i zapewniania zgodności z prawem i regulacjami mającymi wpływ na organizację

4.1.2 Audytor SI powinien zatem dokonać oceny ryzyka aby określić, czy pojawiające się nieprawidłowości lub akty bezprawne są istotne dla przedmiotu raportu.

4.1.3 Ocena ryzyka powinna brać pod uwagę tylko te czynniki, które są właściwe dla organizacji i przedmiotu prac, włączając w to:

- Czynniki ryzyka dotyczące nieprawidłowości i aktów bezprawnych, które wpływają na zapisy księgowe
- Czynniki ryzyka dotyczące nieprawidłowości i aktów bezprawnych, które nie wpływają na zapisy księgowe, ale wpływają na organizację
- Czynniki ryzyka dotyczące innych nieprawidłowości i aktów bezprawnych, które wpływają na dostateczność (sufficiency) mechanizmów kontrolnych organizacji

4.1.4 Audytor SI powinien także rozważyć w ramach oceny ryzyka inne czynniki, które mogą wpływać na ryzyko, w tym:

- Skutki niezadowolenia pracowników
- Potencjalne ograniczenie zatrudnienia, outsourcing lub restrukturyzację
- Istnienie majątku łatwo podatnego na zmianę przeznaczenia
- Słabą wydajność finansową/operacyjną organizacji
- Postawę kierownictwa wobec etyki
- Nieprawidłowości lub akty bezprawne charakterystyczne dla konkretnego przemysłu lub pojawiające się w podobnych organizacjach

4.1.5 Jako część procesu planowania i wykonywania oceny ryzyka, audytor SI powinien zasięgnąć informacji u kierownictwa w zakresie takich problemów jak:

- Ich zrozumienie poziomu ryzyka wystąpienia nieprawidłowości i aktów bezprawnych w organizacji
- Posiadanie wiedzy na temat nieprawidłowości lub aktów bezprawnych popełnionych wobec organizacji lub w ramach organizacji, które wystąpiły lub mogą wystąpić
- Sposób monitorowania i zarządzania nieprawidłowościami i aktami bezprawnymi w organizacji

4.2 Procedury pracy

4.2.1 Audytor SI powinien zaprojektować procedury prac audytorskich biorąc pod uwagę poziom ryzyka zidentyfikowanych nieprawidłowości i aktów bezprawnych.

4.2.2 Rezultaty procedur oceny ryzyka i innych procedur wykonywanych podczas planowania powinny być wykorzystane do określenia natury, obszaru i czasu procedur realizowanych w trakcie prac.

4.2.3 Audytor SI powinien także zasięgnąć informacji u kierownictwa IT i kierownictwa użytkowników (jeśli właściwe) na temat zgodności z prawem i regulacjami.

4.3 Ocena rezultatów procedur pracy

4.3.1 Audytor SI powinien przeglądać rezultaty prac w celu określenia, czy nie pojawiły się symptomy nieprawidłowości lub aktów bezprawnych.

4.3.2 Podczas wykonywania tej oceny powinny być brane pod uwagę czynniki ryzyka określone w sekcji 4.1 i rozważane pod kątem aktualnie wykonywanych procedur, aby dostarczyć rozsądnego zapewnienia, że wszystkie ryzyka były zanalizowane.

4.3.3 Szacunki powinny także obejmować rezultaty realizacji procedur w celu określenia, czy nie istnieją niezidentyfikowane czynniki ryzyka.

5. KIEDY NIEPRAWIDŁOWOŚCI LUB NIELEGALNE DZIAŁANIA SĄ WYKRYWANE

5.1 Odpowiadanie na prawdopodobne działania nielegalne

5.1.1 Kiedy audytor SI staje się świadomy informacji dotyczących możliwych aktów bezprawnych wówczas powinien wykonać co następuje:

- Zrozumieć naturę aktu.
- Zrozumieć warunki, w których się wydarzył.
- Pozyskać wystarczającą ilość innych informacji by ocenić skutki niepożądanych lub bezprawnych aktów.
- Przeprowadzić dodatkowe procedury, aby określić skutki niepożądanych lub bezprawnych aktów oraz czy istnieją inne takie akty.

5.1.2 W celu określenia występowania i skutków nieprawidłowości lub aktów bezprawnych audytor SI powinien współpracować z innymi w ramach organizacji (takimi jak personel bezpieczeństwa), włączając w to kierownictwo (jeżeli jest to możliwe to na poziomie powyżej tego, który jest uwikłany).

5.2 Procedury, które powinny być wykonane

5.2.1 Podczas prac mogą zwracać uwagę audytora SI oznaki istnienia nieprawidłowości lub aktów nielegalnych. Jeśli stwierdzono takie oznaki nieprawidłowości lub aktów nielegalnych, to audytor SI powinien rozważyć ich potencjalne skutki na przedmiot prac, raport i organizację.

5.2.2 Audytor SI powinien radzić się radców prawnych i/lub innych jednostek w organizacji zaraz po zidentyfikowaniu potencjalnej nieprawidłowości lub działania bezprawnego. Tylko radca prawny może ocenić, czy jest to rzeczywiście nieprawidłowość lub akt nielegalny.

5.2.3 Jeżeli okoliczności jasno nie wskazują czego innego, to audytor SI powinien założyć, że nieprawidłowość lub akt nielegalny nie stanowi odosobnionego przypadku.

5.2.4 Audytor SI powinien także zbadać odpowiednią ilość organizacyjnych mechanizmów kontrolnych, aby określić dlaczego zawiodły w zapobieganiu lub wykrywaniu wystąpienia nieprawidłowości lub aktów bezprawnych.

5.2.5 Audytor SI powinien rozpatrzyć ponownie wcześniejszą ocenę dostateczności, działania i skuteczności organizacyjnych mechanizmów kontrolnych.

5.2.6 Kiedy audytor SI zidentyfikował sytuacje, gdzie istnieją nieprawidłowości lub akty bezprawne (niezależnie czy potencjalne, czy faktyczne), wówczas powinien zmodyfikować procedury potwierdzania lub rozwiązywania zagadnienia określonego podczas wykonywania prac.

5.2.7 Obszar takich modyfikacji lub dodatkowych procedur zależy od osądu audytora SI dotyczącego:

- Typu nieprawidłowości i aktu bezprawnego, który może się pojawić
- Dostrzegania ryzyka jego pojawienia
- Potencjalnego wpływu na organizację, włączając w to takie sprawy jak skutki finansowe i reputację organizacji
- Prawdopodobieństwa ponownego wystąpienia podobnych nieprawidłowości lub aktów bezprawnych
- Prawdopodobieństwa, że kierownictwo może mieć wiedzę na temat lub być zaangażowane w nieprawidłowości lub akty bezprawne
- Działań, jeśli są jakieś, które podejmuje ciało regulujące i/lub kierownictwo
- Prawdopodobieństwa, że niezgodność z prawem i regulacjami wystąpiła nieumyślnie
- Prawdopodobieństwa, że jako rezultat niezgodności może być nałożona znacząca kara lub inna sankcja, dla przykładu cofnięcie istotnej licencji
- Skutków wzbudzenia zainteresowania społeczeństwa wywołanego nieprawidłowością

5.3 Kierownictwo

5.3.1 Kiedy w nieprawidłowość uwikłany jest członek kierownictwa, audytor SI powinien ponownie rozważyć rzetelność informacji przekazanych przez kierownictwo.

5.3.2 Zwykle, audytor SI powinien pracować z odpowiednim poziomem kierownictwa, powyżej związanego z nieprawidłowością lub aktem bezprawnym.

6. RAPORTOWANIE

6.1 Raportowanie nieprawidłowości i działań bezprawnych

6.1.1 Nieprawidłowości i akty bezprawne znacząco różnią się w swojej istotności i potencjalnym wpływie na przedmiotową sprawę lub raport.

6.1.2 Jeżeli jest to odpowiednie, to ocena wpływu nieprawidłowości lub aktu bezprawnego powinna być przeprowadzona we współdziałaniu z biurem radców prawnych i stosownym organizacyjnym regulatorem (takim jak zarząd lub komitet audytowy) lub kierownictwem.

6.1.3 Ocena powinna uwzględniać skutki wpływu nieprawidłowości lub aktów bezprawnych ma na takie sprawy jak określone porozumienia, kontrakty, prawo i regulacje.

6.1.4 Potencjalny wpływ jaki ma nieprawidłowość lub akt bezprawny na przedmiotową sprawę lub raport będzie się różnił w zależności od typu aktu bezprawnego i charakteru działań organizacji.

6.1.5 Jeżeli nie, to w przeciwnym razie, audytor jest odpowiedzialny tylko za zaraportowanie zdarzeń i okoliczności towarzyszących aktowi.

6.1.6 Odpowiedzialnością kierownictwa jest, zwykle z konsultacją z radcą prawnym, określenie i zaraportowanie, czy akt jest faktycznie nieprawidłowością lub aktem bezprawnym.

6.1.7 W pewnych jurysdykcjach, audytor SI może mieć dodatkowe obowiązki, które wykraczają poza wymagania przedstawione w

powyższej sekcji 6.1.5. W takim przypadku, audytor SI musi dostarczyć przekonywującego zapewnienia, że działa zgodnie także z tymi dodatkowymi wymaganiami.

6.2 Raporty dla kierownictwa

- 6.2.1** Audytor SI powinien zawrzeć w raporcie opis zdarzeń i okoliczności towarzyszących nieprawidłowości lub aktowi bezprawnemu.
- 6.2.2** Spostrzeżenia powinny być raportowane do odpowiedniego poziomu kierownictwa, wyższego niż to, które jest uwikłane w akt. Jeżeli uwikłane są wszystkie poziomy kierownictwa, lub gdy audytor SI podejrzewa, że wszystkie są uwikłane, wówczas spostrzeżenia powinny być przedstawione organizacyjnemu ciałom regulującym, takim jak zarząd, rada nadzorcza lub komitet audytowy.
- 6.2.3** Audytor powinien używać profesjonalnego osądu kiedy raportuje nieprawidłowość lub akt bezprawny. Audytor SI powinien przedyskutować spostrzeżenia oraz naturę, czas i obszar jakichkolwiek dalszych procedur z odpowiednim poziomem kierownictwa, który jest umiejscowiony przynajmniej powyżej osób, które wydają się uwikłane. W takich okolicznościach, szczególnie ważnym jest aby audytor SI zachował niezależność. Określając odpowiednie osoby, którym raportować nieprawidłowość lub działanie bezprawne, audytor SI powinien rozważyć wszystkie związane okoliczności, włączając w to prawdopodobieństwo uwikłania także starszego kierownictwa.
- 6.2.4** Audytor SI powinien usiłować uniknąć zaalarmowania jakiegokolwiek osoby, która może być wpłątana lub uwikłana w nieprawidłowość lub akt bezprawny, by zredukować możliwość zniszczenia lub ukrycia dowodów przez te osoby.

6.3 Raporty dla stron trzecich

- 6.3.1** Nie przeciwstawiając się organizacyjnemu obowiązkowi raportowania aktu bezprawnego lub nieprawidłowości, powinnością audytora SI jest zaufanie organizacji, wykluczające raportowanie każdej potencjalnej lub zidentyfikowanej nieprawidłowości lub aktu nielegalnego.
- 6.3.2** Jednakże w określonych przypadkach może być wymagane od audytora SI ujawnienie nieprawidłowości lub aktu bezprawnego. Obejmuje to takie sytuacje jak:
- Zgodność z prawem lub wymaganiami regulatorów
 - Żądanie zewnętrznego audytora
 - Żądanie sądu
 - Fundusze lub agencje rządowe, zgodnie z wymaganiami audytów jednostek, które otrzymują rządowe wsparcie finansowe
- 6.3.3** W sytuacjach gdzie od audytora SI jest wymagane ujawnienie potencjalnych lub zidentyfikowanych nieprawidłowości lub aktów bezprawnych powinna być najpierw zaciągnięta opinia prawna.
- 6.3.4** W niektórych jurysdykcjach, audytor SI może być chroniony immunitetem. Nawet w sytuacjach gdzie audytor jest chroniony przywilejem powinien zasięgnąć porady prawnej zanim dokona ujawnienia, aby upewnić się, że jest rzeczywiście chroniony.
- 6.3.5** Jeżeli organizacja nie ujawnia znanej nieprawidłowości lub aktu bezprawnego lub wymaga od audytora SI zatajenia spostrzeżeń, to audytor SI powinien zasięgnąć porady prawnej.

7. TERMIN OBOWIĄZYWANIA

- 7.1 Niniejsza wytyczna obowiązuje wszystkie audyty systemów informatycznych rozpoczęte 1 czerwca 2002 lub później.**

030.020.010 Rozważania audytowe na temat nieprawidłowości

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

- 1.1.1** Standard 030.020 (Należyta staranność zawodowa) stwierdza: „Wobec wszystkich aspektów pracy Audytora Systemów Informatycznych obowiązuje właściwa profesjonalna staranność i przestrzeganie stosowanych standardów audytorskich.”
- 1.1.2** Standard 050.010 (Planowanie audytu) stwierdza: „Audyt Systemów Informatycznych powinien planować prace związane z audytem systemów informatycznych pod kątem realizacji celów audytorskich oraz zgodnie ze stosowanymi standardami.”
- 1.1.3** Standard 060.020 (Dowody) stwierdza: „Zadaniem Audytora Systemów Informatycznych podczas przeprowadzania audytu jest zgromadzenie wystarczających, wiarygodnych, istotnych i użytecznych dowodów służących efektywnej realizacji zadań audytorskich. Wykrycia audytu oraz wnioski powinny być poparte odpowiednią analizą i interpretacją tychże dowodów.”
- 1.1.4** Standard 070.010 (Forma i zawartość raportu) stwierdza: „Zadaniem Audytora Systemów Informatycznych (Audytora SI) jest dostarczenie określonym odbiorcom odpowiednio sformowanego raportu dotyczącego wykonanych prac audytowych. Raport z audytu ma przedstawiać obszar, cele, okres oraz rodzaj i zakres wykonanej pracy audytorskiej. Raport ma wskazywać organizację, odbiorcę raportu oraz wszelkie zastrzeżenia co do jego obiegu. Raport ma przedstawiać wyniki, wnioski i rekomendacje oraz wszelkie zastrzeżenia lub uwarunkowania audytora wobec audytu.”

1.2 Potrzeba wytycznej

- 1.2.1** Niektóre nieprawidłowości mogą być rozważane jako działania nieuczciwe (oszustwa). Określenie działań nieuczciwych (oszustw) zależy od prawnej definicji oszustwa w jurysdykcji odnoszącej się do audytu. Nieprawidłowości zawierają, ale nie są do niego ograniczone, świadome ominięcie mechanizmów kontrolnych w celu ukrycia dowodów oszustwa, nieautoryzowanego użycia zasobów lub usług, itp. i współdziałanie lub pomaganie w ukryciu tych działań. Działania nie mające charakteru oszustwa mogą zawierać:
 - celowe naruszenie ustalonej polityki zarządzania,
 - celowe naruszenie przepisowych wymagań,
 - świadome zniekształcenie lub pominięcie informacji dotyczącej audytowanego obszaru lub organizacji jako całości,
 - duże zaniedbanie,
 - niecelowe działania nielegalne.
- 1.2.2** Wytyczna ta dostarcza wskazówek dla stosowania standardów audytu informatycznego. Audytor SI powinien brać ją pod uwagę podczas określania sposobu implementacji powyższych Standardów, stosowania profesjonalnej oceny przy ich zastosowaniu oraz być przygotowanym do uzasadnienia wszelkich od nich odstępstw..

2. STATUT AUDYTU

2.1 Odpowiedzialność

- 2.1.1** Audytor SI powinien rozważyć zdefiniowanie w statucie audytu lub liście (umowie) w sprawie wykonania audytu, odpowiedzialności kierownictwa i audytu dotyczącej przeciwdziałania nieprawidłowościom, ich wykrywania i raportowania tak, aby było to jasno zrozumiałe w odniesieniu do całej pracy audytowej. Tam, gdzie ta odpowiedzialność jest już udokumentowana w polityce organizacji w stosunku do oszustw lub podobnym dokumencie, statut audytu powinien zawierać stosowną klauzulę nawiązującą do wspomnianych dokumentów.
- 2.1.2** Kierownictwo jest odpowiedzialne za zaprojektowanie, wdrożenie i utrzymywanie systemu kontroli wewnętrznej uwzględniającej przeciwdziałanie i wykrywanie oszustw.
- 2.1.3** Audytor SI jest odpowiedzialny za ocenę ryzyka wystąpienia oszustw i zaprojektowanie i przeprowadzenie testów, które są odpowiednie dla natury przeprowadzanego audytu i z racjonalnego punktu widzenia mogą być oczekiwane w celu wykrycia:
 - nieprawidłowości, które mogą mieć znaczący wpływ zarówno na audytowany obszar jak i całość organizacji,
 - słabości w mechanizmach kontroli wewnętrznej, które mogą powodować znaczące nieprawidłowości, dla których występuje brak przeciwdziałań lub nie są one wykrywane.
- 2.1.4** Audyt nie może gwarantować, że nieprawidłowości będą wykryte. Nawet w sytuacji, gdy audyt jest prawidłowo zaplanowany i wykonany, nieprawidłowości mogą pozostać niewykryte; t.j. jeśli występuje zмова pomiędzy pracownikami, zмова pomiędzy pracownikami a osobami z zewnątrz, lub zaangażowanie kierownictwa w te nieprawidłowości. Audytor SI powinien również rozważyć udokumentowanie tego punktu widzenia w statucie audytu lub liście (umowie) w sprawie wykonania audytu.

3. KOMPETENCJE

3.1 Świadomość dotycząca oszustw

- 3.1.1** Audytor SI powinien w wystarczającym stopniu znać temat oszustw tak, aby być zdolnym do identyfikacji czynników ryzyka, mogących przyczynić się do wystąpienia oszustw..

4. PLANOWANIE

4.1 Ocena ryzyka

- 4.1.1** Audytor SI powinien oceniać ryzyko wystąpienia nieprawidłowości związanych z audytowanym obszarem. Podczas przygotowania takiej oceny, audytor SI powinien rozważyć takie czynniki jak:
 - charakterystyki organizacyjne: tj. korporacyjne kodeksy etyki, strukturę organizacyjną, adekwatność nadzoru, wynagrodzeń i sposobów motywacji, stopień nacisków na wydajność w korporacji,
 - historię organizacji,

- ostatnie zmiany w zarządzaniu, działaniach operacyjnych i systemach informatycznych,
- typy posiadanych aktywów, lub oferowanych usług, i ich podatność na nieprawidłowości,
- siłę odpowiednich mechanizmów kontrolnych,
- stosowne wymagania prawne i inne regulacje,
- historię obserwacji audytowych z poprzednich audytów,
- branżę gospodarki i środowisko konkurencji, w którym działa organizacja,
- obserwacje z przeglądów przeprowadzonych poza zakresem (obecnego) audytu, takie jak obserwacje konsultantów, zespołów kontroli jakości lub specjalnych badań zarządczych
- obserwacje powstające w wyniku codziennych działań biznesowych,
- wyrafinowanie techniczne i złożoność systemów informatycznych wspomagających audytowany obszar,
- obecność aplikacji rozwiniętych/utrzymywanych samodzielnie przez firmę, w porównaniu do gotowego oprogramowania, dla wspierania kluczowego biznesu.

- 4.1.2** Podczas planowania pracy audytowej odpowiedniej do rodzaju przewidzianego audytu, audytor SI powinien wykorzystać rezultaty oceny ryzyka, aby oszacować rodzaj, harmonogram i poziom testowania wymagany do tego, aby otrzymać wystarczający dowód audytowy tak, aby w efekcie dostarczyć racjonalnego zapewnienia, że:
- nieregularności, które mogą mieć istotny wpływ na audytowany obszar lub organizację w całości, będą zidentyfikowane,
 - słabości mechanizmów kontrolnych, które mogłyby prowadzić do nie zapobieżenia lub niewykrycia istotnych nieprawidłowości będą zidentyfikowane .

5. PROWADZANIE PRAC AUDYTOWYCH

5.1 Efekt zaobserwowania nieprawidłowości

- 5.1.1** Jeśli nieprawidłowości zostaną wykryte, audytor SI powinien ocenić wpływ tych działań na cele audytu i na wiarygodność zebranych dowodów audytowych. Ponadto, audytor SI powinien rozważyć, czy kontynuować audyt, w sytuacji, gdy:
- wpływ nieprawidłowości wydaje się być tak znaczący, że nie można otrzymać wystarczających i wiarygodnych dowodów audytowych,
 - dowody audytowe sugerują, że kierownictwo ma udział lub przyryka oczy na nieprawidłowości.

5.2 Efekt zaobserwowania wskaźników/indykatorów nieprawidłowości

- 5.2.1** Jeśli dowód audytowy wskazuje, że nieprawidłowości mogą występować, audytor SI powinien:
- rekomendować kierownictwu, aby sprawa została szczegółowo zbadana lub zostały podjęte odpowiednie działania. Jeśli audytor SI podejrzewa, że kierownictwo ma udział w nieprawidłowościach, powinien znaleźć osobę o odpowiedniej odpowiedzialności w organizacji, której tego rodzaju wnioski powinny być zaraportowane. Jeśli wewnętrzne raportowanie wydaje się niemożliwe, audytor SI powinien rozważyć konsultację z komitetem audytowych i prawnikiem nt. słuszności i ryzyka związanego z raportowaniem obserwacji poza organizację,
 - przeprowadzić odpowiednie działania dla wsparcia obserwacji, wniosków i rekomendacji.

5.3 Względy prawne

- 5.3.1** Jeśli dowód audytowy wskazuje, że nieprawidłowość może pociągać za sobą czyn nielegalny, audytor SI powinien rozważyć zasięgnięcie porady prawnej lub rekomendować kierownictwu jej zasięgnięcie.

6. RAPORTOWANIE

6.1 Raportowanie wewnętrzne

- 6.1.1** Wykrycie nieprawidłowości powinno być zakomunikowane we właściwym czasie odpowiednim osobom w organizacji. Powiadomienie powinno być skierowane na poziom zarządzania wyższy, od tego na którym podejrzewane jest występowanie nieprawidłowości. Ponadto, nieprawidłowości powinny być raportowane do zarządu, komitetu audytowego lub jego ekwiwalentu, z wyjątkiem spraw ewidentnie nieznaczących zarówno w sensie wpływu finansowego jak i słabości mechanizmów kontrolnych.

- 6.1.2** Wewnętrzna dystrybucja raportów z nieprawidłowościami powinna być wnikliwie rozważona. Wystąpienie i wpływ nieprawidłowości jest tematem bardzo wrażliwym i raportowanie wnosi swoje własne ryzyko włączając w to:
- dalsze wykorzystanie słabości mechanizmów kontrolnych w rezultacie opublikowania szczegółów na ich temat,
 - utratę klientów, dostawców i inwestorów, gdy ujawnienie (autoryzowane lub nieautoryzowane) nastąpi poza organizacją,
 - utratę kluczowego personelu i kierownictwa, również tego, które nie było zaangażowane w nieprawidłowość, w efekcie upadku zaufania w kierownictwo i przyszłość organizacji.

- 6.1.3** Audytor SI powinien rozważyć raportowanie nieprawidłowości oddzielnie od innych tematów audytowych, jeśli pomoże to kontroli dystrybuowania raportu.

6.2 Raportowanie zewnętrzne

- 6.2.1** Raportowanie zewnętrzne może być obowiązkiem prawnym lub wynikającym z innych regulacji. Obowiązek może dotyczyć kierownictwa organizacji, lub indywidualnych osób zaangażowanych w wykrycie nieprawidłowości, lub obu stron.

- 6.2.2** Jeśli raportowanie zewnętrzne jest wymagane, raport powinien być zatwierdzony przez odpowiedni szczebel zarządzania audytem, zanim nastąpi wydanie na zewnątrz i powinien być również wcześniej przeglądnięty przez kierownictwo audytowanego, o ile stosowne regulacje lub specyficzne okoliczności tego nie zabraniają. Przykładem specyficznych okoliczności, zabraniających otrzymania (raportu) przez kierownictwo audytowanego może być:
- aktywne zaangażowanie kierownictwa audytowanego w występowanie nieprawidłowości,
 - pasywne przyzwolenie kierownictwa audytowanego na występowanie nieprawidłowości.

- 6.2.3** Jeśli kierownictwo audytowanego nie zgadza się na wydanie raportu na zewnątrz, a zewnętrzne raportowanie jest

obowiązkiem ustawowym lub wynikającym z innych regulacji, to audytor SI powinien rozważyć konsultacje z komitetem audytowym i prawnikiem nt. słuszności i ryzyka związanego z raportowaniem obserwacji poza organizację.

6.2.4 Audytor SI, za zgodą kierownictwa audytu, powinien we właściwym czasie przesłać raport do wszystkich odpowiednich ciał nadzorczych.

6.2.5 W sytuacji, gdy audytor SI jest świadomy tego, że kierownictwo jest zobowiązane do raportowania na zewnątrz działań o charakterze oszustw, audytor SI powinien formalnie powiadomić kierownictwo o ich odpowiedzialności..

6.2.6 Jeśli nieprawidłowość została wykryta przez audytora SI, który nie jest częścią zewnętrznego zespołu audytowego, to audytor SI powinien rozważyć przesłanie we właściwym czasie raportu do audytorów zewnętrznych.

6.3 Ograniczenia zakresu audytu

6.3.1 W sytuacji, gdy zakres audytu został ograniczony, audytor SI powinien zawrzeć w raporcie z audytu wyjaśnienie istoty i wpływu ograniczenia. Takie ograniczenie może wystąpić, jeśli:

- audytor SI nie mógł przeprowadzić dalszej pracy uznanej za niezbędną dla spełnienia celów audytu i poparcia wniosków audytowych, na przykład z powodu niewiarygodności dowodów audytowych, braku zasobów lub ograniczeń na działania audytowe wprowadzonych przez kierownictwo,
- kierownictwo nie przeprowadziło badań rekomendowanych przez audytora SI.

7. DATA OBOWIĄZYWANIA

7.1 Powyższa wytyczna obowiązuje wszystkie audyty systemów informatycznych rozpoczynające się w dniu lub po 1 marca 2000.

030.020.020 Należyta staranność zawodowa

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

1.1.1 Standard 030.010 (Kodeks etyki zawodowej) stwierdza: "Audytor systemów informatycznych ma stosować się do Kodeksu Etyki Zawodowej Stowarzyszenia do spraw audytu i kontroli systemów informatycznych (ISACA - Information Systems Audit and Control Association)".

1.1.2 Standard 030.020 (Należyta staranność zawodowa) stwierdza: "Wobec wszelkich aspektów pracy Audytora Systemów Informatycznych obowiązuje należyta staranność zawodowa oraz przestrzeganie odpowiednich standardów audytu."

1.2 Potrzeba wprowadzenia Wytycznej

1.2.1 Celem wprowadzenia tej Wytycznej jest wyjaśnienie terminu "należyta staranność zawodowa", tak jak odnosi się on do przeprowadzenia audytu zgodnego ze Standardami Audytowania SI 030.010 i 030.020.

1.2.2 Niniejsza Wytyczna dostarcza wskazówek jak stosować standardy audytowania systemów informatycznych. Audytor SI powinien uwzględnić ją podczas określania sposobu wdrożenia wyżej wymienionych Standardów, powinien posłużyć się profesjonalną oceną podczas jej stosowania i być przygotowanym do uzasadnienia każdego odstępstwa od niej.

2. PRZEPROWADZANIE PRAC AUDYTOWYCH

2.1 Należyta staranność

2.1.1 Standard "należytej staranności" określa taki poziom dbałości (pilności), jaki w określonych warunkach zastosowałaby osoba rozsądna i kompetentna. "Należyta staranność zawodowa" odnosi się do osoby, która zawodowo stosuje specjalne umiejętności, jak na przykład audytowanie systemów informatycznych. Należyta staranność zawodowa nakłada na osobę obowiązek podnoszenia swoich umiejętności do poziomu ogólnie posiadanego przez praktyków danej specjalności.

2.1.2 Należyta staranność zawodowa dotyczy dokonywania profesjonalnej oceny w trakcie przeprowadzanych prac. Należyta staranność zawodowa oznacza, że profesjonalista podchodzi do spraw wymagających profesjonalnej oceny z odpowiednią pilnością (dbałością). Mogą jednak wystąpić sytuacje, w których pomimo, że uczyniono zadość należytej staranności zawodowej i profesjonalnej ocenie, to na podstawie pieczołowicie przeprowadzonego przeglądu dostępnych faktów i okoliczności, wyciągnięte mogą zostać niepoprawne wnioski. Dlatego, następujące po fakcie, stwierdzenie nieprawidłowości wnioskowania nie musi oznaczać, tym samym, niedostatecznej (profesjonalnej) oceny czy braku należytej dbałości po stronie Audytora SI.

2.1.3 Należyta staranność zawodowa powinna obejmować każdy aspekt przeprowadzanego audytu, włącznie z oceną ryzyka audytu, formułowaniem celów audytu, ustalaniem zakresu audytu, wyborem testów kontrolnych oraz oceną wyników testów. Podczas wykonywania powyższych czynności audytor powinien ustalić lub oszacować:

- Typ oraz poziom zasobów audytowych wymaganych do osiągnięcia celów audytu,
- Istotność zidentyfikowanych ryzyk oraz ich potencjalny wpływ na wykonywany audyt,
- Zgromadzone dowody audytowe,
- Kompetencje, uczciwość oraz wnioski innych osób, na których pracy Audytor SI chce się oprzeć

2.1.4 Przewidywani odbiorcy raportów z audytów mają prawo oczekiwać, że Audytor SI wykazał się należyłą starannością zawodową przy wykonywaniu prac audytowych. Audytor SI nie powinien przyjmować zadań, jeśli nie posiada odpowiednich umiejętności, wiedzy oraz zasobów do wykonania swojej pracy w sposób oczekiwany od profesjonalisty.

2.1.5 Audytor SI powinien przeprowadzać audyty z należyłą dbałością, stosując się do standardów zawodowych. Audytor SI powinien ujawnić okoliczności wszelkich odstępstw od standardów zawodowych w sposób zgodny do sposobu komunikowania wyników audytu.

3. DATA OBOWIĄZYWANIA

3.1 Powyższa Wytyczna obowiązuje w stosunku do wszystkich audytów systemów informatycznych rozpoczynających się począwszy od dnia 1 września 1999r.

050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

1.1.1 Standard 050.010 (Planowanie Audytu) stwierdza, że „Audytor Systemów Informatycznych (Audytor SI) zobowiązany jest do planowania prac audytowych (audytów systemów informatycznych), tak aby uwzględnić cele audytu oraz aby zapewnić zgodność z odpowiednimi standardami profesjonalnego audytowania.”

1.2 Potrzeba wytycznej

1.2.1 Wytyczna audytowania SI dotycząca planowania stwierdza, że „Podczas procesu planowania Audytor SI powinien zwyczajowo ustanowić poziomy ważności (istotności) w taki sposób, że planowane prace audytowe będą wystarczające, aby spełnić cele audytu i wydajnie wykorzystać zasoby audytowe” (Paragraf 2.2.1.)

1.2.2 Audytorzy finansowi mierzą zwykle ważność przy pomocy pojęć finansowych (wartości wyrażanych w pieniądzu) ponieważ audytowane przez nich zagadnienia są również mierzone i raportowane przy pomocy wielkości finansowych (pieniężnych). Audytor SI może przeprowadzać audyty zagadnień niefinansowych, np. mechanizmy kontroli dostępu fizycznego, mechanizmy kontroli dostępu logicznego, mechanizmy kontroli zmian w oprogramowaniu, oraz systemy wykorzystywane do zarządzania personelem, kontroli produkcji, projektowania, kontroli jakości, generowania haseł, produkcji kart płatniczych i sprawowania opieki nad pacjentami. Dlatego audytorzy mogą potrzebować wskazówek jak oceniać ważność (istotność), aby efektywnie planować swoje audyty, aby skupić swoje wysiłki na obszarach wysokiego ryzyka oraz aby ocenić dotkliwość wszystkich znalezionych błędów i słabości.

1.2.3 Niniejsza wytyczna dostarcza wskazówek, jak stosować standardy audytowania SI. Audytor SI powinien wziąć ją pod uwagę określając sposób wdrożenia powyższego Standardu, powinien posłużyć się swoim profesjonalnym osądem podczas jej stosowania i być gotowym uzasadnić każde od niej odstępstwo.

2. PLANOWANIE

2.1 Ocena istotności

2.1.1 Ocena tego, co jest, a co nie jest ważne (istotne) jest sprawą profesjonalnego osądu i obejmuje rozważenie wywieranego na organizację jako całość wpływu błędów, zaniedbań, nieprawidłowości lub niedozwolonych czynów czy działań, które mogą mieć miejsce jako rezultat słabości kontroli w ramach audytowanego obszaru.

2.1.2 Podczas oceny ważności (istotności) Audytor SI powinien rozważyć:

- Łączny, całkowity poziom błędów możliwy do zaakceptowania przez kierownictwo, Audytora SI oraz odpowiednie organy nadzorcze,
- Zdolność do kumulowania się małych błędów i słabości (tworzenia tzw. efektu kumulatywnego) i stawania się przez to znacznymi (ważnymi).

2.1.3 Planując w sposób wystarczający prace audytowe tak aby spełnić cele audytu, audytor SI powinien zidentyfikować odpowiednie cele kontrolne i określić, opierając się na ważności (istotności), które mechanizmy kontrolne będą badane. Jeśli chodzi o poszczególne cele kontrolne, to ważna (istotna) kontrola jest mechanizmem kontrolnym (kontrolą) lub zespołem mechanizmów kontrolnych (zespołem kontroli) bez których procedury kontrolne nie dają rozsądnego zapewnienia, że cele kontrolne zostaną spełnione.

2.1.4 W przypadkach, gdy cele audytu SI odnoszą się do systemów lub operacji, w ramach których przetwarza się transakcje finansowe, przy ocenie ważności (istotności) pod uwagę powinna być brana wartość aktywów kontrolowanych przez system(y) lub wartość transakcji przetwarzanych w ciągu dnia/ tygodnia/ miesiąca/ roku.

2.1.5 Poniższe punkty dostarczają przykładów miar, które powinny być brane pod uwagę przy ocenianiu ważności w przypadkach, gdy nie są przetwarzane transakcje finansowe:

- Krytyczność procesów biznesowych wspieranych przez system lub eksploatację,
- Koszt systemu lub eksploatacji (sprzętu, oprogramowania, personelu, usług świadczonych przez partnerów zewnętrznych, koszty ogólne, lub kombinacja powyższych),
- Potencjalne koszty błędów (jeśli to możliwe wyrażone w terminach straconej sprzedaży, zobowiązań z tytułu gwarancji, niemożliwych do odzyskania kosztów rozwojowych, kosztów ponoszonych w związku z informowaniem opinii publicznej, kosztów poprawek i korekt, kosztów związanych z kwestiami zdrowotnymi i zapewnieniem bezpieczeństwa, niepotrzebnie wysokich kosztów produkcji, wysokich strat i marnotrawstwa, itp.),
- Liczba wejść/ transakcji/ zapytań przetwarzanych w danym okresie,
- Charakter, terminarz i zakres przygotowanych raportów oraz utrzymywanych plików,
- Charakter i ilości wykorzystanych materiałów (np. w przypadkach , gdy ruch, obieg składników inwentarza jest rejestrowany bez odnotowywania jego wartości),
- Wymagania umów dotyczących poziomów usług i koszty potencjalnych kar,
- Kary za niezachowanie zgodności z wymaganiami prawnymi i wynikającymi z umów,
- Kary za niezachowanie zgodności z wymaganiami dotyczące zdrowia i bezpieczeństwa publicznego.

3. RAPORTOWANIE

3.1.1 Identyfikowanie zagadnień do zaraportowania (raportowalnych)

3.1.2 Podczas określania wyników badań (wykryć), wniosków i rekomendacji, które powinny znaleźć się w raporcie, Audytor SI

- powinien wziąć pod uwagę ważność wszystkich znalezionych błędów i potencjalną ważność błędów, które mogą powstać jako wynik słabości mechanizmów kontrolnych (słabości kontroli).
- 3.1.3** Tam gdzie audyt służy kierownictwu do uzyskania formalnego zapewnienia dotyczącego mechanizmów kontrolnych w SI, opinia bez zastrzeżeń odnośnie adekwatności mechanizmów kontrolnych powinna oznaczać, że istniejące mechanizmy kontrolne są zgodne z szeroko akceptowanymi praktykami kontrolnymi tak by spełniać cele kontrolne oraz są wolne od jakichkolwiek istotnych słabości kontroli (mechanizmów kontrolnych).
- 3.1.4** Słabość kontroli powinna być oceniona jako istotna i stąd właściwa do ujęcia w raporcie, jeśli brak kontroli nie pozwala na rozsądne zapewnienie, że cele kontrolne będą spełnione. Jeśli podczas prac audytowych stwierdzona zostanie istotna słabość kontroli, Audytor SI powinien uwzględnić wydanie opinii z zastrzeżeniami lub opinii negatywnej dotyczącej celu audytu.
- 3.1.5** W zależności od celów danego audytu, Audytor SI powinien rozważyć zaraportowanie kierownictwu słabości mniej istotnych, zwłaszcza jeśli koszty wzmocnienia mechanizmów kontrolnych są niskie.
- 4. DATA OBOWIĄZYWANIA**
- 4.1 Powyższa Wytyczna obowiązuje wszystkie audyty systemów informatycznych rozpoczynające się od dnia 1 sierpnia 1999 roku.**

050.010.020 Planowanie

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

1.1.1 Standard 050.010 (Planowanie audytu) stwierdza „Audytor systemów informatycznych ma zaplanować pracę audytu systemów informatycznych, zajmować się celami kontrolnymi oraz stosować się do profesjonalnych standardów audytowych”.

1.2 Potrzeba wytycznej

1.2.1 Celem tej wytycznej jest określenie składowych procesu planowania jak stwierdzono w Standardzie 050.010 Standardów Audytowania Systemów Informatycznych.

1.2.2 Wytyczna ta również zapewnia, żeby planowanie w ramach procesu audytowego spełniło cele ustanowione przez COBIT.

2. PLANOWANIE

2.1 Wymagania biznesowe

2.1.1 Wytyczna ta odnosi się bardziej do określonego projektu audytu niż do całkowitego planu wydziału lub grupy audytowej.

2.1.2 Audytor SI powinien rozwijać plan audytu, aby wziąć pod uwagę cele strony audytowanej istotne dla audytu i jego technologicznej infrastruktury. Tam gdzie to właściwe, audytor SI powinien rozpatrywać (strategicznie, finansowo, i/lub operacyjnie) przeglądany obszar i jego powiązania z organizacją oraz uzyskać informacje na temat planu strategicznego łącznie ze strategicznym planem SI.

2.1.3 Audytor SI powinien rozumieć architekturę informatyczną i kierunki technologiczne strony audytowanej, aby być w stanie zaprojektować plan odpowiedni dla obecnej, a gdzie to właściwe przyszłej technologii strony audytowanej.

2.1.4 Specyfikacja warunków powinna być elementem planu audytu.

2.1.5 Ocena ryzyka i priorytetyzacja zidentyfikowanych ryzyk dla podlegającego przeglądowi obszaru i środowiska SI organizacji powinny być prowadzone w koniecznym zakresie. Patrz wytyczne audytowania SI Wykorzystanie oceny ryzyka w planowaniu audytu.

2.2 Wiedza o organizacji

2.2.1 Przed rozpoczęciem projektu audytu, praca audytora SI powinna być zaplanowana w odpowiedni, dla spełnienia celów audytowych, sposób. Jako część procesu planowania audytorzy SI powinni posiadać znajomość organizacji i jej procesów. Oprócz zrozumienia przez audytora SI działania organizacji i jej wymagań odnośnie SI, pomoże mu to w określeniu znaczenia zasobów SI podlegających przeglądowi, ??? jak/ ponieważ/ one odnoszą się do celów organizacji. ??? Audytor SI powinien także ustanowić zakres pracy audytowej i wykonać wstępna ocenę kontroli wewnętrznej nad funkcjami podlegającymi przeglądowi.

2.2.2 Zakres wiedzy o organizacji i jej procesach wymagany przez audytora zostanie wyznaczony przez naturę/istotę organizacji oraz poziom szczegółowości, na którym będzie wykonywana praca audytowa. Audytor SI może potrzebować specjalistycznej wiedzy gdy ma do czynienia z niecodziennymi lub złożonymi działaniami. Bardziej rozległa wiedza o organizacji i jej procesach będzie wymagana zazwyczaj, gdy cele audytowe dotyczą szerokiego zasięgu funkcji/działań systemów informatycznych, a nie ograniczonych funkcji/działań. Przykładowo, przegląd mający na celu ocenę kontroli systemu placowego zwykle wymagałby większego zrozumienia organizacji niż przegląd mający na celu testowanie mechanizmów kontrolnych określonego systemu biblioteki programów.

2.2.3 Audytor SI powinien zrozumieć typy zdarzeń, transakcji i praktyk, które mogą mieć znaczący wpływ na określoną organizację, funkcję, proces lub dane, które są przedmiotem projektu audytu. Wiedza o organizacji powinna obejmować ryzyka biznesowe, finansowe i inherentne, które napotykają organizację jak i warunki na rynku organizacji. Powinna także obejmować spełnienie celów w obszarze do przekazywania przez organizację w outsourcing.

2.3 Ważność

2.3.1 W procesie planowania audytora SI powinien zwykle ustalić poziomy planowania ważności/istotności, tak żeby praca audytowa była wystarczająca do spełnienia celów audytowych i efektywnie wykorzystywała zasoby audytowe. Przykładowo, w przeglądzie istniejącego systemu Audytor SI będzie oceniał ważność/istotność różnych składowych systemu w planowaniu programu audytowego dla pracy, która będzie wykonywana. Audytor SI powinien w okraślaniu ważności/istotności rozważyć zarówno aspekty jakościowe jak i ilościowe. Więcej informacji na temat ważności – patrz przewodnik audytora SI „Materiality Concept for Auditing Information System”.

2.4 Ocena ryzyka

2.4.1 Ocena ryzyka powinna być dokonywana by zapewnić, że wszystkie istotne punkty będą poruszone podczas pracy audytowej. Ocena ta powinna rozpoznać obszary występowania stosunkowo wysokiego ryzyka w istotnych problemach.

2.5 Ocena kontroli wewnętrznej

2.5.1 Projekty audytowe powinny obejmować mechanizmy kontroli wewnętrznej zarówno bezpośrednio jako część celów projektu audytowego jak i podstawy, na której opiera się informacja gromadzona jako część projektu audytowego. ??? Gdy celem jest ocena mechanizmów kontrolnych audytor SI powinien rozważyć niezbędny zakres dokonywania przeglądu tych mechanizmów kontrolnych. Gdy celem jest ocena skuteczności mechanizmów kontrolnych w danym okresie czasu, plan audytu powinien zawierać procedury odpowiednie dla spełnienia celów audytowych i procedury te powinny obejmować testy zgodności mechanizmów kontrolnych. Gdy celem nie jest ocena skuteczności mechanizmów kontrolnych w danym okresie czasu, ale raczej rozpoznanie procedur kontrolnych w danym momencie, testowanie zgodności mechanizmów kontrolnych można wylączyć.

2.5.2 Gdy audytor SI ocenia mechanizmy kontrolne w celu określenia w jakim stopniu można polegać na procedurach kontrolnych we wsparciu informacji gromadzonej jako część audytu, audytor SI zwykle powinien dokonać wstępnej oceny mechanizmów kontrolnych i rozwinąć plan audytu na podstawie tej oceny. Podczas przeglądu audytor SI rozważy jak odpowiednia/właściwa jest ta ocena w określeniu stopnia polegania na mechanizmach kontrolnych podczas testów. Przykładowo w użyciu

programów komputerowych do testowania zbiorów danych, audytor SI powinien ocenić mechanizmy kontrolne nad bibliotekami programowymi zawierającymi programy używane dla celów audytowych aby ustalić w jakim stopniu programy są chronione przed nieautoryzowaną zmianą.

3. DOKUMENTACJA

3.1 Dokumentacja planowania

3.1.1 Dokumentacja robocza audytora SI powinna obejmować plan i program audytu.

3.1.2 Plan audytu można być opisany w formie papierowej lub innej, odpowiedniej i dającej się odzyskać formie.

3.2 Poparcie planu

3.2.1 Aby określić właściwy zakres, plan audytu, program audytu i wszystkie późniejsze zmiany powinny zostać zaakceptowane przez zarządzających audytem

4. PROGRAM AUDYTU

4.1.1 Wstępny program przeglądu powinien być zazwyczaj ustanowiony przez audytora SI przed rozpoczęciem pracy. Program audytu powinien zostać opisany w sposób, który pozwoli audytorowi SI zapisać ukończenie pracy audytowej oraz określić pozostałą do wykonania pracę. W miarę postępu pracy, audytor SI powinien oceniać odpowiedność programu opartego na informacji gromadzonej podczas audytu. Gdy audytor SI stwierdza, że zaplanowane procedury nie są wystarczające, powinien odpowiednio zmodyfikować program.

4.1.2 W zależności od wymaganych przez audyt zasobów, audytor SI powinien włączyć w skład planu audytu kierownictwo wymaganych zasobów ludzkich. Plan audytu powinien zostać tak przygotowany, aby był zgodny z innymi odpowiedziami, zewnętrznymi wymaganiami oprócz Standardów Audytu SI.

4.1.3 Oprócz wypisania listy prac do wykonania, audytor SI powinien w celu wykonania przewidzianego zakresu przygotować listę personelu i innych zasobów wymaganych do ukończenia pracy, harmonogram pracy i budżetu.

4.1.4 Podczas biegu prac, audytor SI powinien rozważyć zmiany do programu audytu w oparciu o audytorską ocenę odpowiedności programu i wstępnych wniosków audytora.

4.2 DATA WEJŚCIA W ŻYCIE

4.3 Wytuczna jest obowiązująca dla wszystkich audytów systemów informatycznych rozpoczętych w dniu 1 marca 2002 r. i później.

050.010.030 Ocena ryzyka podczas planowania audytu

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

- 1.1.1 Standard 050.010 – planowanie audytu: audytor systemów informatycznych ma tak planować prace audytu informatycznego, aby sprostać obowiązującym standardom i zrealizować określone cele audytu.
- 1.1.2 Standard 060.020. – dowody: podczas przeprowadzania audytu, audytor systemów informatycznych jest zobowiązany do tego, aby uzyskać wystarczające, wiarygodne i odpowiednie dowody, aby w efektywny sposób osiągnąć cel audytu. Konkluzje i wyniki audytu powinny być wsparte przez odpowiednie analizy i interpretacje zidentyfikowanych dowodów.
- 1.1.3 Paragraf 2.2.2 – wytyczne dotyczące planowania audytu: ocena ryzyka powinna być przeprowadzona w taki sposób, aby zapewnić, iż istotne kwestie i problemy zostaną objęte zakresem prac audytowych. Ocena powinna identyfikować obszary o relatywnie wysokim ryzyku pojawienia się istotnych kwestii i problemów.

1.2 Potrzeba wytycznej

- 1.2.1 Zakres prac wykonywanych w ramach audytu informatycznego, niezbędny do osiągnięcia specyficznych celów audytowych zależy od subiektywnej decyzji audytora. Ryzyko wyciągnięcia niewłaściwych wniosków (ryzyko audytowe) na podstawie wyników audytu informatycznego jest jednym z aspektów tej decyzji. Innym aspektem jest ryzyko błędu, występującego w audytowanych obszarach. Rekomendowane praktyki dotyczące oceny ryzyka, przy przeprowadzaniu audytu finansowego zostały dokładnie udokumentowane w standardach audytowych dla audytorów finansowych. Niezbędne są jednak wskazówki określające jak zastosować te praktyki do prowadzenia audytów informatycznych.
- 1.2.2 Kadra zarządzająca opiera swoje decyzje odnośnie wymaganego zakresu kontroli na wynikach oceny poziomu ryzyka, które jest gotowa zaakceptować. Np. niemożność użytkowania aplikacji przez dany okres czasu, może być rezultatem nieoczekiwanego i niepożądanego wypadku (np. pożar serwerowni). Skutki wystąpienia ryzyka mogą być zredukowane przez implementację odpowiednio zaprojektowanych kontroli. Kontrole te najczęściej wynikają z prawdopodobieństwa wystąpienia niepożądanych zdarzeń lub sytuacji i służą obniżeniu tego prawdopodobieństwa. Np. alarm przeciwpożarowy nie eliminuje ryzyka wystąpienia pożaru, ale znacząco zmniejsza straty przez niego spowodowane.
- 1.2.3 Niniejsze wskazówki dostarczają wytycznych pomocnych w stosowaniu standardów dotyczących audytu systemów informatycznych. Audytor systemów informatycznych powinien je wziąć pod uwagę określając sposób wdrożenia powyższych standardów, posługiwać się profesjonalną oceną każdej sytuacji w czasie stosowania tych standardów oraz być przygotowanym na wyjaśnienie wszelkich odstępstw.

2. PLANOWANIE

2.1 Wybór metodologii oceny ryzyka

- 2.1.1 Występuje wiele metodologii oceny ryzyka, wykorzystujących zarówno techniki komputerowe jak i metody tradycyjne, z których każdy audytor może wybrać najkorzystniejszą. Zakres dostępnych metodologii jest bardzo szeroki, poczynając od prostej klasyfikacji, opartej na ocenie ryzyka na wysokie, średnie, niskie, a kończąc na metodach opartych o złożone obliczenia, których wynikiem jest ilościowa ocena ryzyk. Audytor systemów informatycznych powinien zastosować metodologię adekwatną dla audytowanej firmy, biorąc pod uwagę stopień skomplikowania i szczegółowość wybranej metodologii.
- 2.1.2 Wszystkie metodologie oceny ryzyka zawierają element subiektywnej oceny na pewnym etapie procesu (np. przydział wag poszczególnym parametrom). Audytor systemów informatycznych powinien identyfikować subiektywne decyzje mające wpływ na zastosowania określonych metodologii i rozważyć, czy decyzje te zostały podjęte z odpowiednim poziomem dokładności.
- 2.1.3 Przy określeniu najbardziej odpowiedniej metodologii oceny ryzyk, audytor systemów informatycznych powinien rozważyć następujące kwestie:
 - Rodzaj informacji, którą należy zgromadzić (pewne systemy używają wskaźników finansowych jako jedyne miernika, co nie zawsze jest właściwe w przypadku audytu systemów informatycznych),
 - Koszt oprogramowania lub innych licencji niezbędnych do zastosowania określonej metodologii,
 - Dostępność wymaganej informacji,
 - Ilość dodatkowych informacji niezbędnych do osiągnięcia wiarygodnego wyniku oceny łącznie z kosztem uzyskania tych informacji (włączając czas potrzebny do zebrania tych informacji).
 - Opinie innych użytkowników danej metodologii i ich zdanie na temat przydatności danej metodologii w zwiększeniu efektywności przeprowadzonych audytów,
 - Gotowość zarządu do zaakceptowania danej metodologii jako środka określającego sposób i zakres przeprowadzanych prac audytowych.
- 2.1.4 Żadna metodologia oceny ryzyk nie może być adekwatna do wszystkich rozwiązań. Warunki wpływające na audyt mogą się zmieniać w czasie. Okresowo, audytor systemów informatycznych powinien dokonywać ponownej oceny przydatności danej metodologii oceny ryzyk.

2.2 Zastosowanie oceny ryzyka

- 2.2.1 Audytor systemów informatycznych powinien stosować wybraną metodę oceny ryzyka planując prace audytowe. Ocena ryzyka, w połączeniu z innymi technikami audytowymi, powinna być wykorzystywana w procesie planowania audytu informatycznego, a w szczególności:
 - istoty, zakresu i ram czasowych procedur audytowych,
 - obszarów lub funkcji biznesowych podlegających audytowi,
 - ilości czasu i zasobów niezbędnych do zrealizowania danego audytu.
- 2.2.2 Audytor systemów informatycznych powinien rozważyć każdy z następujących typów ryzyka, aby ocenić ogólny poziom ryzyka:
 - Ryzyko wewnętrzne (Inherent Risk),

- Ryzyko kontroli (Control Risk),
 - Ryzyko detekcji (Detection Risk).
- 2.3 Ryzyko wewnętrzne**
- 2.3.1** Ryzyko wewnętrzne jest to podatność na wystąpienie istotnego błędu, który sam lub w połączeniu z innymi błędami będzie miał istotny wpływ na analizowany obszar, przy braku odpowiednich kontroli wewnętrznych. Przykładowo, ryzyko wewnętrzne związane z bezpieczeństwem systemu operacyjnego jest zazwyczaj wysokie, gdyż zmiany lub ujawnienie danych lub programów w wyniku słabości bezpieczeństwa systemu operacyjnego mogą powodować generowanie niewłaściwych informacji dla zarządu lub utratę przewagi konkurencyjnej. Przeciwnie, ryzyko wewnętrzne związane z bezpieczeństwem wolnostojącego komputera klasy PC, który nie jest wykorzystywany w kluczowych obszarach, jest najczęściej niskie.
- 2.3.2** Ryzyko wewnętrzne, dla większości obszarów podlegających audytowi, jest na ogół wysokie, gdyż efekt potencjalnego błędu w tych obszarach zahacza o wiele systemów i wielu użytkowników.
- 2.3.3** Przy ocenie ryzyka wewnętrznego, audytor systemów informatycznych powinien rozważyć zarówno ogólne, jak i szczegółowe kontrole systemów informatycznych. Zasada ta nie jest stosowana w sytuacjach, gdy zakres pracy audytora systemów informatycznych dotyczy tylko kontroli ogólnych.
- 2.3.4** Na poziomie ogólnych kontroli systemów informatycznych, audytor powinien wziąć pod uwagę następujące kwestie, uwzględniając jednocześnie specyfikę danego audytu:
- Spójność zarządzania systemami informatycznymi, jak również doświadczenie i wiedza związana z zarządzaniem systemami informatycznymi,
 - Zmiany w zarządzaniu systemami informatycznymi,
 - Presja na osoby zarządzające systemami informatycznymi, która może powodować ukrywanie bądź nieprawdziwą prezentację posiadanych informacji (np. przedłużanie się projektów o dużym znaczeniu dla firmy, działalność hakerów),
 - Istota prowadzonego biznesu i systemów obecnych w danej organizacji (np. plany związane z e-commerce, poziom skomplikowania systemów i niezintegrowane systemy),
 - Czynniki wpływające na branżę, w której działa dana organizacja (np. zmiana wykorzystywanej technologii, dostępność pracowników związanych z systemami informatycznymi),
 - Zakres wpływu „stron trzecich” na kontrolę audytowanych systemów (np. integracja kanału dostaw, outsourcing procesów związanych z systemami informatycznymi, wspólne przedsięwzięcia „joint-ventures”, bezpośredni dostęp klientów do systemów),
 - Informacje uzyskane podczas poprzednich audytów.
- 2.3.5** Na poziomie szczegółowej kontroli systemów informatycznych, audytor systemów informatycznych powinien rozważyć następujące kwestie, uwzględniając jednocześnie specyfikę danego audytu:
- Wyniki (wykrycia) oraz daty poprzednich audytów w danym obszarze.
 - Poziom skomplikowania systemów,
 - Poziom wymaganej manualnej interwencji w systemach informatycznych,
 - Podatność na utratę lub sprzeniewierzenie aktywów kontrolowanych przez system (np. zapasy, lista plac),
 - Prawdopodobieństwo wystąpienia szczytu aktywności w trakcie audytu,
 - Działania, różniące się od codziennych działań, związanych z przetwarzaniem danych (np. użycie systemów operacyjnych do wprowadzania zmian do danych),
 - Uczciwość, doświadczenie i wiedza osób zarządzających i obsługujących systemy informatyczne, we wdrażaniu odpowiednich kontroli nad systemami informatycznymi.
- 2.4 Ryzyko kontroli**
- 2.4.1** Ryzyko kontroli jest to ryzyko, polegające na braku możliwości uniknięcia błędu, jego wykrycia i skorygowania we właściwym czasie przez system kontroli wewnętrznej. Np. ryzyko kontroli związane z manualnym przeglądem „logów” może być wysokie, ponieważ zdarzenia, które powinny zostać poddane kontroli są często pomijane ze względu na dużą ilość informacji zawartych w „logach”. Z kolei ryzyko kontroli odnoszące się do procedur komputerowej walidacji danych jest zazwyczaj niskie, gdyż odpowiednie procesy są realizowane na bieżąco i w sposób ciągły.
- 2.4.2** Audytor systemów informatycznych powinien oceniać ryzyko kontroli jako wysokie dopóki odpowiednie kontrole wewnętrzne nie zostaną:
- zidentyfikowane,
 - ocenione jako efektywne,
 - przetestowane i sprawdzone jako działające prawidłowo.
- 2.5 Ryzyko detekcji**
- 2.5.1** Ryzyko detekcji jest ryzykiem polegającym na tym, iż analityczne procedury audytowe nie ujawnią błędu, który sam lub w połączeniu z innymi błędami będzie miał istotny wpływ na analizowany obszar. Np. ryzyko detekcji związane z identyfikacją naruszenia bezpieczeństwa aplikacji jest na ogół wysokie, ponieważ nie wszystkie logi odnoszące się do okresu poddanego audytowi są dostępne w czasie przeprowadzania prac audytowych. Z kolei ryzyko detekcji związane z wykryciem braku planów ciągłości działalności jest zazwyczaj niskie, ze względu na łatwą weryfikację ich istnienia.
- 2.5.2** Określając właściwy zakres testów analitycznych audytor systemów informatycznych powinien rozważyć następujące czynniki:
- ocenę ryzyka wewnętrznego,
 - wnioski wynikające z ryzyka kontroli, na podstawie wyników testów zgodności.
- 2.5.3** Im wyższe ryzyko wewnętrzne i ryzyko kontroli, tym więcej dowodów powinien zebrać audytor systemów informatycznych w czasie prowadzonych procedur audytowych.
- 3. PROWADZENIE PRAC**
- 3.1 Dokumentacja**
- 3.1.1** Audytor systemów informatycznych powinien rozważyć sposób udokumentowania stosowanych technik i przyjętej metodologii

oceny ryzyka zastosowanych podczas prac audytowych. Dokumentacja powinna zawierać:

- Opis wykorzystanej metodologii oceny ryzyka,
- Identyfikację istotnych zagrożeń i związanych z nimi ryzyk,
- Zagrożenia i ryzyka, które mają zostać poddane analizie podczas audytu,
- Dokumentację i dowody zebrane podczas audytu, obrazujące sposób oceny ryzyk.

4. DATA OBOWIĄZYWANIA

5. Powyższe wskazówki stają się obowiązujące dla wszystkich audytów systemów informatycznych począwszy od 1 września 2000 roku.

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

1.1.1 Standard 050.010 – (Planowanie Audytu): „Audytor systemów informatycznych ma tak planować prace audytu informatycznego, aby sprostać obowiązującym standardom i zrealizować określone cele audytu”.

1.1.2 Standard 060.020. – (Dowody): „Podczas przeprowadzania audytu, audytor systemów informatycznych jest zobowiązany do tego, aby uzyskać wystarczające, wiarygodne i odpowiednie dowody, aby w efektywny sposób osiągnąć cel audytu. Konkluzje i wyniki audytu powinny być poparte odpowiednimi analizami i interpretacjami zidentyfikowanych dowodów.”

1.2 Definicje

1.2.1 ISP—(Internet service provider) Dostawca usług internetowych: Strona trzecia dostarczająca organizacji różne usługi internetowe lub związane z Internetem

1.2.2 ASP/MSP—(application or managed service provider) Dostawca usług aplikacyjnych: Strona trzecia dostarczająca i zarządzająca usługami aplikacyjnymi i komputerowymi, uwzględniając w tym usługi związane z bezpieczeństwem dla wielu użytkowników z wykorzystaniem Internetu lub sieci prywatnych.

1.2.3 BSP—(business service provider) Dostawca usług biznesowych: Dostawca usług aplikacyjnych, dostarczający również usługi zewnętrzne dla procesów biznesowych takich jak: przetwarzanie płatności, przetwarzanie zamówień i rozwój aplikacji.

1.2.4 Wytyczna do dostawców typu ISP, ASP/MSP i BSP odnosi się wspólnie jako do stron trzecich. W ramach tej wytycznej nazwa - strona trzecia - uwzględnia każdą organizację, która jest oddzielna wobec (badanej) organizacji (tak jak organizacje dzielące usługi – dzielące się usługami) (*such as shared service organisations*), obojętne czy jest to rozdzielnosc z punktu widzenia prawa czy nie.

1.3 Zastosowanie wytycznej

1.3.1 Stosując tą wytyczną, audytor IT powinien rozważyć jej wskazówki w powiązaniu z innymi adekwatnymi wytycznymi ISACA.

1.4 Potrzeba wytycznej

1.4.1 Wytyczna określa zgodny ze standardami ISACA i COBITem sposób postępowania audytora IT podczas oceny wpływu stron trzecich na mechanizmy kontrolne IT organizacji oraz powiązane cele kontrolne. (*This guideline sets out how the IS auditor should comply with the ISACA Standards and COBIT when assessing the effect a third party has on an organisation's information system controls and related control objectives.*)

1.4.2 Wytyczna ta nie jest przewidziana jako źródło wskazówek na temat raportowania audytora IT odnośnie mechanizmów kontrolnych zewnętrznego usługodawcy w zgodzie ze standardami innych organizacji. *This guideline is not intended to provide guidance on how IS auditor's report on third-party provider controls in accordance with other standard setting entities.*

2. ROLA ZEWNĘTRZNYCH USŁUGODAWCÓW

2.1 Usługi dostarczane przez strony trzecie

2.1.1 Organizacje używają Internetu i Intranetów korporacyjnych do różnych celów. Uwzględnione jest w tym dostarczanie pracownikom, sprzedawcom i klientom dostępu do istniejących i/lub nowych aplikacji kadrowych, księgowych, obsługujących zakupy i sprzedaż. Dostęp ten, w wielu wypadkach, jest zapewniany przez jedną lub więcej stron trzecich.

2.1.2 Strony trzecie mogą dostarczać następujących usług:

- Łączność sieci wewnętrznych z Internetem
- Łączność z partnerami biznesowymi poprzez wirtualne sieci prywatne (VPN) lub extranety
- Łączność z klientami z użyciem technologii (łączności) bezprzewodowej
- Opracowywanie stron Web
- Utrzymanie, zarządzanie i monitorowanie stron Web
- Usługi związane z bezpieczeństwem stron Web
- Zapewnianie fizycznej lokalizacji dla sprzętu (tzw. co-location)
- Monitorowanie dostępu do systemu i aplikacji
- Usługi składowania i odtwarzania
- Rozwój aplikacji, zarządzanie i udostępnianie (takich jak systemy ERP, handlu elektronicznego)
- Usługi biznesowe z uwzględnieniem przetwarzania płatności, zamówień, obsługi kart kredytowych i usług call center

3. WPŁYW NA MECHANIZMY KONTROLNE

3.1 Wpływ zewnętrznych usługodawców na mechanizmy kontrolne

3.1.1 W sytuacji współpracy organizacji z usługodawcami, mogą się oni stać kluczowymi elementami w systemie kontrolnym organizacji i osiągnięciu adekwatnych celów kontrolnych.

3.1.2 Audytor IT powinien ocenić rolę, jaką pełni usługodawca w ramach środowiska IT, adekwatnych mechanizmów i celów kontrolnych.

3.1.3 W sytuacji ograniczonej współpracy organizacji z usługodawcami, takiej jak usługa typu co-location (kolokacja, ko-lokalizacja), może ona jedynie w ograniczonym stopniu polegać na usługodawcy w osiągnięciu swoich celów kontrolnych. (*An organisation that uses third-party providers for limited purposes, such as co-location services, may rely upon these third parties for only limited purposes in achieving its control objectives.*)

3.1.4 Jednakże, w sytuacji współpracy z usługodawcą w innych celach, takich jak udostępnianie systemów finansowo-księgowych i

systemów handlu elektronicznego, organizacja wykorzystuje mechanizmy kontrolne usługodawcy w pełni lub w połączeniu z własnymi tak, aby osiągnąć swoje cele kontrolne.

3.1.5 Skuteczność mechanizmów kontrolnych usługodawcy może zwiększyć zdolność organizacji do osiągnięcia swoich celów kontrolnych i przeciwnie, nieskuteczne mechanizmy kontrolne usługodawcy mogą osłabić zdolność organizacji do osiągnięcia swoich celów kontrolnych. Słabości te mogą pochodzić z wielu źródeł z uwzględnieniem następujących:

- Luki w środowisku kontrolnym powstające przy zleceniu usług do realizacji na zewnątrz (outsourcing)
- Niewłaściwy projekt mechanizmów kontrolnych powodujący nieskuteczność ich działania
- Brak wiedzy i/lub doświadczenia osób odpowiedzialnych za funkcjonowanie mechanizmów kontrolnych
- Nadmierne poleganie na mechanizmach kontrolnych usługodawcy (jeśli nie ma kompensacyjnych mechanizmów kontrolnych wewnątrz organizacji).

4. PROCEDURY DO WYKONANIA PRZEZ AUDYTORA IT

4.1 Zrozumienie

4.1.1 Jako część procesu planowania, audytor IT powinien uzyskać i udokumentować zrozumienie relacji pomiędzy usługami dostarczonymi przez firmę trzecią a środowiskiem kontrolnym organizacji. Audytor IT powinien wziąć pod uwagę przegląd takich rzeczy jak kontrakt, SLA, polityki i procedury pomiędzy usługodawcą a organizacją.

4.1.2 Audytor IT powinien udokumentować procesy i mechanizmy kontrolne usługodawcy, które mają bezpośredni wpływ na procesy organizacji i jej cele kontrolne.

4.1.3 Audytor IT powinien zidentyfikować każdy mechanizm kontrolny, jego umiejscowienie w układzie środowiska kontrolnego (zewnętrznego lub wewnętrznego), typ kontroli, jej funkcję (prewencja, detekcja, korekcja) i organizację, która ją wykonuje (zewnętrzna lub wewnętrzna).

4.1.4 Audytor IT powinien oszacować ryzyko usług dostarczanych dla organizacji przez firmy trzecie, ich mechanizmy i cele kontrolne oraz określić znaczenie mechanizmów kontrolnych usługodawcy dla zdolności organizacji w osiągnięciu swoich celów kontrolnych.

4.2 Potwierdzenie zrozumienia

4.2.1 Audytor IT powinien potwierdzić swoje zrozumienie środowiska kontrolnego.

4.2.2 Audytor IT może potwierdzić swoje zrozumienie środowiska kontrolnego różnymi metodami uwzględniając takie jak przedstawianie pytań, obserwacja, śledzenie przebiegu transakcji.

4.3 Ocena mechanizmów kontrolnych zewnętrznego usługodawcy

4.3.1 Jeśli rola lub wpływ firmy trzeciej na cele kontrolne organizacji jest znaczący, to audytor IT powinien oszacować te mechanizmy kontrolne, aby ocenić czy funkcjonują tak jak zostały zaprojektowane, działają skutecznie i są pomocne dla organizacji w osiągnięciu jej celów kontrolnych.

5. RYZYKA ZWIĄZANE Z ZEWNĘTRZNYMI USŁUGODAWCAMI

5.1 Wpływ zewnętrznych usługodawców na organizację

5.1.1 Zewnętrzni usługodawcy mogą wpływać na organizację (a także jej partnerów biznesowych), jej procesy, mechanizmy i cele kontrolne na wielu różnych poziomach. Uwzględniony jest przy tym wpływ wynikający z:

- "Ekonomicznej żywotności" usługodawcy
- Dostępu usługodawcy do informacji przesyłanej przez jej systemy komunikacyjne i aplikacje
- Dostępności systemów i aplikacji
- Integralności przetwarzania
- Procesów rozwoju aplikacji i zarządzania zmianami
- Ochrony systemów i zasobów informacyjnych za pomocą składowania/odtworzenia, planowania ciągłości działania i nadmiarowości.

5.1.2 Brak mechanizmów kontrolnych i/lub ich słabość w projekcie, działaniu lub skuteczności może prowadzić do:

- Utraty poufności i prywatności informacji
- Niedostępności systemów w momencie, gdy są potrzebne
- Nieautoryzowanego dostępu i zmian w systemach, aplikacjach lub danych
- Zmian w systemach, aplikacjach lub danych będących wynikiem awarii systemu, awarii w systemie zabezpieczeń, utraty danych, utraty integralności danych, utraty ochrony danych lub niedostępności systemu
- Utraty zasobów systemu i/lub aktywów związanych z informacją
- Zwiększonych kosztów na jakie narażona jest organizacja w wyniku dowolnej z w/w sytuacji

5.2 Ocena zaobserwowanych słabości mechanizmów kontrolnych

5.2.1 Audytorzy IT powinni oszacować prawdopodobieństwo (lub ryzyko kontroli) tego, że słabość w występowaniu, projekcie lub działaniu mechanizmu kontrolnego może istnieć w środowisku IT. Audytor IT powinien zidentyfikować, gdzie występuje słabość mechanizmu kontrolnego.

5.2.2 Audytor IT powinien następnie oszacować czy ryzyko kontroli jest znaczące i jaki ma wpływ na środowisko kontrolne.

5.2.3 Jeśli słabości są zidentyfikowane, audytor IT powinien także ocenić, czy istnieją kontrole kompensacyjne dla zniwelowania wpływu zidentyfikowanych słabości (kontrole kompensacyjne mogą występować zarówno w organizacji, firmie trzeciej jak i w obu jednocześnie). Jeśli kontrole kompensacyjne występują, audytor IT powinien ocenić czy niwelują one wpływ zidentyfikowanych słabości mechanizmów kontrolnych.

6. KONTRAKTY Z ZEWNĘTRZNYMI USŁUGODAWCAMI

6.1 Role i zakresy odpowiedzialności

6.1.1 Relacje pomiędzy organizacją a firmą zewnętrzną powinny być udokumentowane w formie wykonywanego kontraktu.

Kontrakt jest elementem krytycznym w relacji pomiędzy organizacją a dostawcą usługi. Kontrakty te zawierają szereg postanowień, rządzące działaniami i odpowiedzialnością każdej ze stron.

6.1.2 Audytor IT powinien przejrzeć kontrakt pomiędzy organizacją i firmą trzecią.

6.1.3 W kontekście tej wytycznej, audytor IT powinien przejrzeć (o ile to możliwe z pomocą doradcy prawnego organizacji) aby określić rolę firmy trzeciej i odpowiedzialność w ramach pomocy organizacji w osiąganiu jej celów kontrolnych. Wskazówki nt. jak przeglądać kontrakt pozostają poza zakresem tej wytycznej; jednakże następująca lista przedstawia przykłady zagadnień, które powinny być wzięte pod uwagę przez audytora IT w trakcie przeglądania kontraktu:

- Poziom usługi jaki ma być zapewniony przez usługodawcę (zarówno dla organizacji, jej partnerów jak i obu jednocześnie)
- Uzasadnienie opłat naliczanych przez usługodawcę
- Odpowiedzialność za poufność i prywatność danych i aplikacji
- Odpowiedzialność mechanizmów kontrolnych dotyczące dostępu i administrowania systemem, kanałami komunikacyjnymi, systemem operacyjnym, oprogramowaniem użytkowym, danymi i oprogramowaniem aplikacyjnym
- Monitorowanie aktywów i powiązanych z nimi danych oraz procedury reakcji (organizacji i strony trzeciej) i raportowania (standardowego, nt. incydentów)
- Specyfikacja własicielstwa aktywów uwzględniając nazewnictwo danych i domen
- Specyfikacja własicielstwa oprogramowania na zamówienie opracowanego dla organizacji przez stronę trzecią uwzględniając dokumentację zmian, kod źródłowy i umowy typu escrow
- Postanowienia dotyczące ochrony systemów i danych włączając w to składowanie i odtwarzanie, planowanie ciągłości działania i nadmiarowość
- Klauzula zawierająca prawo do audytu (włączając w to możliwość spotkania z audytorami wewnętrznymi usługodawcy i przeglądu ich dokumentacji audytowej i raportów)
- Proces negocjacji, przeglądu i zatwierdzania zmian w kontrakcie i powiązanych dokumentach (takich jak SLA i procedury)

6.1.4 Jako minimum, audytor IT powinien przejrzeć kontrakt aby określić obszar odpowiedzialności za mechanizmy kontrolne, który strona trzecia przejęła w imieniu organizacji. Ten proces powinien oszacować adekwatność zidentyfikowanych mechanizmów kontrolnych i monitorowania/raportowania zgodności z nimi, ich projekt skuteczność działania.

6.2 Zarządzanie korporacyjne

6.2.1 Nawet wtedy, gdy zaangażowani są usługodawcy zewnętrzni, kierownictwo jest nadal odpowiedzialne za osiągnięcie adekwatnych celów kontrolnych. Jako jeden z elementów tej odpowiedzialności kierownictwo powinno dysponować procesem rządzenia relacjami z usługodawcą i jego sposobem działania. Audytor IT powinien zidentyfikować i przejrzeć komponenty tego procesu. Audytor IT powinien przejrzeć takie aspekty jak proces zarządzania traktuje identyfikację ryzyk związanych z usługodawcą zewnętrznym, usługi dostarczane przez stronę trzecią oraz jak kierownictwo rządzi relacjami pomiędzy dwiema instytucjami.

6.2.2 Przegląd procesu zarządzania powinien stwierdzić czy kierownictwo dokonuje przeglądów usługodawców zewnętrznych w stosunku do standardów wydajności lub zestawu kryteriów ustalonych w kontrakcie oraz innych standardach określonych przez ciała regulujące. Proces rządzenia powinien zawierać przegląd takich elementów jak:

- Finansowy status usługodawcy
- Zgodność z warunkami kontraktu
- Zmiany w środowisku kontrolnym zalecone przez stronę trzecią, jego audytorów i/lub regulatorów
- Rezultaty przeglądów kontrolnych przeprowadzonych przez innych z uwzględnieniem audytorów usługodawcy, konsultantów lub innych
- Zarządzanie adekwatnością poziomu zabezpieczeń

7. PRZEGLĄD MECHANIZMÓW KONTROLNYCH ZEWNĘTRZNYCH USŁUGODAWCÓW

7.1 Aspekty kontraktowe

7.1.1 Podczas przeglądu mechanizmów kontrolnych usługodawcy, audytor IT powinien wziąć pod uwagę kontraktowe relacje pomiędzy organizacją i usługodawcą zewnętrznym, ocenę usługodawcy i raportowanie nt. swoich mechanizmów kontrolnych.

7.1.2 Postanowienia kontraktowe mogą wykluczyć możliwość przeglądu mechanizmów kontrolnych usługodawcy przez audytora IT. W tej sytuacji, audytor IT powinien ocenić wpływ tego ograniczenia zakresu na swoją zdolność do oceny środowiska kontrolnego IT.

7.2 Niezależne raporty

7.2.1 Usługodawcy zewnętrzni mogą przedstawiać raporty pochodzące z niezależnych źródeł nt. swoich mechanizmów kontrolnych. Takie raporty mogą mieć formę raportów z biura świadczącego usługi audytowe lub innych raportów control-based. Audytor IT może użyć tych raportów jako podstawy dla budowania swojego zaufania do środowiska kontrolnego IT.

7.2.2 Jeśli audytor IT decyduje się na użycie niezależnego raportu jako podstawy zaufania do mechanizmów kontrolnych IT u usługodawcy, to powinien przejrzeć te raporty w celu sprawdzenia następujących spraw:

- Strona niezależna ma odpowiednie kwalifikacje. Uwzględnia się tutaj czy strona niezależna posiada odpowiednie profesjonalne certyfikacje, ma należyte doświadczenie i zajmuje dobrą pozycję w ocenie odpowiednich profesjonalnych i regulujących (jeśli mają w tym przypadku znaczenie) autorytetów.
- Strona niezależna nie pozostaje z usługodawcą w żadnej relacji, która mogłaby naruszyć niezależność i obiektywizm
- Okres czasu, który raport obejmuje

- Czy raport jest wystarczający (tzn., raport obejmuje odpowiednie systemy i mechanizmy kontrolne i zawiera testy obszarów, które zostałyby włączone przez audytora IT w celu wykonania zadania)
- Czy testowanie mechanizmów kontrolnych jest odpowiednie, aby audytor IT mógł polegać na pracy strony niezależnej (tzn. Testowanie mechanizmów kontrolnych jest odpowiednie w swojej naturze, czasie i zakresie)
- Raport wyraźnie rozróżnia pomiędzy odpowiedzialnością usługodawcy i organizacją użytkownika
- Organizacja użytkownika określiła i przypisała swoją odpowiedzialność za odpowiednie mechanizmy kontrolne

7.3 Testowanie mechanizmów kontrolnych stron trzecich

7.3.1 Jeśli audytor IT zdecyduje się na bezpośredni przegląd i testowanie mechanizmów kontrolnych usługodawcy powinien wykonać następujące rzeczy:

- Współpracować z kierownictwem i, jeśli to możliwe lub brane pod uwagę jako odpowiednie, z audytem wewnętrznym obu organizacji w celu zaplanowania zadania audytowego, ustalenia jego celów i zakresu przeglądu
- Współpracować z kierownictwem i, jeśli to możliwe lub brane pod uwagę jako odpowiednie, z audytem wewnętrznym obu organizacji w celu określenia harmonogramu, zasobów ludzkich i innych zagadnień
- Określić zarówno takie zagadnienia jak dostęp do systemów i zasobów usługodawcy, jak i poufność
- Opracować program audytu, budżet i plan umowy o badanie
- Zweryfikować cele kontrolne

7.3.2 Po zakończeniu prac audytowych (*fieldwork*) audytor IT powinien opracować wnioski nt. operacyjnej skuteczności przetestowanych mechanizmów kontrolnych. Audytor IT powinien sprawdzić skuteczność mechanizmów kontrolnych w każdej organizacji i współdziałanie mechanizmów kontrolnych pomiędzy organizacją a stroną trzecią.

7.3.3 W większości sytuacji, mechanizmy kontrolne będą zachodzić na siebie pomiędzy organizacją a stroną trzecią. Audytor IT powinien ocenić operacyjną skuteczność mechanizmów kontrolnych w całości jak i dla każdego z osobna.

7.3.4 Może występować również sytuacja, w której mechanizmy kontrolne dla szczególnego celu kontrolnego nie będą istniały w żadnej organizacji lub będą nieskuteczne. W tej sytuacji audytor IT powinien oszacować wpływ tej słabości na całość środowiska kontrolnego i ogółu procedur. *Situations may also exist where controls for a particular objective in either organisation may not exist or do not operate effectively. In this situation, the IS auditor should assess the effect this weakness has on the overall control environment and on the extent of their procedures.*

7.3.5 Może wystąpić również sytuacja, w której siła mechanizmów kontrolnych jednej organizacji jest częściowo lub całkowicie zniwelowana przez słabość mechanizmów kontrolnych drugiej organizacji. Odpowiedzialnością audytora IT w tej sytuacji jest ocena wpływu na całość środowiska kontrolnego.

7.4 Wewnętrzni audytorzy zewnętrznych usługodawców

7.4.1 Audytor IT powinien również wziąć pod uwagę czy usługodawca posiada audyt wewnętrzny. Obecność audytorów wewnętrznych u usługodawcy może zwiększyć siłę środowiska kontrolnego usługodawcy zewnętrznego.

7.4.2 Jeśli audyt wewnętrzny istnieje, audytor IT powinien rozważyć zakres ich działań w odniesieniu do systemów i mechanizmów kontrolnych, które mogą mieć wpływ na organizację.

7.4.3 Jeśli to możliwe, audytor IT powinien przejrzeć odpowiednie raporty audytu wewnętrznego usługodawcy.

7.4.4 W sytuacji, w której nie jest możliwe przejrzanie tych raportów, audytor IT powinien przedyskutować zakres tych przeglądów, zidentyfikować które systemy i mechanizmy kontrolne były objęte tymi przeglądami i jakie istotne zagadnienia i słabości zidentyfikowano.

7.4.5 Jeśli usługodawca nie umożliwia dostępu do raportów lub pracowników audytu wewnętrznego, audytor IT powinien uwzględnić to ograniczenie w zakresie swoich procedur.

7.4.6 Audytor IT powinien również wziąć pod uwagę ocenę umiejętności i biegłość pracowników audytu wewnętrznego usługodawcy. Może być to wykonane przez rozmowy w pracownikami i inne procedury takie jak przegląd ich planów audytowych, dokumentacji roboczej i raportów.

8. PODWYKONAWCY STRON TRZECICH

8.1 Wpływ na mechanizmy kontrolne

8.1.1 Audytor IT powinien wziąć pod uwagę czy strona trzecia wykorzystuje podwykonawców dla dostarczenia systemów i usług.

8.1.2 W sytuacji występowania podwykonawców, audytor IT powinien przejrzeć znaczenie tych podwykonawców, aby określić wpływ jaki mogą mieć na podstawowe mechanizmy kontrolne strony trzeciej będące w relacji z organizacją.

8.2 Wpływ na umowę o przeprowadzenie audytu, badania (o badanie ?????)

8.2.1 Jeśli podwykonawca nie ma istotnego wpływu na mechanizmy kontrolne odnoszące się do organizacji, to audytor IT powinien udokumentować ten fakt w swojej dokumentacji roboczej.

8.2.2 Jeśli podwykonawca ma istotny wpływ na mechanizmy kontrolne odnoszące się do organizacji audytor IT powinien ocenić procesy strony trzeciej wykorzystywane do zarządzania i monitorowania relacjami z podwykonawcą. Audytor IT powinien rozważyć sekcje 6 i 7 tej wytycznej w trakcie oceny mechanizmów kontrolnych usługodawcy w stosunku do podwykonawcy.

9. RAPORTOWANIE

9.1 Słabości

9.1.1 Raport audytora IT powinien wskazywać, że mechanizmy kontrolne będące przedmiotem badania rozciągają się na te wewnątrz organizacji jak i te, które występują u usługodawcy. Ponadto audytor IT powinien zidentyfikować mechanizmy kontrolne, ich słabości i kontrole kompensacyjne występujące w każdej organizacji.

9.1.2 Zakres, w jakim wnioski i rekomendacje zostaną zakomunikowane, powinien być udokumentowany w opisie zakresu działania [w formie referencji]. *The extent to which conclusions and recommendations are communicated should be documented in the terms of reference.* Niektórzy z usługodawców mogą nie wyrażać woli lub nie być zdolni do wdrożenia

rekomendacji. W tej sytuacji audytor IT powinien zarekomendować kontrole kompensacyjne, które organizacja powinna zaimplementować dla zniwelowania słabości mechanizmów kontrolnych strony trzeciej.

10. DATA OBOWIĄZYWANIA

10.1 Powyższe wskazówki stają się obowiązujące dla wszystkich audytów systemów informatycznych począwszy od 1 marca 2002 roku.

060.020.010 Dokumentacja audytu

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

- 1.1.1** Standard 060.020 (Dokumentacja) głosi, że „W celu efektywnej realizacji celów audytu Audytor Systemów Informatycznych podczas przeprowadzania audytu ma zebrać wystarczającą, wiarygodną, istotną i użyteczną dokumentację”.
- 1.1.2** Standard 070.010 (Forma i Zawartość Raportu) określa, że „Zadaniem Audytora Systemów Informatycznych jest dostarczenie określonym odbiorcom odpowiednio sformowanego raportu dotyczącego wykonanej pracy audytorskiej. Raport z audytu ma przedstawiać obszar, cele, okres oraz rodzaj i zakres wykonanej pracy audytorskiej. Raport ma wskazywać organizację, odbiorcę raportu oraz wszelkie zastrzeżenia co do jego obiegu. Raport ma przedstawiać wyniki, wnioski i rekomendacje oraz wszelkie zastrzeżenia lub uwarunkowania audytora wobec audytu.”

1.2 Potrzeba wprowadzenia Wytycznej

- 1.2.1** Celem wprowadzenia tej Wytycznej jest opisanie dokumentacji, jaką dla wsparcia działań audytorskich powinien przygotować i zachować Audytor SI..
- 1.2.2** Wytyczna ta dostarcza wskazówek dotyczących stosowania standardów audytu informatycznego. Audytor SI powinien wziąć ją pod uwagę przy określaniu metody zastosowania powyższych standardów, przy użyciu profesjonalnej oceny jej zastosowania oraz powinien być przygotowany do uzasadnienia wszelkich od niej odstępstw..

2. PLANOWANIE

2.1 Zawartość zbioru dokumentacji

- 2.1.1** Dokumentację audytu systemów informatycznych stanowi zapis przeprowadzonej przez audytora pracy oraz dowody audytorskie potwierdzające wykrycia Audytora SI oraz jego wnioski. Możliwości zastosowania dokumentacji obejmują:
- Przedstawienie zakresu, do którego Audytor SI zastosował Standardy Audytu SI,
 - Wsparcie przy planowaniu, przeprowadzaniu i analizowaniu audytu,
 - Ułatwienie przeglądu audytu osobom zewnętrznym,
 - Ocena przez audyt SI programu zabezpieczenia jakości funkcjonowania,
 - Wsparcie w przypadkach takich, jak roszczenia ubezpieczeniowe, defraudacje i postępowanie procesowe,
 - Pomoc dla profesjonalnego rozwoju personelu.
- 2.1.2** Dokumentacja powinna zawierać co najmniej zapisy dotyczące:
- Planowanie i przygotowanie zakresu i celów audytu,
 - Program Audytu,
 - Wykonywane kolejne kroki audytorskie oraz zgromadzone dowody,
 - Wykrycia, wnioski i rekomendacje będące wynikiem audytu,
 - Wszelkie raporty będące wynikiem pracy audytorskiej,
 - Przegląd pracy audytorskiej ze strony kierownictwa.
- 2.1.3** Zakres dokumentacji zgromadzonej przez Audytora SI zależy od potrzeb określonego audytu i powinien zawierać rzeczy takie, jak:
- Zrozumienie przez Audytora SI obszaru i środowiska poddanego kontroli,
 - Wiedzę Audytora SI dotyczącą systemów przetwarzania informacji oraz wewnętrznych zasad zarządzania,
 - Autorów i źródła dokumentów audytu oraz daty ich uzyskania,
 - Dowody audytorskie i źródła dokumentów oraz daty ich zgromadzenia,
 - Odpowiedzi osób kontrolowanych na rekomendacje audytorskie.
- 2.1.4** Dokumentacja powinna zawierać informacje kontrolne wymagane przez prawo, regulacje rządowe lub przez stosowane standardy profesjonalne. Dokumentacja powinna być czytelna, kompletna i zrozumiała dla osób ją przeglądających.

2.2 Zabezpieczanie, przechowywanie i odzyskiwanie dokumentacji

- 2.2.1** Powinna być stosowana odpowiednia polityka i procedury zapewnienia właściwego zabezpieczenia i przechowywania dokumentacji wspierającej wykrycia i wnioski audytu, przez okres odpowiedni w stosunku do regulacji prawnych, zawodowych oraz wymagań organizacyjnych firmy.
- 2.2.2** Dokumentacja powinna być zorganizowana, przechowywana i zabezpieczana w sposób odpowiedni dla rodzaju mediów, na których się znajduje, oraz powinna być ciągle dostępna przez okres czasu regulowany zdefiniowaną powyżej polityką i procedurami.

3. DATA OBOWIĄZYWANIA

- 3.1** Wytyczna ma zastosowanie dla wszystkich audytów systemów informatycznych poczynawszy od 1 września 1999 roku.

060.020.020 Przegląd systemów aplikacyjnych

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

1.1.1 Standard 060.020 (Dowód) stwierdza "Podczas audytu audytor systemów informatycznych, ma uzyskać wystarczające, wiarygodne, odpowiednie i użyteczne dowody by osiągnąć skutecznie cele audytowe. Spostrzeżenia audytowe i wnioski mają być poparte odpowiednimi analizami i interpretacją tych dowodów."

1.2 Potrzeba wytycznej

1.2.1 Celem tej wytycznej jest opisanie rekomendowanych praktyk w wykonywaniu przeglądu systemów aplikacyjnych.

1.2.2 Celem przeglądu systemów aplikacyjnych jest zidentyfikowanie, udokumentowanie, testowanie i ocena mechanizmów kontrolnych aplikacji, które są wdrożone przez organizację aby osiągnąć właściwe cele kontrolne. Te cele kontrolne mogą być podzielone na kategorie dotyczące celów kontrolnych odnośnie systemu i związanych z nim danych.

2. PLANOWANIE

2.1 Planning Considerations

2.1.1 Integralną częścią planowania jest zrozumienie środowiska systemu informatycznego organizacji przez audytora SI w stopniu wystarczającym do określenia rozmiaru i złożoności systemów oraz stopnia zależności organizacji od systemów informatycznych. Audytor SI powinien uzyskać zrozumienie misji organizacji i celów biznesowych, poziomu i sposobu w jaki technologia i systemy informatyczne wspierają organizację oraz ryzyka i ujawnienia skojarzone z celami organizacji i jej systemami informatycznymi. Powinien również zrozumieć strukturę organizacyjną łącznie z rolami i odpowiedzialnością kluczowych pracowników SI oraz właścicieli procesu biznesowego systemu aplikacyjnego

2.1.2 Podstawowym celem planowania jest zidentyfikowanie poziomu ryzyk aplikacji. Względny poziom ryzyka wpływa na poziom wymaganych dowodów audytowych.

2.1.3 Poziom ryzyk aplikacji na poziomie systemu i danych obejmuje takie rzeczy jak:

- Ryzyka dostępności systemu odnoszące się do braku zdolności operacyjnych systemu
- Ryzyka bezpieczeństwa systemu odnoszące się do nieautoryzowanych dostępów do aplikacji i/lub danych
- Ryzyka integralności odnoszące się do braku kompletności, dokładności, nie na czas lub nieautoryzowanego przetwarzania danych
- Ryzyka utrzymywania odnoszące się do braku możliwości wykonania update'u systemu, gdy jest on wymagany, w sposób ciągły, zapewniający systemowi dostępność, bezpieczeństwo i integralność
- Ryzyka danych odnoszące się do ich kompletności, integralności, poufności, prywatności i dokładności

2.1.4 Aplikacyjne mechanizmy kontrolne, które zajmują się poziomem ryzyk aplikacyjnych mogą być w formie skomputeryzowanych mechanizmów kontrolnych wbudowanych w system, mechanizmów kontrolnych wykonywanych ręcznie lub kombinacja obu z nich. Przykłady obejmują komputerowe porównanie dokumentów (zamówienie, fakturę i świadectwo otrzymania towaru), sprawdzenie i podpisanie czeku wygenerowanego komputerowo i przegląd raportów ze szczególnymi przypadkami (wyjątkami) przez kierownictwo wyższego szczebla.

2.1.5 Tam, gdzie wybrano opcję mechanizmów kontrolnych opartych na oprogramowaniu, powinny być brane pod uwagę ogólne mechanizmy kontrolne IT, jak również mechanizmy kontrolne specjalnie powiązane z celem audytu. Ogólne mechanizmy kontrolne IT mogą być przedmiotem odrębnego przeglądu, który obejmowałby takie sprawy jak: fizyczne mechanizmy kontrolne, bezpieczeństwo na poziomie systemu, zarządzanie siecią, backup danych i planowanie ciągłości. Zależnie od celów kontrolnych przeglądu, audytor SI nie musi dokonywać przeglądu ogólnych mechanizmów kontrolnych w sposób, w jaki system aplikacyjny jest oceniany w celu zakupu.

2.1.6 Przeglądy systemu aplikacyjnego mogą być wykonywane gdy gotowy system aplikacyjny jest oceniany przed zakupem, przed wejściem systemu aplikacyjnego do produkcji (przedwdrożeniowy) i po wejściu systemu aplikacyjnego do produkcji (powdrożeniowy). Sprawozdanie z przeglądu przedwdrożeniowego systemu aplikacyjnego obejmuje architekturę na poziomie bezpieczeństwa systemu, plany wdrożenia zabezpieczeń (bezpieczeństwa), odpowiedniość (dokładność) dokumentacji systemu i użyteczność oraz odpowiedniość rzeczywistego lub planowanego testów akceptacyjnych użytkownika. Sprawozdanie z przeglądu powdrożeniowego obejmuje bezpieczeństwo na poziomie aplikacji po wdrożeniu i może obejmować konwersję systemu jeśli miał miejsce transfer danych i informacji ze zbioru głównego (masterfile) starego do nowego systemu.

2.1.7 Cele I zakres Przeglądu Systemów Aplikacyjnych (Application Systems Review) zwykle tworzy część Specyfikacji Warunków (Terms of Reference). Postać i zawartość Specyfikacji Warunków mogą się różnić, lecz muszą zawierać:

- Cele i zakres przeglądu
- Wykonanie przeglądu przez audytora/audytorów SI
- Oświadczenie odnośnie niezależności audytora/audytorów SI od projektu
- Kiedy przegląd zostanie rozpoczęty
- Ramy czasowe przeglądu
- Ustalenia odnośnie raportowania
- Ustalenia końcowe zebrania???
- Cele powinny być tak rozwinięte by uwzględnić kryteria informatyczne nr 7 COBIT'u, a następnie uzgodnione przez organizację:
 - Efektywność (Skuteczność)
 - Wydajność (Sprawność)

- Poufność
- Integralność
- Dostępność
- Zgodność
- Niezawodność informacji

2.1.8 Tam, gdzie audytor SI został zaangażowany wcześniej w rozwój, nabywanie, wdrożenie lub utrzymywanie systemu aplikacyjnego i jest przydzielony do zadania??? audytowego, niezależność audytora SI może być osłabiona. Audytor SI powinien korzystać z odpowiedniej wytycznej, która dotyczy takiej sytuacji.

3. WYKONANIE PRACY AUDYTOWEJ

3.1 Dokumentowanie przepływu transakcji

3.1.1 Zebrana informacja powinna obejmować zarówno skomputeryzowane jak i ręczne aspekty systemu. Uwaga powinna być skierowana na wejście danych (czy elektroniczne, czy ręczne), przetwarzanie, składowanie, i wyjście, które mają duże znaczenie dla celu audytu. Audytor SI może uważać zależnie od procesów biznesowych i użycia technologii, że dokumentowanie przepływu transakcji może nie być możliwe w praktyce. W takim wypadku audytor SI powinien przygotować diagram przepływów danych wysokiego poziomu lub opis i/lub wykorzystanie dokumentacji systemowej jeśli została dostarczona. Powinna być także wzięta pod uwagę dokumentacja interfejsów aplikacji powiązana z innymi systemami.

3.1.2 Audytor SI może uzyskać potwierdzenie dokumentacji poprzez procedury przetwarzania takie, jak sprawdzenie za pomocą testowania.

3.2 Identyfikowanie i testowanie mechanizmów kontrolnych systemów aplikacyjnych

3.2.1 Aby ograniczyć ryzyka aplikacyjne, mogą być zidentyfikowane określone mechanizmy kontrolne i otrzymany wystarczający dowód audytu, żeby upewnić audytora SI, że mechanizmy kontrolne działają jak zamierzono. Może on być osiągnięty przez procedury takie jak:

- Zapytanie i obserwacja
- Przegląd dokumentacji
- Testowanie aplikacyjnych mechanizmów kontrolnych, tam gdzie zaprogramowane mechanizmy kontrolne są testowane; można rozważyć wykorzystanie CAAT

3.2.2 Istota, harmonogram i zasięg testowania powinny być oparte na poziomie ryzyka obszaru podlegającego przeglądowi i celach audytu. Wobec braku silnych ogólnych mechanizmów kontrolnych IT, audytor SI może dokonać oceny wpływu tej słabości na niezawodność skomputeryzowanych mechanizmów kontrolnych aplikacji.

3.2.3 Jeśli audytor SI odkryje/stwierdzi znaczące słabości w skomputeryzowanych mechanizmach kontrolnych aplikacji, powinno się uzyskać (w zależności od celu audytu), jeśli to możliwe, zabezpieczenie ze strony ręcznie wykonywanych mechanizmów kontrolnych.

3.2.4 Skuteczność skomputeryzowanych mechanizmów kontrolnych zależy od silnych ogólnych mechanizmów kontrolnych IT. Stąd, jeśli ogólne mechanizmy kontrolne IT nie podlegają przeglądowi, możliwość oparcia się na aplikacyjnych mechanizmach kontrolnych może być poważnie ograniczona i audytor SI powinien rozważyć procedury alternatywne.

4. RAPORTOWANIE

4.1 Słabości

4.1.1 Słabości zidentyfikowane w wyniku przeglądu aplikacji albo wynikające z braku mechanizmów kontrolnych albo ich niezgodności powinny zwrócić uwagę właściciela procesu biznesowego i kierownictwa SI odpowiedzialnych za wsparcie aplikacji. Tam, gdzie zidentyfikowane słabości podczas przeglądu systemu aplikacyjnego są uważane za znaczące i istotne, kierownictwo odpowiedniego szczebla powinno być powiadomione, aby podjąć natychmiastowe działania naprawcze.

4.1.2 Ponieważ skuteczne, skomputeryzowane mechanizmy kontrolne aplikacji są uzależnione od ogólnych mechanizmów kontrolnych IT, słabości w tym obszarze powinny być także raportowane. W przypadku, gdy takie mechanizmy kontrolne nie zostały sprawdzone, fakt ten powinien być ujęty w raporcie.

4.1.3 Audytor SI powinien wprowadzić do raportu odpowiednie rekomendacje aby wzmocnić mechanizmy kontrolne.

5. DATA OBOWIĄZYWANIA

5.1 Wytyczna jest obowiązująca dla wszystkich audytów systemów informatycznych wykonywanych począwszy od dnia 1 listopada 2001 roku.

060.020.030 Wymóg dowodów audytu

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

1.1.1 Standard 060.020 (Dowody) stanowi, że "Podczas przeprowadzania audytu Audytor Systemów Informatycznych (Audytor SI) zobowiązany jest uzyskać wystarczające, wiarygodne, relewantne (powiązane) i użyteczne dowody, aby efektywnie zrealizować cele audytu. Stwierdzenia i wnioski z audytu mają być poparte odpowiednią analizą i interpretacją tych dowodów."

1.2 Potrzeba wytycznej

1.2.1 Celem niniejszej Wytycznej jest zdefiniowanie pojęcia "dowodów" tak, jak zostało ono użyte w Standardzie 060.020 ze zbioru Standardów Audytowania Systemów Informatycznych oraz odniesienie się do zagadnienia rodzajów i wystarczalności dowodów audytu wykorzystywanych w audytowaniu systemów informatycznych.

1.2.2 Prezentowana Wytyczna dostarcza wskazówek jak stosować standardy audytowania systemów informatycznych. Audytor SI powinien uwzględnić ją podczas określania sposobu wdrożenia powyższego Standardu, powinien posłużyć się profesjonalnym osądem podczas jej stosowania i być przygotowanym do uzasadnienia każdego od niej odstępstwa.

2. PLANOWANIE

2.1 Rodzaje dowodów audytu

2.1.1 Podczas planowania prac audytu systemów informatycznych, Audytor SI powinien wziąć pod uwagę rodzaj dowodów audytowych, które ma zgromadzić, ich wykorzystanie w celu spełnienia celów audytu, oraz ich różny stopień wiarygodności. Między innymi, należy rozpatrzyć niezależność i kwalifikacje strony (osoby), która dostarcza dowodów audytu. Na przykład potwierdzający coś dowód audytowy od niezależnej strony z zewnątrz (tzw. strony trzeciej) może być bardziej wiarygodny niż dowód pochodzący od audytowanej organizacji. Materialne (fizyczne) dowody audytowe są generalnie bardziej wiarygodne niż świadectwa uzyskane od osób.

2.1.2 Różne rodzaje dowodów audytu, których wykorzystanie Audytor SI powinien wziąć pod uwagę, obejmują:

- Zaobserwowane procesy i istnienie przedmiotów (składników) materialnych (fizycznych),
- Materiały dowodowe dokumentacyjne (dokumentacje),
- Świadectwa reprezentujące ("reprezentacje") ,
- Analizy.

2.1.3 Zaobserwowane procesy i istnienie przedmiotów (składników) materialnych może obejmować obserwacje działań, posiadanego mienia i funkcji pełnionych przez (komórki organizacyjne) IT, takie jak:

- spis nośników (danych) w zewnętrznej lokalizacji, gdzie są one przechowywane,
- system bezpieczeństwa pomieszczeń komputerowych podczas działania.

2.1.4 Dokumentacyjne dowody audytowe, zarejestrowane na papierze lub innym nośniku, mogą obejmować:

- wyniki ekstrakcji danych,
- zapisy transakcji,
- listingi programów,
- faktury,
- logi wykonanych działań i logi kontrolne,
- dokumentacja rozwoju systemu.

2.1.5 Świadectwa reprezentujące ("reprezentacje") jednostek audytowanych, które mogą być dowodami audytowymi, to:

- spisane polityki i procedury,
- schematy systemowe,
- oświadczenia, spisane lub ustne.

2.1.6 Rezultaty analizowania informacji za pomocą porównań, symulacji, kalkulacji i rozumowania również mogą być wykorzystane jako dowody audytu. Przykłady obejmują:

- Badania porównawcze wydajności systemów informatycznych w stosunku do innych organizacji lub okresów minionych,
- Porównywanie wskaźników błędów pomiędzy aplikacjami, transakcjami i użytkownikami.

2.2 Dostępność dowodów audytu

2.2.1 Audytor SI powinien wziąć pod uwagę okres, w trakcie którego informacje istnieją lub są dostępne, przy określaniu charakteru, właściwego czasu oraz zakresu testowania dowodowego (udowadniającego), oraz, jeśli to właściwe, testowania zgodności. Na przykład, dowody audytowe przetwarzane za pomocą Elektronicznej Wymiany Danych (ang. Elektronic Data Interchange - EDI), Przetwarzania Obrazów Dokumentów (ang. Document Image Processing - DIP), czy takich dynamicznych systemów jak arkusze kalkulacyjne, mogą być nie do przywrócenia po określonym czasie, jeśli nie kontroluje się zmian w plikach lub pliki nie zostaną skopiowane.

2.3 Wybór dowodów audytowych

2.3.1 Audytor SI powinien planować użycie jak najlepszych dowodów audytowych możliwych do zdobycia, zgodnych z ważnością celów audytu oraz czasem i wysiłkiem włożonym w osiągnięcie dowodów.

2.3.2 Tam gdzie dowody uzyskane w postaci świadectw ustnych są krytyczne dla opinii czy wniosków z audytu, Audytor SI powinien rozważyć pozyskanie udokumentowanego potwierdzenia świadectw, albo w postaci papierowej lub na innym nośniku.

3. PROWADZENIE PRAC

3.1 Charakter (natura) dowodów audytu

3.1.1 Dowody audytu powinny być wystarczające, wiarygodne, relewantne, oraz użyteczne, aby umożliwić sformułowanie opinii lub poprzeć stwierdzenia i wnioski Audytora IT. Jeśli, w przekonaniu Audytora IT, uzyskane dowody audytu nie spełniają tych kryteriów, Audytor powinien zdobyć dodatkowe dowody. Na przykład, listing programu może nie być wystarczającym dowodem audytu, o ile nie zbierze się innych dowodów w celu zweryfikowania, że listing przedstawia faktyczny program wykorzystywany w procesie produkcyjnym.

3.2 Gromadzenie dowodów audytu

3.2.1 Procedury wykorzystywane do gromadzenia dowodów audytu różnią się w zależności od audytowanego systemu informatycznego. Audytor SI powinien wybrać procedurę najbardziej odpowiednią do celu audytu. Powinno się uwzględnić następujące procedury:

- Zapytania ,
- Obserwacje,
- Inspekcje,
- Poświadczenia (potwierdzenia),
- Powtórne wykonanie działań, operacji ,
- Monitorowanie.

3.2.2 Powyższe metody mogą być stosowane w ramach korzystania z procedur ręcznych, technik audytowych wspomaganych komputerowo, lub z połączenia (kombinacji) obu sposobów. Na przykład:

- System, który wykorzystuje ręcznie prowadzone sumy kontrolne w celu zbilansowania operacji wprowadzania danych, może dostarczyć dowodu audytowego, że procedury kontrolne istnieją, za pomocą odpowiednio uzgodnionego i objaśnionego raportu. Audytor SI powinien uzyskać dowody audytu przeglądając i badając ten raport,
- Szczegółowe zapisy transakcji mogą być dostępne tylko w formacie odczytywalnym maszynowo (komputerowo), wymagając od Audytora IT, aby dowody audytu uzyskał stosując wspomagane komputerowo techniki audytowe (ang. skrót CAATs).

3.3 Dokumentacja Audytu

3.3.1 Dowody audytu zebrane przez Audytora IT powinny być odpowiednio udokumentowane i zorganizowane, tak by poprzeć stwierdzenia i wnioski Audytora.

4. RAPORTOWANIE

4.1 Ograniczenia zakresu

4.1.1 W sytuacjach, w których Audytor SI jest przekonany, że uzyskanie wystarczających dowodów audytowych nie jest możliwe, powinien on ujawnić ten fakt w sposób zgodny ze sposobem komunikowania rezultatów audytu.

5. DATA OBOWIĄZYWANIA

5.1 Powyższa wytyczna obowiązuje w stosunku do wszystkich audytów systemów informatycznych rozpoczynających się począwszy od 1 grudnia 1998.

060.020.040 Próbkiowanie audytowe

1. PODSTAWA

1.1 Powiązanie ze Standardami

1.1.1 Standard 060.020 (Evidence) stanowi, że "Zadaniem Audytora Systemów Informatycznych podczas przeprowadzania audytu jest zgromadzenie wystarczających, wiarygodnych, odpowiednich (relewantnych) i użytecznych dowodów, tak by efektywnie zrealizować zadania audytu. Wyniki audytu oraz wnioski powinny być poparte odpowiednią analizą i interpretacją tychże dowodów."

1.2 Potrzeba wytycznej

1.2.1 Celem tej Wytycznej jest dostarczenie wskazówek audytorowi systemów informatycznych do projektowania i wyboru próby audytowej i oceny rezultatów próbkowania. Właściwe próbkowanie i ocena wspierają spełnienie wymagania "wiarygodnych, odpowiednich (relewantnych) i użytecznych dowodów" i "poparcia wniosków odpowiednią analizą i interpretacją dowodów".

1.2.2 Audytor systemów informatycznych powinien rozważyć techniki próbkowania, których wynikiem są reprezentatywne próby statystyczne dla wykonania badania zgodności lub testowania dowodowego.

1.2.3 Przykładami testów badania zgodności mechanizmów kontrolnych, w ramach których można rozważyć próbkowanie mogą być prawa dostępu użytkowników, procedury kontroli zmian programu, procedury dokumentowania, dokumentacja programu, postępowanie z wyjątkami, przegląd dzienników (logów), audyty licencji oprogramowania, itp.

1.2.4 Przykładami testów dowodowych, w ramach których można rozważyć próbkowanie mogą być ponowne wykonanie złożonych obliczeń (np., odsetek, procentów) na przykładowych kontach, przykładowych transakcjach by zaręczyć za dokumentację wspierającą, itp.

1.2.5 Ta wytyczna dostarcza wskazówek do stosowania standardów audytu systemów informatycznych. Audytor systemów informatycznych powinien rozważyć to podczas określania jak osiągnąć wdrożenie powyższego standardu, używać zawodowej oceny w jego stosowaniu i być przygotowanym do uzasadnienia jakiegokolwiek odstępstwa.

1.2.6 Inne użyteczne informacje dotyczące próbkowania audytowego zawarte są w International Standard on Auditing #530, Audit Sampling and other Selective Testing Procedures, wydanych przez the International Federation of Accountants (IFAC).

2. WYKONANIE PRACY AUDYTORSKIEJ

2.1 Próbkiowanie audytowe

2.1.1 Używając zarówno statystycznych jak i niestatystycznych metod próbkowania, audytor systemów informatycznych powinien zaprojektować i wybrać próbę audytową, wykonać procedury audytowe i ocenić wyniki próby, by uzyskać wystarczające, rzetelne, właściwe (relevant) i użyteczne dowody audytowe.

2.1.2 Kształtując opinię audytową audytorzy systemów informatycznych często nie badają wszystkich dostępnych informacji, jako że mogło by to być niepraktyczne, a poprawne wnioski mogą być wyciągnięte z użyciem próbkowania audytowego.

2.1.3 Próbkiowanie audytowe jest określone jako zastosowanie procedur audytowych do mniej niż 100% populacji by umożliwić audytorowi systemów informatycznych ocenienie dowodów audytowych pod kątem pewnych charakterystyk wybranych obserwacji w celu sformułowania lub wsparcia sformułowania wniosków dotyczących populacji.

2.1.4 Próbkiowanie statystyczne wymaga użycia technik, z których mogą być matematycznie wyciągnięte wnioski dotyczące populacji.

2.1.5 Próbkiowanie niestatystyczne nie jest oparte na statystyce i rezultaty nie powinny być ekstrapolowane na całą populację, jako że mało prawdopodobnym jest, że próbka jest reprezentatywna dla populacji.

2.2 Projektowanie próby

- 2.2.1** Podczas projektowania rozmiaru i struktury próby audytowej, audytor systemów informatycznych powinien rozważyć określone cele kontrolne, naturę populacji oraz metody próbkowania i wyboru.
- 2.2.2** Audytor systemów informatycznych powinien rozważyć potrzebę angażowania odpowiednich specjalistów w trakcie projektowania i analizy prób.
- 2.2.3** Jednostka próbkowana- Jednostka próbkowana będzie zależeć od celu próbkowania. Dla badania zgodności mechanizmów kontrolnych (compliance testing of controls), zazwyczaj jest używane próbkowanie atrybutowe, gdzie jednostką próbkowaną jest zdarzenie lub transakcja (np., kontrola taka jak autoryzacja na fakturze). Dla testowania dowodowego (substantive testing), jest często używane próbkowanie zmiennych lub estymacja, gdzie jednostka próbkowana jest często monetarna.
- 2.2.4** Cele audytowe - Audytor systemów informatycznych powinien wziąć pod uwagę specyficzne cele audytowe, które mają być osiągnięte i procedury audytowe, które najprawdopodobniej osiągną te cele. Dodatkowo, kiedy próbkowanie audytowe jest właściwe, powinno się wziąć pod uwagę naturę poszukiwanych dowodów audytowych i możliwych przyczyn błędów.
- 2.2.5** Populacja - Populacja jest całym zbiorem danych, z którego audytor systemów informatycznych zamierza próbować w celu uzyskania wniosków na temat populacji. Zatem populacja, z której wybierana próba ma być odpowiednia i zweryfikowana jako kompletna dla określonego celu audytowego.
- 2.2.6** Stratyfikacja - Do pomocy w sprawnym i skutecznym projektowaniu próby, może być odpowiednia stratyfikacja. Stratyfikacja jest procesem dzielenia populacji na subpopulacje z o podobnej, jasno określonej charakterystyce, tak że każda próbkowana jednostka może należeć tylko do jednego stratum.
- 2.2.7** Wielkość próby - Podczas określania wielkości próby, audytor systemów informatycznych powinien wziąć pod uwagę ryzyko próbkowania, wielkość błędu, która powinna być do przyjęcia oraz zakres, dla którego spodziewane są błędy.
- 2.2.8** Ryzyko próbkowania - Ryzyko próbkowania bierze się z możliwości, że wnioski audytora systemów informatycznych mogą być różne od wniosków, które byłyby wyciągnięte, gdyby cała populacja była przedmiotem tej samej procedury audytowej. Istnieją dwa typy ryzyka próbkowania.
- Ryzyko niewłaściwego przyjęcia - ryzyko, że istotne nieprawidłowości zostały ocenione jako nieprawdopodobne, podczas gdy populacja jest znacząco obciążona błędami
 - Ryzyko niewłaściwego odrzucenia - ryzyko, że istotny błąd jest uznany za prawdopodobny, podczas gdy populacja nie jest znacząco obciążona błędami
- 2.2.9** Wielkość próby jest uzależniona od poziomu ryzyka audytowego, które audytor systemów informatycznych ma zamiar zaakceptować. Ryzyko próbkowania powinno być także rozważone w relacji do modelu ryzyka audytowego i jego komponentów, ryzyka wrodzonego (inherent risk), ryzyka kontroli (control risk) i ryzyka detekcji (detection risk).
- 2.2.10** Dopuszczalny błąd (tolerable error) - dopuszczalny błąd jest maksymalnym błędem w populacji, który audytor systemów informatycznych zamierza zaakceptować i nadal wnioskować, że cel audytowy został osiągnięty. Dla testowania dowodowego (substantive tests), tolerable error jest powiązany z profesjonalnym osądem audytora systemów informatycznych, co do istotności. W testowaniu zgodności (compliance tests), jest maksymalnym współczynnikiem odchylenia od nakazanej procedury kontrolnej, który audytor systemów informatycznych zamierza zaakceptować.
- 2.2.11** Oczekiwany błąd - Jeżeli audytor systemów informatycznych oczekuje istnienia błędów w populacji, to musi wówczas zbadać większą próbę, niż zwykle w przypadku gdy nie oczekuje błędów, aby wnioskować, że faktyczne błędy w populacji są na poziomie nie większym niż zaplanowany tolerable error. Mniejszy rozmiar próby jest uzasadniony, gdy oczekuje się, że populacja jest wolna od błędów. Podczas określania oczekiwanego poziomu błędów w populacji, audytor systemów informatycznych powinien rozważyć takie sprawy jak poziomy błędów rozpoznane podczas poprzednich audytów, zmiany w procedurach organizacji i dowody dostępne z oceny systemu kontroli wewnętrznej oraz rezultaty procedur przeglądów analitycznych.

2.3 Wybór próby

2.3.1 Istnieją cztery powszechnie stosowane metody próbkowania:

Metody próbkowania statystycznego

- Próbkowanie losowe - zapewnia, że wszystkie kombinacje jednostek wybieranych z populacji mają taką samą szansę wyboru
- Próbkowanie systematyczne - wymaga selekcji jednostek wybieranych z użyciem stałego interwału pomiędzy wyborami, przy pierwszym wyborze rozpoczynającym się losowo. Przykłady obejmują próbkowanie jednostek pieniężnych (Monetary Unit Sampling) lub wybór ważony wartością (Value Weighted selection), gdzie każda jednostkowa wartość pieniężna (np. \$1) w populacji ma równą szansę wyboru. Jako, że pojedyncza jednostka pieniężna nie może być zazwyczaj badana oddzielnie dlatego jednostka, która obejmuje jednostkę pieniężną jest wybierana do badania. Ta metoda systematycznie waży wybór foworyzując większe ilości, ale ciągle dając każdej jednostce pieniężnej takie same prawdopodobieństwo wyboru. Innym przykładem może być wybieranie każdej n-tej jednostki.

Metody próbkowania niestatystycznego

- próbkowanie na chybił trafił (haphazard sampling) - w którym audytor wybiera próbę bez posługiwania się techniką strukturalną, chociaż unikając jakiegokolwiek świadomego uprzedzenia lub przewidywania. Jednakże, analiza próbkowania na chybił trafił nie powinna zależeć od formy wniosków na temat populacji
 - próbkowanie osądowe (judgmental sampling) - w którym audytor systemów informatycznych in which the IS Auditor stosuje uprzedzenie do próby (np., wszystkie próbkowane jednostki o określonej wartości, wszystkie o specyficznym typie odchyień, wszystkie ujemne, wszyscy nowi użytkownicy itp.). Należy zauważyć, że próbkowanie osądowe nie jest statystyczne i jego rezultaty nie powinny być rozszerzane na całą populację, jako że próba nie jest reprezentatywna dla populacji.
- 2.3.2** Audytor systemów informatycznych powinien wybrać przykładowe pozycje, w taki sposób, że od próby oczekuje się, że jest reprezentatywna dla populacji odnośnie testowanej charakterystyki, np. używając metod próbkowania statystycznego. Aby utrzymać niezależność audytu, audytor systemów informatycznych powinien zapewnić, kompletność populacji i kontrolę nad wyborem próby
- 2.3.3** Aby próba były reprezentatywna dla populacji, wszystkie próbkowane jednostki w populacji powinny mieć takie samo lub

znane prawdopodobieństwo bycia wybranym, np. metody próbkowania statystycznego.

2.3.4 Istnieją dwie powszechnie wykorzystywane metody wyboru: selection on records, oraz selection on quantitative fields (n.p., jednostki pieniężne).

Dla selection on records, common methods are:

- Random Sample (próba statystyczna)
- Haphazard Sample (niestatystyczna)
- Judgmental Sample (niestatystyczna; wysokie prawdopodobieństwo prowadzenia do stroniczych wniosków)
- Dla selection on quantitative fields, pospolitymi metodami są:
- Random Sample (próba statystyczna lub jednostki pieniężne)
- Fixed Interval Sample (próba statystyczna z użyciem stałego interwału)
- Cell Sample (próba statystyczna z użyciem losowego wyboru interwału)

2.4 Dokumentacja

2.4.1 Materiały robocze audytu powinny zawierać wystarczająco dużo detali do jasnego określenia celu próbkowania i wykorzystanego procesu próbkowania. Materiały robocze powinny zawierać źródło populacji, wykorzystaną metodę statystyczną, parametry próbkowania (n.p., losowy numer startowy lub metodę za pomocą której losowy numer startowy został osiągnięty, interwał próbkowania), wybrane obserwacje, szczegóły przeprowadzonych testów audytowych i uzyskane wnioski.

2.5 Ocena rezultatów próby

2.5.1 Mając wykonane, na każdej obserwacji, te procedury audytu, które są odpowiednie do określonego celu audytowego, audytor systemów informatycznych powinien zanalizować wszystkie możliwe błędy wykryte w próbie, by określić, czy są one rzeczywiście błędami i czy odpowiednie do natury i przyczyny błędów. Dla tych, które są ocenione jako błędne, błędy powinny być naświetlone jako właściwe dla populacji, jeżeli wykorzystana metoda próbkowania, jest metodą statystyczną.

2.5.2 Wszystkie możliwe błędy wykryte w próbie powinny być przejrane w celu określenia, czy są rzeczywiście błędami. Audytor systemów informatycznych powinien rozważyć jakościowe aspekty błędów. To obejmuje naturę i przyczynę błędu i prawdopodobny efekt błędu na inne fazy audytu. Błędy, które są rezultatem załamania zautomatyzowanego procesu zazwyczaj mają większy wpływ na stopę błędów niż błędy popełnione przez człowieka.

2.5.3 Kiedy oczekiwane dowody audytowe dotyczące określonej obserwacji nie mogą być pozyskane, audytor systemów informatycznych może być w stanie pozyskać wystarczająco odpowiednie dowody poprzez wykonanie procedur alternatywnych na wybranej obserwacji.

2.5.4 Audytor systemów informatycznych powinien rozważyć przeniesienie wyników z próby na populację za pomocą metody przeniesienia spójnej z metodą wykorzystaną do wyboru jednostki próbkowania. Przeniesienie próby może wymagać estymowania prawdopodobieństwa błędu w populacji i estymowania wszystkich innych błędów, które mogą nie być wykryte z powodu nieściśłości w technice w połączeniu z jakościowymi aspektami znalezionych błędów.

2.5.5 Audytor systemów informatycznych powinien rozważyć, czy błędy w populacji mogą być przekraczać tolerowany błąd przez porównanie szacowanego błędu populacji z dopuszczalnym błędem, biorąc pod uwagę rezultaty innych procedur audytowych, odpowiednich do celu audytu. Kiedy szacowany błąd populacji przekracza dopuszczalny błąd, audytor systemów informatycznych powinien ponownie ocenić ryzyko próbkowania i jeżeli jest ono nieakceptowalne, rozważyć rozszerzenie procedury audytowej lub wykonanie alternatywnych procedur audytowych.

3. DATA OBOWIĄZYWANIA

3.1 Nieniejsza wytyczna obowiązuje wszystkie audyty systemów informatycznych rozpoczęte począwszy od dnia 1 marca 2000 roku.

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

1.1.1 Standard 060.020 (Dowody) stwierdza: "Podczas przeprowadzania audytu, audytor systemów informatycznych (SI) zobowiązany jest uzyskać wystarczające, rzetelne, stosowne i użyteczne dowody, tak aby skutecznie zrealizować cele audytu. Spostrzeżenia i wnioski z audytu mają być poparte odpowiednią analizą i interpretacją tychże dowodów."

1.2 Potrzeba wytycznej

1.2.1 Część publikacji COBIT pt. "Struktura ramowa" (COBIT Framework) stwierdza: "Organizacje muszą spełniać wymagania wobec posiadanych informacji, jak również innych zasobów, dotyczące jakości, powiernictwa i bezpieczeństwa. Kierownictwo musi również zoptymalizować wykorzystanie dostępnych zasobów włączając w to dane, aplikacje, rozwiązania technologiczne, infrastrukturę i ludzi. Aby wypełnić ten obowiązek, jak również aby zrealizować swoje cele, kierownictwo musi ustanowić adekwatny system kontroli wewnętrznej."

1.2.2 Wykorzystanie technologii we wszystkich aspektach przedsięwzięć ekonomicznych i społecznych stworzyło krytyczną zależność od technologii informatycznych, podczas inicjowania, rejestrowania, przeprowadzania i zarządzania wszystkimi aspektami transakcji ekonomicznych, informacją i wiedzą, stwarzając tym samym krytyczną przestrzeń dla nadzoru nad IT (IT governance) w ramach nadzoru nad przedsiębiorstwem (enterprise governance).

1.2.3 Głośne problemy (np. awarie systemów wskutek ataków wirusów, utrata zaufania lub dostępności systemów wskutek ataków hakerskich na strony www) doświadczane przez wiele organizacji w ostatnich latach skupiły powszechną uwagę na zagadnieniach nadzoru korporacyjnego (ang. corporate governance). Formalne środki za pomocą których kierownictwo wypełnia swoje obowiązki dotyczące tworzenia skutecznego systemu kontroli wewnętrznej nad działalnością operacyjną i finansową w organizacjach, są obecnie przedmiotem badawczego zainteresowania opinii publicznej i często stanowią część zakresu audytów przeprowadzanych przez audytorów zarówno wewnętrznych jak i zewnętrznych.

1.2.4 Celem niniejszej wytycznej jest dostarczenie informacji odnośnie tego, jak audytor SI powinien podejść do zagadnienia audytu nadzoru nad IT, obejmując właściwe umocowanie organizacyjne zainteresowanego audytora SI, kwestie do uwzględnienia podczas planowania audytu, oraz dowody, które należy przeglądać podczas samego audytu. Wytyczna ta udziela również wskazówek na temat dróg raportowania i jego zawartości, oraz działań poaudytowych, które należy rozważyć.

2. STATUT AUDYTU

2.1 Pełnomocnictwo

2.1.1 Nadzór (governance) nad IT, jako jedna z dziedzin nadzoru nad przedsiębiorstwami, obejmuje zespół zagadnień podejmujących kwestię, jak w ramach przedsiębiorstwa wykorzystuje się technologie informatyczne (IT). IT są obecnie silnie zintegrowane i szeroko rozpowszechnione w ramach przedsiębiorstw, i raczej nie stanowią odrębnego obszaru funkcjonującego gdzieś na uboczu firmy. To jak IT zostaną zastosowane w ramach przedsiębiorstwa będzie miało ogromny wpływ na zrealizowanie przez nie swojej misji, wizji i celów strategicznych. Z tego powodu, przedsiębiorstwo musi dokonać oceny jak jest w nim sprawowany nadzór nad IT, w miarę jak staje się on coraz ważniejszym elementem nadzoru nad przedsiębiorstwem w ogóle. Raportowanie na temat nadzoru nad IT pociąga za sobą przeprowadzenie audytu na najwyższych poziomach struktur organizacyjnych, i może przekraczać granice wielu różnych obszarów, funkcji czy departamentów. Dlatego też, audytor SI powinien potwierdzić, czy specyfikacja warunków działania ustala:

- zakres prac, włączając w to jasne określenie obszarów funkcjonalnych i zagadnień objętych przeglądem;
- ścieżkę raportowania dla przypadków, gdy zagadnienia nadzoru nad IT zidentyfikowane są na najwyższych poziomach struktury organizacyjnej;
- uprawnienia audytora SI do dostępu do informacji.

3. NIEZALEŻNOŚĆ

3.1 Status organizacyjny

3.1.1 Audytor SI powinien rozważyć, czy jego/jej status organizacyjny jest odpowiedni do charakteru planowanego audytu. Jeśli jest inaczej, to kierownictwo na odpowiednim szczeblu powinno rozważyć zaangażowanie niezależnej strony trzeciej do pokierowania lub przeprowadzenia audytu.

4. PLANOWANIE

4.1 Stwierdzanie stanu faktycznego

4.1.1 Audytor SI powinien pozyskać informacje na temat struktury [organizacyjnej] nadzoru nad IT, włączając w to poziomy odpowiedzialne za:

- nadzorowanie przedsiębiorstwa,
- wyznaczanie strategicznych kierunków działań przedsiębiorstwa,
- ocenę wyników działań przewodniczącego zarządu/ zarządu z wdrażania strategii przedsiębiorstwa,

- ocenę wyników działań kierownictwa wyższego szczebla oraz szczebli podporządkowanych raportujących na temat realizacji strategii (włączając w to użytą wiedzę, informacje i technologie),
- określanie czy przedsiębiorstwo rozwinęło zdolności oraz infrastrukturę informatyczną wymagane do spełnienia wyznaczonych przed przedsiębiorstwem celów strategicznych,
- ocenę zdolności przedsiębiorstwa do podtrzymania realizacji bieżących operacji.

4.1.2 Audytor SI powinien zidentyfikować i uzyskać ogólne zrozumienie procesów umożliwiających strukturalnemu nadzoru IT realizację funkcji wylistowanych w punkcie 4.1.1 włączając w to kanały komunikowania wykorzystane do wyznaczenia celów i zadań niższym szczeblom organizacyjnym (w kierunku góra-dół) oraz informacje wykorzystane do monitorowania zgodności z nimi (kierunek z dołu do góry).

4.1.3 Audytor SI powinien pozyskać informacje dotyczące strategii organizacji wobec technologii informatycznych (udokumentowaną lub nie), włączając w to:

- długo i krótko terminowe plany realizacji misji i celów organizacji,
- długi i krótko terminowe strategie i plany dla IT oraz systemy wspierające realizację tych planów,
- sposób podejścia do wyznaczania strategii IT, budowy planów i monitorowania postępów z realizacji tych planów,
- sposób podejścia do kontroli zmian strategii i planów IT,
- deklarację misji IT i uzgodnionych zamierzeń i celów działalności IT,
- oceny dotychczasowych działań i systemów IT.

4.2 Cele audytu SI

4.2.1 Na cele audytu dotyczącego nadzoru nad TI mogą mieć wpływ potrzeby zakładanych zainteresowanych stron, planowany zakres rozpowszechnienia wyników. Audytor SI powinien rozważyć następujące opcje podczas ustalania całościowych celów audytu:

- raportowanie na temat systemu nadzoru i/lub jego skuteczności,
- włączenie lub wyłączenie informatycznych systemów finansowych,
- włączenie lub wyłączenie informatycznych systemów nie-finansowych.

4.2.2 Szczegółowe cele audytu SI w przypadku audytu nadzoru nad IT będą zwykle zależały od struktury kontroli wewnętrznej zrealizowanej przez najwyższe kierownictwo. W przypadku braku jakichkolwiek ustanowionych ram, jako minimum w celu ustalenia celów szczegółowych powinno się wykorzystać strukturę ramową zaproponowaną w COBIT'cie.

4.3 Zakres Audytu

4.3.1 Audytor SI powinien włączyć w zakres audytu stosowne procesy dotyczące planowania i organizowania działalności związanej z IT, oraz procesy dotyczące jej monitorowania.

4.3.2 Zakres audytu powinien obejmować system(y) kontroli dotyczący(e) użytkownika i ochrony całego spektrum zasobów informatycznych określonych w części standardu COBIT pt. "Struktura ramowa". Obejmują one:

- dane,
- aplikacje,
- technologię,
- infrastrukturę,
- ludzi.

4.4 Obsadzanie stanowisk (zapewnienie właściwej obsady)

4.4.1 Audytor SI powinien zapewnić, że w skład personelu, który będzie przeprowadzał dany audyt, będą wchodziły osoby o odpowiedniej pozycji i kompetencjach.

5. PRZEPROWADZANIE PRAC AUDYTOWYCH

5.1 Przegląd Działań Najwyższego Kierownictwa (Zarządu)

5.1.1 Nadzorem nad IT, jako elementem nadzoru nad całym przedsiębiorstwem powinny kierować (powodować) cele biznesowe. Audytor SI powinien ocenić czy istnieje proces planowania strategicznego biznesu biorąc pod uwagę czy:

- istnieje jasne określenie wizji i misji biznesu,
- istnieje i jest stosowana metodyka strategicznego planowania biznesu,
- poziom osób zaangażowanych w ten proces jest odpowiedni,
- planowanie jest okresowo uaktualniane.

5.1.2 Podczas przeglądu procesu planowania strategicznego IT audytor SI powinien rozważyć (wziąć pod uwagę) czy:

- istnieje jasne określenie misji i wizji IT,
- istnieje i jest stosowana metodyka strategicznego planowania dla technologii informatycznych,
- metodyka ta koreluje (zestawia, wiąże z sobą, wzajemnie) cele biznesowe z celami biznesowymi IT,
- proces planowania jest okresowo uaktualniany (przynajmniej raz do roku),
- plan ten identyfikuje główne inicjatywy IT oraz potrzebne zasoby,
- poziom osób zaangażowanych w ten proces jest odpowiedni.

- 5.1.3** Podczas przeglądu planowania IT na poziomie taktycznym, audytor SI powinien rozpatrzyć praktyki zarządzania projektami, biorąc pod uwagę:
- w jakim stopniu stosuje się metodyki zarządzania projektami,
 - zastosowane mechanizmy kontrolne dotyczące zarządzania projektami,
 - wykorzystywane narzędzia do zarządzania projektami,
 - zintegrowanie personelu IT i strony biznesowej na różnych etapach projektów,
 - metodyki zarządzania zmianami stosowane dla dużych projektów pociągających za sobą znaczące zmiany w organizacji.
- 5.1.4** Podczas przeglądu procesu dostarczania audytor SI powinien wziąć pod uwagę:
- istniejące operacyjne mechanizmy kontrolne (cele COBIT'owe związane z rozwojem aplikacji),
 - proces rozwoju lub modyfikacji.
 - proces zarządzania projektami (tak jak omówiono w punkcie 5.1.3).
- 5.1.5** Koncentrując się na metodyce i praktykach rozwoju aplikacji oraz mechanizmach kontrolnych użytych wobec procesu rozwoju, audytor SI może włączyć do przeglądu:
- metodykę rozwoju aplikacji (uwzględniając jej jakość, np. czy posiada odpowiednio rozbudowaną strukturę i czy obejmuje wszystkie aspekty cyklu życia systemu, oraz biorąc pod uwagę specjalne właściwości środowiska takie jak outsourcing czy systemy rozproszone),
 - metryki rozwojowe używane do szacowania rozmiaru projektu i jego postępów,
 - techniki wykorzystywane do badania zagadnień związanych z testowaniem, wyciągania z nich lekcji oraz doskonalenia metodyki i mechanizmów kontrolnych na potrzeby przyszłych projektów.
- 5.1.6** Podczas przeglądu procesów służących do administrowania posiadanymi na dany moment systemami, audytor SI powinien uwzględnić w jakim stopniu obecne systemy pokrywają strategiczne i wspierające obszary organizacji. Audytor SI może włączyć do przeglądu:
- obszary pokrywane przez wydane polityki określające strategiczne obszary, zdefiniowane w ramach procesu strategicznego planowania biznesowego,
 - proces stosowany przez najwyższe kierownictwo w celu opracowywania, komunikowania, narzucania i monitorowania zgodności z politykami,
 - udokumentowane polityki w następujących dziedzinach, które mogą być przydatne: bezpieczeństwo, zasoby ludzkie, własność danych, przetwarzanie danych na poziomie użytkownika końcowego, własność intelektualna, zachowanie danych, nabywanie i wdrażanie systemów, outsourcing, niezależne zapewnienie, planowanie ciągłości działania, ubezpieczenia i prywatność,
 - określenie ról i obowiązków ludzi zaangażowanych w procesy podlegające przeglądowi (na przykład właściciele danych, kierownictwo IT, kierownictwo wykonawcze) oraz ocena czy są one odpowiednie aby wspierać te procesy,
 - zbadanie czy ludzie zaangażowani w procesy podlegające przeglądowi posiadają umiejętności, doświadczenie i zasoby potrzebne do pełnienia swoich ról,
 - ocenę czy zapewniony jest właściwy udział audytu wewnętrznego (jeśli dana organizacja posiada takie zasoby),
 - ocenę czy pozycja personelu (specjalistów) lub funkcji IT jest odpowiednia, aby umożliwić organizacji jak najlepsze wykorzystanie IT w celu osiągnięcia jej celów biznesowych,
 - ocenę czy organizacja i zarządzanie specjalistami z dziedziny IT, jak również niespecjalistami w dziedzinie IT z obowiązkami dotyczącymi IT, są adekwatne w celu uwzględnienia ryzyka dla organizacji dotyczącego błędów, zaniedbań, nieprawidłowości oraz czynów nielegalnych.
- 5.1.7** Audytor SI powinien zastanowić się [rozważyć] czy uzyskane podczas wyżej wymienionych przeglądów dowody wskazują na to, że objęto nimi odpowiednie obszary. Kwestie, które powinno się tu uwzględnić są ustalone w COBIT'cie w Wytycznych dla Kierownictwa dotyczących Nadzoru nad IT (IT Governance Management Guidelines). Wytyczna ta obejmuje kluczowe wskaźniki celu, krytyczne czynniki sukcesu oraz kluczowe wskaźniki wydajności, które prowadzą nadzór nad IT do jego celów. Przykładami informacji, które powinny być uwzględnione są:
- istnienie opublikowanej [ogłoszonej] misji IT oraz uzgodnionych celów i zadań działalności IT,
 - ocena ryzyk związanych z użytkowaniem zasobów IT organizacji, oraz podejście do zarządzania tymi ryzykami,
 - plany wdrażania strategii IT i monitorowanie postępów względem tych planów,
 - budżety IT i monitorowanie rozbieżności,
 - ogólne polityki (polityki wysokiego poziomu) dotyczące wykorzystywania i ochrony IT oraz monitorowanie zgodności z tymi politykami,
 - porównanie stosownych wskaźników wydajności dla IT, takich jak benchmarki (wzorce, dane wzorcowe) z podobnych organizacji, obszarów funkcjonalnych, odpowiednich standardów międzynarodowych, modeli dojrzałości czy uznanych najlepszych praktyk,
 - regularne monitorowanie wydajności [realizacji, wykonania] w porównaniu do uzgodnionych wskaźników wydajnościowych,
 - dowody przeprowadzania okresowych przeglądów IT przez funkcje i ciała nadzorujące, wraz z określeniem, przydzieleniem, rozwiązaniem i śledzeniem punktów wymagających podjęcia działań,
 - dowody skutecznego i sensownego powiązania pomiędzy procesami opisanymi w punktach od 5.1.1 do 5.1.5.
- 5.1.8** Audytor SI powinien rozpatrzyć czy najwyższe kierownictwo podjęło odpowiednie działania kierownicze wiążące się z IT i czy są one odpowiednio monitorowane.

6. RAPORTOWANIE

6.1 Adresaci raportów

6.1.1 Audytor SI powinien kierować raporty dotyczące nadzoru nad IT do komitetu audytowego i najwyższego kierownictwa.

6.1.2 Jeśli znajdowane są niedociągnięcia w dziedzinie nadzoru nad IT, powinno się je natychmiast raportować do właściwych osób lub grup określonych w statucie audytu.

6.2 Treść

6.2.1 Oprócz zachowania zgodności z pozostałymi standardami ISACA dotyczącymi raportowania, raport a audytu nadzoru nad IT powinien zawierać , w zgodzie ze specyfikacją warunków audytu:

- stwierdzenie, że najwyższe kierownictwo jest odpowiedzialne za system kontroli wewnętrznej organizacji,
- stwierdzenie, że system kontroli wewnętrznej może dać tylko rozsądne (umiarkowane) a nie absolutne poświadczenie [zapewnienie] jeśli chodzi o istotne przekłamania lub straty,
- opis kluczowych procedur ustanowionych przez najwyższe kierownictwo w celu uzyskania skutecznego systemu nadzoru nad IT oraz dotyczącą je dokumentację,
- informacje o każdej niezgodności z politykami danej organizacji lub dowolnymi innymi przepisami prawa, regulacjami, przepisami branżowymi dotyczącymi nadzoru w przedsiębiorstwach,
- informacje o wszystkich większych ryzykach poza kontrolą,
- informacje na temat wszystkich nieskutecznych czy niewydajnych struktur kontroli, mechanizmów kontrolnych lub procedur, razem z rekomendacjami audytora SI odnośnie ich naprawy,
- ogólne wnioski audytora SI na temat nadzoru nad IT, tak jak to zdefiniowano w specyfikacji warunków audytu.

7. DZIAŁANIA POAUDYTOWE

7.1 Realizacja zgodnie z harmonogramem

7.1.1 Skutki dowolnej słabości w systemie nadzoru przedsiębiorstwa mają zwykle szeroki zasięg i stanowią wysokie ryzyko. Dlatego audytor SI powinien, tam gdzie to jest właściwe, przeprowadzić wystarczające, terminowe prace poaudytowe w celu weryfikacji, że kierownictwo podjęło właściwe działania w celu naprawy słabości.

8. OBOWIĄZYWANIE

8.1 **Powyższa wytyczna obowiązuje w stosunku do wszystkich audytów systemów informatycznych rozpoczynających się począwszy od dnia 1 lipca 2002 roku.**

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

1. PODSTAWA

1.1 Powiązanie ze standardami

1.1.1 Standard 060.020 (Dowody) stanowi, że "Podczas przeprowadzania audytu Audytor Systemów Informatycznych (Audytor SI) zobowiązany jest uzyskać wystarczające, wiarygodne, stosowne i użyteczne dowody, aby efektywnie zrealizować cele audytu. Spostrzeżenia i wnioski z audytu mają być poparte odpowiednią analizą i interpretacją tych dowodów".

1.2 Potrzeba Wytycznej

1.2.1 Zarządzanie i monitorowanie dowolnej organizacji, departamentu lub funkcji ma wpływ na sposób, w jaki ta organizacja, departament lub funkcja się zachowuje, uwzględniając w tym sposób stosowania mechanizmów kontrolnych. Zasadę tę stosuje się zarówno do wykorzystywania SI jak i kierowania firmą produkcyjną, departamentem płatności, jak i departamentem skarbu.

1.2.2 Skuteczność szczegółowych mechanizmów kontrolnych SI działających w ramach organizacji jest ograniczona skutecznością zarządzania i monitorowania wykorzystania SI w organizacji jako całości. Często jest to uwzględniane w wytycznych dla audytu finansowego, gdzie potwierdzony jest wpływ "ogólnych" mechanizmów kontrolnych stosowanych w środowisku SI na "aplikacyjne" mechanizmy kontrolne w systemach finansowych. Na przykład, brytyjska Wytyczna Audytu 3.2.407 (Audyt w Środowisku Komputerowym) stwierdza: "Silne ogólne mechanizmy kontrolne przyczyniają się do poziomu pewności, który audytor może uzyskać w stosunku do aplikacyjnych mechanizmów kontrolnych. Niesatysfakcjonujące ogólne mechanizmy kontrolne mogą podważyć silne mechanizmy kontrolne aplikacji lub pogorszyć niesatysfakcjonujące aplikacyjne mechanizmy kontrolne."

1.2.3 Publikacja "Control Objectives for Information and related Technology" (COBIT) wydana przez ISACF (Information Systems Audit and Control Foundation) dostarcza zasad, mogących pomóc audytorowi SI rozróżnić pomiędzy:

- szczegółowymi mechanizmami kontrolnymi SI, bezpośrednio związanymi z zakresem audytu SI,
- cechami zarządzania i monitorowania SI, przyczyniającymi się do poziomu pewności, który może uzyskać audytor SI w stosunku do tych szczegółowych mechanizmów kontrolnych.

1.2.4 Podział na ogólne i aplikacyjne mechanizmy kontrolne został zaprojektowany w szczególności do stosowania w trakcie audytów, których celem jest sformułowanie opinii stwierdzającej czy informacja finansowa jest wolna od istotnych błędów (audyt finansowy).

1.2.5 Podczas przeprowadzania audytu SI przez audytorów wewnętrznych i niezależnych konsultantów, zazwyczaj cel i zakres audytu jest inny niż dla audytu finansowego. Używane systemy są kombinacją procesów manualnych i komputerowych, a cele kontrolne muszą obejmować całość procesu, który może być zarówno szerszy jak i węższy od (prowadzenia - przyp. tłum.) zapisów księgowych. Dlatego też, struktura mechanizmów kontrolnych stosowana dla audytów finansowych może być nieodpowiednia dla pewnych audytów SI.

1.2.6 W celu sformułowania opinii nt. skuteczności szczegółowych mechanizmów kontrolnych poddawanych audytowi, audytor SI powinien rozważyć potrzebę oceny skuteczności zarządzania i monitorowania SI, nawet jeśli tego typu sprawy pozostają poza uzgodnionym zakresem audytu. Wynik tych rozważań może prowadzić do szeregu konsekwencji: od rozszerzenia zakresu audytu do sporządzenia raportu z odpowiednimi zastrzeżeniami.

1.2.7 Całkowita liczba mechanizmów kontrolnych dotyczących zarządzania i monitorowania jest duża, a niektóre z nich mogą być niezwiązane z określonym celem audytu. Aby oszczędzić ryzyko audytu i przyjąć odpowiednie podejście audytowe, audytor SI potrzebuje strukturalnej metody określającej:

- te mechanizmy kontrolne dotyczące zarządzania i monitorowania, które będą stosowne dla zakresu i celu audytu,
- te mechanizmy kontrolne dotyczące zarządzania i monitorowania, które powinny być przetestowane,
- wpływ stosownych mechanizmów kontrolnych dotyczących zarządzania i monitorowania na opinię audytora.

Może być to osiągnięte poprzez użycie specyficznej dla SI i technologii informatycznych struktury mechanizmów kontrolnych, która pomoże audytorowi SI w skupieniu się na kluczowych mechanizmach kontrolnych, wpływających na systemy informacyjne i operacje podlegające audytowi.

1.2.8 Niniejsza Wytyczna dostarcza wskazówek, jak wdrażać standardy audytowania SI. Audytor SI powinien wziąć ją pod uwagę określając sposób wdrożenia w/w Standardu (060.020 - Dowody), powinien posłużyć się swoim profesjonalnym osądem podczas jej stosowania i być gotowym uzasadnić każde odstępstwo od niej.

2. STRUKTURA MECHANIZMÓW KONTROLNYCH

2.1 Wstęp

2.1.1 COBIT definiuje "kontrolę" jako "Polityki, procedury, praktyki i struktury organizacyjne, które muszą dostarczać racjonalnych zapewnień, że cele biznesowe będą osiągnięte oraz będzie wykonywana prewencja przez niepożądanymi zdarzeniami lub będą one wykryte i nastąpią działania korekcyjne". Dla każdego audytu SI, audytor SI powinien rozróżnić pomiędzy ogólnymi mechanizmami kontrolnymi, które wpływają na wszystkie systemy informacyjne i operacje (skrótnie mechanizmy kontrolne), a ogólnymi i aplikacyjnymi mechanizmami kontrolnymi, działającymi na bardziej specyficznym poziomie (szczegółowe mechanizmy kontrolne), aby skoncentrować działania audytowe na obszarach ryzyka związanych z celem audytu SI. Zamierzeniem poniższego opisu struktury mechanizmów kontrolnych jest pomoc audytorowi SI w osiągnięciu wspomnianej koncentracji działań..

2.2 Skrótnie mechanizmy kontrolne SI

2.2.1 Termin "skrótnie mechanizmy kontrolne SI" zdefiniowany jest w słowniczku (umieszczonym na końcu niniejszej wytycznej - przyp. tłum.). Przykłady tego typu mechanizmów kontrolnych obejmują mechanizmy kontrolne procesów SI zdefiniowane w

standardzie COBIT w domenach Planowanie i Organizacja oraz Monitorowanie; t.j. "PO1 - Definiowanie planu strategicznego IT" i "M1 - Monitorowanie procesów". Skróśne mechanizmy kontrolne są podzbiorem ogólnych mechanizmów kontrolnych, będąc tymi ogólnymi mechanizmami kontrolnymi, które skupiają się na zarządzaniu i monitorowaniu SI.

2.2.2 Wpływ skróśnych mechanizmów kontrolnych SI na pracę audytora SI nie jest ograniczony jedynie do rzetelności mechanizmów kontrolnych w systemach finansowych. Skróśne mechanizmy kontrolne SI wpływają również na rzetelność szczegółowych mechanizmów kontrolnych SI dotyczących np.:

- Program development
- rozwoju oprogramowania,
- wdrażania systemów,
- zarządzania bezpieczeństwem,
- procedur składowania.

2.2.3 Słabe zarządzanie i monitorowanie SI (t.j. słabe skróśne mechanizmy kontrolne) powinny ostrzec audytora SI o możliwości wystąpienia wysokiego poziomu ryzyka, że mechanizmy kontrolne zaprojektowane dla działań na poziomie szczegółowym mogą być nieskuteczne.

2.3 Szczegółowe mechanizmy kontrolne

2.3.1 Termin szczegółowe mechanizmy kontrolne zdefiniowany jest w słowniczku (umieszczonym na końcu niniejszej wytycznej - przyp. tłum.). Składają się na nie aplikacyjne mechanizmy kontrolne i te ogólne mechanizmy kontrolne, które nie są zawarte w skróśnych mechanizmach kontrolnych. W części "Struktura" standardu COBIT (COBIT framework), szczegółowe mechanizmy kontrolne to te, które dotyczą nabywania, wdrażania, dostarczania i wspierania systemów i usług SI. Przykładami mogą być mechanizmy kontrolne dotyczące:

- wdrażania pakietów oprogramowania,
- parametrów bezpieczeństwa systemów,
- planowania odtworzenia po awarii,
- sprawdzania poprawności i ważności danych wejściowych,
- generowania raportów nt. występowania błędów/sytuacji wyjątkowych,
- blokowania kont użytkowników po próbach niepoprawnego logowania się.

Aplikacyjne mechanizmy kontrolne są podzbiorem szczegółowych mechanizmów kontrolnych. Np. sprawdzanie poprawności i ważności danych wejściowych jest zarówno szczegółowym mechanizmem kontrolnym SI, jak i aplikacyjnym mechanizmem kontrolnym. Instalowanie i akredytacja systemów (AI5) jest szczegółowym mechanizmem kontrolnym SI, ale nie jest aplikacyjnym mechanizmem kontrolnym.

2.3.2 Związki pomiędzy mechanizmami kontrolnymi SI przedstawione są poniżej:

Mechanizmy kontrolne SI

- Ogólne mechanizmy kontrolne
 - Skróśne mechanizmy kontrolne
 - Szczegółowe mechanizmy kontrolne
- Aplikacyjne mechanizmy kontrolne

Dodatkowo, audytor SI powinien rozważyć wpływ mechanizmów kontrolnych nie dotyczących SI na zakres i procedury audytowe.

2.4 Wzajemne współdziałanie skróśnych i szczegółowych mechanizmów kontrolnych

2.4.1 Struktura standardu COBIT (COBIT framework) dzieli procesy kontrolne SI na cztery domeny:

- Planowanie i organizowanie,
- Nabywanie i wdrażanie,
- Dostarczanie i wspieranie,
- Monitorowanie.

2.4.2 Na skuteczność mechanizmów kontrolnych działających w ramach domen: Nabywanie i wdrażanie (AI) oraz Dostarczanie i wspieranie (DS) wpływa skuteczność mechanizmów kontrolnych działających w ramach domen: Planowanie i organizowanie (PO) oraz Monitorowanie (M). Niewłaściwe planowanie, organizowanie i monitorowanie przez kierownictwo powoduje to, że mechanizmy kontrolne dotyczące nabywania, wdrażania i dostarczania usług oraz wspierania będą nieskuteczne. I odwrotnie, właściwe planowanie, organizowanie i monitorowanie mogą zidentyfikować i skorygować nieskuteczne mechanizmy kontrolne dotyczące nabywania, wdrażania i dostarczania usług oraz wspierania.

2.4.3 Przykładowo, na skuteczność szczegółowych mechanizmów kontrolnych SI dotyczących procesu "Nabywanie i utrzymywanie oprogramowania aplikacyjnego" (ozn. AI2 wg COBIT) wpływa adekwatność skróśnych mechanizmów kontrolnych SI dotyczących następujących procesów:

- "Definiowanie strategicznego planu IT" (proces PO1 wg COBIT),
- "Zarządzanie projektami" (proces PO10 wg COBIT),
- "Zarządzanie jakością" (proces PO11 wg COBIT),
- "Monitorowanie procesów" (proces M1 wg COBIT).

2.4.4 Audyt procesu nabywania oprogramowania aplikacyjnego powinien zawierać identyfikację wpływu strategii SI, podejścia do zarządzania projektami, zarządzania jakością i podejścia do monitorowania. Tam, gdzie np. zarządzanie projektami jest nieodpowiednie, audytor SI powinien rozważyć:

- zaplanowanie dodatkowych prac, zmierzających do uzyskania zapewnienia, że określony projekt, który jest audytowany, jest skutecznie zarządzany,

- zaraportowanie kierownictwu słabości skrótnych mechanizmów kontrolnych.
- 2.4.5** Kolejnym przykładem jest to, że na skuteczne szczegółowe mechanizmy kontrolne SI dotyczące procesu "Zapewnienie bezpieczeństwa systemu" (proces DS5 wg COBIT) wpływa adekwatność skrótnych mechanizmów kontrolnych dotyczących procesów:
- "Definiowanie organizacji i relacji IT" (proces PO4 wg COBIT),
 - "Komunikowanie celów i kierunków określonych przez kierownictwo" (proces PO6 wg COBIT),
 - "Szacowanie ryzyka" (proces PO9 wg COBIT),
 - "Monitorowanie procesów" (proces M1 wg COBIT).
- 2.4.6** Audyt adekwatności parametrów bezpieczeństwa w systemie, np. UNIX, Windows NT, RACF, powinien uwzględnić rozważenie polityk zarządzania bezpieczeństwem (PO9) i procedur monitorowania zgodności z tymi politykami (M1). Nawet, jeśli parametry nie są zgodne z poglądami audytora SI na tzw. "najlepsze praktyki", to mogą być ocenione jako odpowiednie z punktu widzenia ryzyka zidentyfikowanego przez kierownictwo oraz polityk zarządzania, wskazujących, w jaki sposób należy się odnieść do takiego poziomu ryzyka. Każda rekomendacja wynikająca z audytu powinna więc uwzględniać zarówno zarządzanie ryzykiem i polityki dotyczące ryzyka, jak i same szczegółowe parametry.

3. PLANOWANIE

3.1 Podejście do powiązanych (z audytem - przyp. tłum) skrótnych mechanizmów kontrolnych SI

3.1.1 Wytyczna audytu dotycząca planowania audytu stanowi, że audytor SI powinien przeprowadzić wstępną ocenę mechanizmów kontrolnych dotyczących funkcji, które będą audytowane. Ta wstępna ocena powinna uwzględniać identyfikację i ocenę stosownych skrótnych mechanizmów kontrolnych SI. Testowanie skrótnych mechanizmów kontrolnych może przebiegać w różnym cyklu dla specyficznego prowadzonego audytu SI, gdyż z powodu swojej istoty obejmują wiele różnych aspektów użytkownika SI. Dlatego audytor SI powinien rozważyć, czy nie można oprzeć się na wynikach któregoś z poprzednich audytów, w celu zidentyfikowania i oceny tych mechanizmów kontrolnych.

3.1.2 Jeśli audyt wskazuje, że skrótno mechanizmy kontrolne SI są niesatysfakcjonujące, to audytor SI powinien rozważyć wpływ tej obserwacji na planowane podejście dla osiągnięcia celu audytu:

- silne skrótno mechanizmy kontrolne SI mogą przyczynić się do uzyskania przez audytora SI zapewnienia w odniesieniu do szczegółowych mechanizmów kontrolnych SI,
- słabe skrótno mechanizmy kontrolne SI mogą podważyć silne szczegółowe mechanizmy kontrolne SI lub zwiększyć słabości na szczegółowym poziomie.

3.2 Należyte procedury audytu

3.2.1 W sytuacji, gdy skrótno mechanizmy kontrolne mają potencjalnie znaczący wpływ na cel audytu, nie jest wystarczające planowanie audytu wyłącznie szczegółowych mechanizmów kontrolnych. Jeśli audyt skrótnych mechanizmów kontrolnych jest niemożliwy lub niepraktyczny, należy w raporcie umieścić stwierdzenie o takim ograniczeniu.

3.2.2 Audytor SI powinien planować testowanie stosownych skrótnych mechanizmów kontrolnych, w sytuacji gdy przyczyni się to do osiągnięcia celu audytu.

3.3 Stosowne mechanizmy kontrolne

3.3.1 Stosowne skrótno mechanizmy kontrolne to te, które mają wpływ na specyficzne cele audytu określone dla zadania audytowego. Przykładowo, jeśli celem audytu jest raport na temat mechanizmów kontrolnych dotyczących wprowadzania zmian do określonej biblioteki programowej, to skrótno mechanizmy kontrolne SI dotyczące polityk bezpieczeństwa (PO6) będą istotne (dla celu audytu - przyp. tłum.), natomiast skrótno mechanizmy kontrolne dotyczące określania kierunku technologicznego (PO3) mogą być nieistotne (dla celu audytu - przyp. tłum.).

3.3.2 Podczas planowania audytu, audytor SI powinien rozpoznać, które z ogólnej liczby skrótnych mechanizmów kontrolnych mają wpływ na specyficzne cele audytu i powinien zaplanować ich włączenie do zakresu audytu. Cele kontrolne COBIT dla domen Planowanie i Organizacja i "Monitorowanie" mogą pomóc w doborze istotnych, skrótnych mechanizmów kontrolnych SI.

3.4 Dowód audytowy

3.4.1 Skrótno mechanizmy kontrolne niekoniecznie mogą być udokumentowane, ale audytor SI powinien zaplanować pozyskanie dowodów audytowych, świadczących o skutecznym działaniu stosownych mechanizmów kontrolnych. Potencjalne testy są naszkicowane w punkcie Przeprowadzenie Audytu.

3.5 Podejście do stosownych szczegółowych mechanizmów kontrolnych SI

3.5.1 W sytuacji, gdy przeprowadzany audyt wskazuje, że skrótno mechanizmy kontrolne są satysfakcjonujące, audytor SI powinien rozważyć obniżenie poziomu testowania, zaplanowanego dla szczegółowych mechanizmów kontrolnych. Dowody audytowe istnienia mocnych skrótnych mechanizmów kontrolnych będą przyczyniać się do uzyskania przez audytora SI poziomu pewności, odnoszącego się do szczegółowych mechanizmów kontrolnych.

3.5.2 W sytuacji, gdy przeprowadzany audyt wskazuje, że skrótno mechanizmy kontrolne nie są satysfakcjonujące, audytor SI powinien przeprowadzić wystarczające testowanie szczegółowych mechanizmów kontrolnych. Celem jest uzyskanie dowodów, że szczegółowe mechanizmy kontrolne działają skutecznie pomimo słabych skrótnych mechanizmów kontrolnych istotnych dla audytowanego obszaru.

4. PROWADZENIE PRAC

4.1 Testowanie skrótnych mechanizmów kontrolnych SI

4.1.1 Audytor SI powinien przeprowadzić odpowiednie testowanie, dostarczające zapewnienia, że stosowne skrótnie mechanizmy kontrolne SI działają skutecznie w okresie prowadzenia audytu lub określonym momencie czasu. Procedury testów, które mogą być odpowiednie do tego celu, uwzględniają:

- obserwację,
- badania (zapytania) potwierdzające,
- przegląd stosownej dokumentacji (polityk, standardów, protokołów ze spotkań itp.),
- ponowne wykonanie (działań kontrolnych - przyp. tłum.) np. z użyciem CAAT - komputerowych technik wspomaganie audytu.

4.1.2 Jeśli testowanie stosownych skrótnych mechanizmów kontrolnych wskazuje, że są one satysfakcjonujące, to audytor SI powinien kontynuować zaplanowany przegląd szczegółowych mechanizmów kontrolnych SI, które są bezpośrednio powiązane z celem audytu. Poziom takiego testowania może być mniejszy od poziomu wymaganego w sytuacji, gdy skrótnie mechanizmy kontrolne SI nie działałyby w sposób satysfakcjonujący.

5. RAPORTOWANIE

5.1 Słabości skrótnych mechanizmów kontrolnych

5.1.1 W sytuacji, gdy audytor SI zidentyfikuje słabości skrótnych mechanizmów kontrolnych SI, powinny być one przedstawione kierownictwu, nawet jeśli tego typu zagadnienia nie były wyraźnie określone w uzgodnionym zakresie prac audytowych.

5.2 Ograniczenia zakresu

5.2.1 W sytuacji, gdy skrótnie mechanizmy kontrolne SI mogą mieć potencjalnie znaczący wpływ na skuteczność szczegółowych mechanizmów kontrolnych, a nie były one poddane audytowi, audytor SI powinien przedstawić ten fakt w raporcie końcowym, razem z określeniem jego potencjalnego wpływu na spostrzeżenia, wnioski i rekomendacje zawarte w raporcie. Na przykład, jeśli audytor SI przygotowuje raport z audytu dotyczącego nabywania pakietów oprogramowania, ale nie widział strategii organizacji dotyczącej SI, powinien w raporcie umieścić zdanie, że strategia SI nie była dostępna lub nie istnieje. Jeśli jest to istotne, audytor SI powinien umieścić w raporcie zapis o potencjalnym wpływie tego faktu na spostrzeżenia, wnioski i rekomendacje np. zdanie o braku możliwości stwierdzenia, że nabycie oprogramowania jest spójne ze strategią SI i że będzie wspierać przyszłe plany biznesowe.

6. OBOWIĄZYWANIE

7. Niniejsza Wytyczna obowiązuje wszystkie audyty systemów informatycznych rozpoczynające się począwszy od 1 marca 2000.

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

- 1.1.1** Standard 060.020 (Dowody) stwierdza: „Zadaniem Audytora Systemów Informatycznych podczas przeprowadzania audytu jest zgromadzenie wystarczających, wiarygodnych, istotnych i użytecznych dowodów służących efektywnej realizacji zadań audytorskich. Wykrycia audytu oraz wnioski powinny być poparte odpowiednią analizą i interpretacją tychże dowodów.
- 1.1.2** Standard 050.010 (Planowanie audytu) stwierdza: „Audytor Systemów Informatycznych powinien planować prace związane z audytem systemów informatycznych pod kątem realizacji celów audytorskich oraz zgodnie ze stosowanymi standardami.”
- 1.1.3** Standard 030.020 (Należyta profesjonalna staranność) stwierdza: „Wobec wszystkich aspektów pracy Audytora Systemów Informatycznych obowiązuje właściwa profesjonalna staranność i przestrzeganie stosowanych standardów audytorskich.”

1.2 Potrzeba wytycznej

- 1.2.1** Techniki Komputerowego Wspomaganie Audytu (CAATs) stanowią dla Audytora Systemów Informatycznych (SI) ważne narzędzie do przeprowadzania audytów.
- 1.2.2** CAATs składają się z wielu rodzajów narzędzi i technik, jak standardowe oprogramowanie audytorskie, oprogramowanie użytkowe, dane testowe, aplikacje do śledzenia i mapowania oraz eksperckie systemy audytorskie.
- 1.2.3** Narzędzi CAATs można używać do przeprowadzania różnorodnych operacji audytorskich, do których należą:
 - Testowanie szczegółów transakcji i sald,
 - Procedury przeglądów analitycznych,
 - Testy zgodności z ogólnymi regułami zarządzania systemami informatycznymi,
 - Testy zgodności z zasadami zarządzania aplikacjami,
 - Testy włamaniowe.
- 1.2.4** Narzędzia CAATs mogą generować dużą ilość dowodów audytorskich związanych z audytem systemów informatycznych, tak więc Audytor SI powinien w sposób ostrożny zaplanować zbiór dowodów rzeczowych, zgodnie z właściwą profesjonalną starannością w stosowaniu narzędzi CAATs.
- 1.2.5** Wytyczna ta dostarcza wskazówek dla stosowania standardów audytu informatycznego. Audytor SI powinien brać ją pod uwagę podczas określania sposobu implementacji powyższych Standardów, stosowania profesjonalnej oceny przy ich zastosowaniu oraz być przygotowanym do uzasadnienia wszelkich od nich odstępstw.
- 1.2.6** Wskazówki te powinny być stosowane wobec używania narzędzi CAATs niezależnie od tego, czy audytorem jest Audytor SI, czy inny.

2. PLANOWANIE

2.1 Czynniki decyzyjne stosowania CAATs

- 2.1.1** Audytor SI w trakcie planowania audytu powinien rozważyć zastosowanie odpowiedniej kombinacji technik manualnych oraz narzędzi CAATs. Przy podejmowaniu decyzji o tym, czy stosować CAATs, powinny być brane pod uwagę następujące czynniki:
 - Wiedza informatyczna, biegłość i doświadczenie Audytora SI,
 - Dostępność odpowiednich narzędzi CAATs oraz narzędzi informatycznych,
 - Przewaga stosowania narzędzi CAATs nad technikami manualnymi pod względem wydajności i efektywności,
 - Ograniczenia czasowe,
 - Integralność systemu informatycznego ze środowiskiem informatycznym,
 - Poziom ryzyka.

2.2 Kolejne kroki planowania CAATs

- 2.2.1** Podstawowymi krokami, jakie powinien podjąć Audytor SI podczas przygotowywania się do zastosowania wybranych narzędzi CAATs, są:
 - Ustalenie celów audytorskich związanych z CAATs,
 - Wyznaczenie poziomu i łatwości dostępu do funkcjonujących w organizacji narzędzi informatycznych, programów/systemów oraz danych,
 - Zdefiniowanie procedur, które należy przeprowadzić (np. próbkowania statystycznego, rekalkulacji, potwierżeń, itd.),
 - Zdefiniowanie wymagań dotyczących danych wyjściowych,
 - Ustalenia wymagań co do zasobów, np. personelu, narzędzi CAATs, środowiska przetwarzania (narzędzia informatyczne organizacji oraz narzędzia audytu informatycznego),
 - Określenia zasad dostępu do funkcjonujących w organizacji narzędzi informatycznych, programów/systemów oraz danych, z definicją zbiorów włącznie,
 - Udokumentowanie wskazanych do zastosowania narzędzi CAATs, włącznie z obiektami docelowymi, tablicami przepływu danych oraz instrukcjami obsługi.

2.3 Uzgodnienie warunków z osobami, których dotyczy audyt

- 2.3.1** Ponieważ zbiory danych takie, jak na przykład szczegółowe zbiory transakcyjne, są przechowywane tylko przez krótki okres

- czasu, Audytor SI powinien dokonać ustaleń dotyczących przechowania danych obejmujących wskazany czas audytu.
- 2.3.2** W celu zminimalizowania zakłóceń w środowisku produkcyjnym organizacji, dostęp do organizacyjnych narzędzi informatycznych, programów/systemów oraz danych powinien zostać uzgodniony z właściwym wyprzedzeniem.
- 2.3.3** Audytor SI powinien oszacować ewentualne zakłócenia, jakie spowodować mogą zmiany w programach/systemach produkcyjnych wywołane zastosowaniem narzędzi CAATs. Robiąc to, Audytor SI powinien wziąć pod uwagę wpływ tych zmian na integralność i użyteczność CAATs tak samo, jak na integralność używanych programów/systemów oraz danych.

2.4 Testowanie CAATs

- 2.4.1** Przeprowadzając odpowiednie planowanie, projektowanie, testowanie, przetwarzanie oraz uważnie śledząc dokumentację Audytor SI powinien uzyskać realne zapewnienie integralności, wiarygodności, użyteczności oraz bezpieczeństwa użytkowania CAATs. Wszystko to powinno zostać wykonane zanim zaufa się narzędziom CAATs. Rodzaj, czas i zakres testów zależy od dostępności na rynku oraz stabilności CAATs.

2.5 Bezpieczeństwo danych oraz CAATs

- 2.5.1** Wszędzie tam, gdzie do pobierania danych do przeprowadzenia analiz używa się narzędzi CAATs, Audytor SI powinien sprawdzać integralność systemu informatycznego oraz środowiska, z którego pobierane są te dane..
- 2.5.2** CAATs mogą być używane do pobierania szczególnie wrażliwych informacji systemowych oraz danych produkcyjnych, które powinny być utrzymywane w tajemnicy. Audytor SI powinien zapewnić odpowiedni poziom poufności i bezpieczeństwa informacji systemowych oraz danych produkcyjnych. Robiąc to, Audytor SI powinien brać pod uwagę poziom poufności i bezpieczeństwa, wymagany przez organizację, będącą właścicielem tych danych, oraz odpowiednie regulacje prawne.
- 2.5.3** Aby zapewnić bieżącą integralność, wiarygodność, użyteczność oraz bezpieczeństwo narzędzi CAATs, Audytor SI powinien stosować odpowiednie procedury i dokumentować ich wyniki. W ramach tego, na przykład w celu upewnienia się, że w oprogramowaniu audytorskim CAATs zostały wykonane tylko autoryzowane zmiany, powinien dokonywać przeglądu obsługi programów i zmiany wbudowanych w oprogramowanie parametrów sterujących.
- 2.5.4** Jeśli rezydujące w środowisku narzędzia CAATs nie znajdują się pod bezpośrednią kontrolą Audytora SI, to w celu identyfikacji zmian w CAATs powinien zostać ustawiony odpowiedni poziom kontroli. Poprzez odpowiednie sposoby planowania, projektowania, testowania, przetwarzania i przeglądania dokumentacji Audytor powinien uzyskiwać zapewnienie integralności, wiarygodności, użyteczności oraz bezpieczeństwa narzędzi CAATs, zanim jeszcze nabierze do nich zaufania.

3. PROWADZENIE PRAC

3.1 Gromadzenie dowodów audytorskich

- 3.1.1** Aby Audytor SI mógł w sposób realny upewnić się, że zostały osiągnięte cele audytu oraz szczegółowe specyfikacje związane z narzędziami CAATs, powinien kontrolować ich stosowanie. Audytor SI powinien:
- Tam, gdzie jest to właściwe, dokonywać uzgodnienia sum kontrolnych,
 - Sprawdzać realność danych wyjściowych,
 - Dokonywać przeglądu narzędzi CAATs pod kątem ich logiki, parametryzacji i innych charakterystycznych danych,
 - Kontrolować główne informatyczne dane sterujące, używane w organizacji, które mogą mieć wpływ na integralność narzędzi CAATs (np. programowe zmiany danych sterujących oraz dostępu do systemów, oprogramowania i/lub zbiorów danych).

3.2 Uniwersalne oprogramowanie audytorskie

- 3.2.1** Uzyskując dostęp do danych produkcyjnych przy zastosowaniu uniwersalnego oprogramowania audytorskiego Audytor SI powinien przedsięwziąć odpowiednie kroki zabezpieczające integralność tych danych. Przy wbudowanym systemie audytorskim Audytor SI powinien być włączony do projektu systemu, jak również w ramach funkcjonujących w organizacji programów/systemów muszą być rozwijane odpowiednie techniki ich obsługi.

3.3 Oprogramowanie użytkowe

- 3.3.1** Posługując się oprogramowaniem użytkowym Audytor SI powinien upewnić się, że podczas jego przetwarzania nie wystąpiły żadne nieplanowane ingerencje, oraz że zostało ono uzyskane z odpowiedniej biblioteki systemowej. Audytor SI powinien również podjąć odpowiednie kroki zabezpieczające integralność funkcjonującego w organizacji systemu oraz zbiorów, jako że oprogramowanie użytkowe łatwo może je uszkodzić.

3.4 Dane testowe

- 3.4.1** Używając danych testowych Audytor SI powinien być świadomy tego, że dane te służą jedynie do wskazania potencjalnie błędnych procesów; technika ta nie pozwala ocenić bieżących danych produkcyjnych. Audytor SI powinien również zdawać sobie sprawę z tego, że analiza danych w zależności od liczby przetwarzanych transakcji, liczby testowanych programów oraz złożoności programów/systemów może być wyjątkowo skomplikowana i czasochłonna. Przed użyciem danych testowych Audytor SI powinien sprawdzić, czy ich zastosowanie nie odbije się w sposób trwały na systemie produkcyjnym.

3.5 Oprogramowanie aplikacyjne do śledzenia i mapowania

3.5.1 Posługując się oprogramowaniem do śledzenia i mapowania Audytor SI powinien uzyskać potwierdzenie, że oceniany kod źródłowy posłużył do wygenerowania oprogramowania, które w chwili obecnej używane jest jako produkcyjne. Audytor SI powinien wiedzieć, że oprogramowanie do śledzenia i mapowania może jedynie wskazać potencjalnie błędne procesy, lecz nie oddaje oceny aktualnych danych produkcyjnych.

3.6 Eksperckie systemy audytorskie

3.6.1 Używając eksperckich systemów audytorskich Audytor SI, w celu uzyskania zapewnienia, że opracowane ścieżki decyzyjne odpowiadają konkretnej sytuacji i środowisku poddawanemu audytowi, powinien posiadać dogłębną wiedzę na temat działania systemu.

4. DOKUMENTOWANIE CAATs

4.1 Dokumenty robocze

4.1.1 Aby otrzymać odpowiednie dowody audytorskie, należy w sposób wystarczający dokumentować krok po kroku wszystkie procesy przeprowadzane przy pomocy narzędzi CAATs.

4.1.2 Audytorskie dokumenty robocze powinny zawierać w szczególności dokumentację opisującą zastosowanie narzędzi CAATs, włącznie z detalami opisanymi poniżej.

4.2 Planowanie

4.2.1 Dokumentacja powinna zawierać:

- Cele zastosowania narzędzi CAATs,
- Wyznaczone do użycia narzędzia CAATs,
- Badania do przeprowadzenia,
- Osoby wykonujące oraz harmonogram.

4.3 Wykonanie

4.3.1 Dokumentacja powinna zawierać:

- Sposób przygotowania narzędzi CAATs oraz procedury testowe i parametry sterujące,
- Szczegółowy opis testów przeprowadzanych przy pomocy narzędzi CAATs,
- Szczegółowy opis danych wejściowych (np. użyte dane, zbiory wynikowe), przetwarzań (np. tablice przepływów, schematy logiczne) oraz danych wyjściowych (np. raporty, zapisy zdarzeń systemowych – log files),
- Listę istotnych parametrów lub kod źródłowy.

4.4 Dowody audytorskie

4.4.1 Dokumentacja powinna zawierać:

- Powstałe zbiory wyjściowe,
- Opis sposobu przeprowadzania analizy audytorskiej zbiorów wyjściowych,
- Wykrycia audytorskie,
- Wnioski z prac audytorskich,
- Rekomendacje audytorskie.

5. RAPORTOWANIE

5.1 Opis narzędzi CAATs

5.1.1 Sekcja raportu dotycząca celów, zakresu oraz metodologii pracy powinna zawierać klarowny opis użytych narzędzi CAATs. Opis ten nie powinien być nadmiernie szczegółowy, lecz ma dać czytającemu dobry ogłęd sprawy.

5.1.2 Opis użytych narzędzi CAATs powinien być również umieszczony w części raportu dotyczącej konkretnych wykryć związanych z użyciem wskazanych narzędzi.

5.1.3 Jeśli opis narzędzi CAATs ma zastosowanie do kilku wykryć lub jest zbyt szczegółowy, powinien zostać krótko omówiony w części raportu dotyczącej celów, zakresu i metodologii pracy, a czytający może zostać odesłany do załącznika zawierającego bardziej szczegółowy opis.

6. OBOWIĄZYWANIE

6.1 Wytuczna powyższa obowiązuje w stosunku do wszystkich audytów systemów informatycznych rozpoczynających się począwszy od 1 grudnia 1998.

060.020.080 Wykorzystanie prac innych audytorów i ekspertów

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

1.1.1 Standard 060.020 (Dowody): podczas przeprowadzania audytu, audytor systemów informatycznych jest zobowiązany do tego, aby uzyskać wystarczające, wiarygodne i odpowiednie dowody, pozwalające w efektywny sposób osiągnąć cel audytu. Konkluzje i wyniki audytu powinny być wsparte przez odpowiednie analizy i interpretacje zidentyfikowanych dowodów.

1.2 Potrzeba wytycznej

1.2.1 Współzależności zachodzące między klientami i dostawcami oraz działalnością zleconą firmom zewnętrznym i tą prowadzoną przez firmę powoduje, że część obszaru podlegająca audytowi jest kontrolowana lub audytowana przez inne niezależne funkcje i organizacje. Poniższe wytyczne ustalają w jaki sposób audytor systemów informatycznych powinien spełnić powyższy standard w opisanych okolicznościach. Podporządkowanie się tym wytycznym nie jest obowiązkowe, jednak audytor systemów informatycznych powinien być przygotowanym by móc uzasadnić wszelkie odstępstwa.

2. STATUT AUDYTU

2.1 Prawo dostępu do wyników prac innych audytorów i ekspertów

2.1.1 Audytor systemów informatycznych powinien przeanalizować te obszary, w przypadku których prace innych audytorów i ekspertów pokrywają się z celami audytu systemów informatycznych. W takich przypadkach statut audytora lub umowa o badanie uprawniają audytora systemów informatycznych do dostępu do wyników tych prac.

3. PLANOWANIE

3.1 Okoliczności planowania

3.1.1 W przypadku gdy audyt systemów informatycznych wymaga skorzystania z wyników prac innych audytorów i ekspertów, audytor systemów informatycznych powinien uwzględnić ich działalność i ich wpływ na cele audytu podczas planowania badania. Proces planowania powinien obejmować:

- Ocenę niezależności i obiektywności innych audytorów lub ekspertów.
- Ocenę ich kompetencji zawodowych
- Zrozumienie zakresu ich prac i zastosowanego podejścia do zagadnienia
- Określenie wymaganego zakresu przeglądu wyników prac innych audytorów lub ekspertów

3.2 Niezależność i obiektywność

3.2.1 Proces selekcji i wybór, status organizacyjny, sposób raportowania oraz efekt rekomendacji na zmianę sposobu zarządzania są wskaźnikami oceny niezależności i obiektywności innych audytorów i ekspertów.

3.3 Kompetencje zawodowe

3.3.1 Kwalifikacje, doświadczenie i zasoby wykorzystane przez innych audytorów i ekspertów powinny zostać wzięte pod uwagę przy ocenie ich kompetencji zawodowych..

3.4 Zakres prac i zastosowane podejście

3.4.1 Zakres prac i zastosowane podejście z reguły jest określone w statucie audytora lub eksperta, wynika z umowy o badanie bądź z kompetencji audytora czy eksperta..

3.5 Określenie wymaganego zakresu przeglądu wyników prac innych audytorów i ekspertów

3.5.1 Rodzaj, zakres czasowy i jakość dowodów na potrzeby prowadzonego badania będzie uzależniony od istotności prac innych audytorów i ekspertów nad systemami informatycznymi. Proces planowania audytu systemów informatycznych powinien określać zakres przeglądu, wymagany dla otrzymania wiarygodnych, istotnych i przydatnych danych dla skutecznego osiągnięcia celów audytu systemów informatycznych. Audytor systemów informatycznych powinien rozważyć możliwość zapoznania się z raportem końcowym z audytu, programem prowadzenia audytu oraz dokumentacją z badania. Audytor systemów informatycznych powinien również rozważyć, czy konieczne jest dodatkowe testowanie prac innych audytorów i ekspertów.

4. PROWADZENIE PRAC

4.1 Przegląd dokumentacji z badania innych audytorów i ekspertów

4.1.1 W przypadku gdy przegląd dokumentacji z badania innych audytorów i ekspertów jest niezbędny, audytor systemów informatycznych powinien wykonać odpowiednie prace audytowe potwierdzające, że praca innych audytorów i ekspertów była prawidłowo zaplanowana, nadzorowana, udokumentowana i przejrzana, oraz ocenić czy dostarczone przez nich dowody są adekwatne i wystarczające. Zgodność z odpowiednimi standardami zawodowymi powinna również zostać oceniona.

4.2 Przegląd raportów końcowych innych audytorów i ekspertów

4.2.1 Audytor systemów informatycznych powinien dokonać odpowiedniego przeglądu raportów końcowych by potwierdzić, że zakres prac określony w statucie audytora lub w umowie o badanie został spełniony, że główne założenia użyte w ich pracach zostały zidentyfikowane oraz, że ich wnioski i wyniki zostały zaakceptowane przez Zarząd..

4.2.2 Wskazane jest by Zarząd opracował własny raport dotyczący badanych jednostek, będący wyrazem odpowiedzialności za system kontroli wewnętrznej. W tym przypadku audytor systemów informatycznych powinien przeanalizować zarówno raport Zarządu jak i wyniki prac innych audytorów.

4.2.3 Audytor systemów informatycznych powinien dokonać oceny przydatności i adekwatności raportów stworzonych przez innych audytorów i ekspertów oraz przeanalizować istotne kwestie, zidentyfikowane przez innych audytorów i ekspertów. Odpowiedzialność za ocenę efektów prac oraz wniosków i wyników prac innych audytorów i ekspertów, ich wpływu na ogólne cele audytu oraz sprawdzenie, czy wszelka dodatkowa praca do spełnienia tych celów została wykonana, spoczywa na audytorze systemów informatycznych.

5. DZIAŁANIA UZUPEŁNIAJĄCE

5.1 Wdrożenie rekomendacji

5.1.1 W przypadkach gdy będzie to niezbędne, audytor systemów informatycznych powinien rozważyć w jakim stopniu rekomendacje innych audytorów i ekspertów zostały wdrożone przez zarząd.

6. OBOWIĄZYWANIE

6.1 Powyższe wytyczne mają zastosowanie do wszystkich audytów systemów informatycznych rozpoczętych począwszy od 1 czerwca 1998r.

070.010.010 Raportowanie

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami

1.1.1 Standard 070 (Raportowanie) w punkcie 070.010 (Forma i zawartość raportu) stwierdza: „Zadaniem audytora systemów informatycznych jest dostarczenie określonym odbiorcom raportu w odpowiedniej postaci z wykonania prac audytowych. Raport z audytu ma przedstawiać zakres, cele, okres oraz rodzaj i obszar wykonanych prac audytowych. Raport ma wskazywać organizację, planowanych odbiorców raportu oraz wszelkie zastrzeżenia co do jego obiegu. Raport ma przedstawiać wykrycia, wnioski i rekomendacje oraz wszelkie zastrzeżenia lub uwarunkowania audytora względem audytu.”

1.2 Definicje

1.2.1 Przedmiot lub obszar działalności stanowią charakterystyczny temat raportu audytora SI i związanych z nim procedur. Może to obejmować takie sprawy jak budowa lub działanie mechanizmów kontroli wewnętrznej i zgodność z praktykami lub standardami zachowania poufności albo z wymaganiami prawnymi i regulacjami.

1.2.2 Zadanie raportowania poświadczającego (attest reporting engagement) jest zadaniem, w którym audytor SI albo bada twierdzenie kierownictwa na temat określonej sprawy, albo bezpośrednio tę sprawę. Raport audytora SI składa się z opinii na temat jednego z następujących:

- Przedmiotowej sprawy. Te raporty są odnoszą się raczej bezpośrednio do samego przedmiotu niż do opinii o nim. W pewnych okolicznościach kierownictwo nie będzie w stanie wypowiedzieć się na temat przedmiotu prac audytowych. Jako przykład takiej sytuacji może posłużyć outsourcing usług IT do innej organizacji. Kierownictwo zwykle nie będzie w stanie wypowiedzieć się na temat mechanizmów kontrolnych, za które odpowiada inna organizacja. Skutkiem tego audytor SI powinien raczej raportować bezpośrednio o przedmiocie niż o opiniach.
- Opinii kierownictwa na temat skuteczności procedur kontrolnych.
- Zobowiązania raportowania kontroli, gdzie audytor SI wydaje opinię na konkretną przedmiotową sprawę. Te zadania mogą obejmować raporty na temat wdrożonych przez kierownictwo mechanizmów kontrolnych i skuteczności ich działania.

Niniejsza wytyczna jest ukierunkowana na pierwszy typ opinii. Jeśli warunki odniesienia wymagają któregoś z pozostałych typów opinii, wówczas może okazać się potrzebne dostosowanie wymagań raportowania.

1.2.3 Cele kontrolne są celami kierownictwa, które są wykorzystywane jako szkielet do opracowywania i wdrażania mechanizmów kontrolnych (procedur kontrolnych)

1.2.4 Mechanizmy lub procedury kontrolne oznaczają polityki i procedury wdrożone, aby osiągać powiązany cel kontrolny.

1.2.5 Słabość kontroli oznacza wady w konstrukcji lub działaniu procedury kontrolnej. Słabość kontroli potencjalnie może skutkować nie zredukowanymi do akceptowalnego poziomu ryzykami charakterystycznymi dla obszaru działania (ryzyka charakterystyczne, to te które zagrażają osiągnięciu celów związanych z badanym obszarem działalności). Słabość kontroli może być istotna, gdy budowa lub działanie jednej lub więcej procedur kontrolnych nie redukuje, do relatywnie niskiego poziomu, ryzyka pojawienia błędów spowodowanych czynami nielegalnymi lub nieprawidłowościami, które nie będą wykryte przez odpowiednie procedury kontrolne.

1.2.6 Kryteria są standardami lub wzorcami wykorzystywanymi do pomiaru i prezentowania tematu, względem których audytor SI ocenia temat. Kryteria powinny być:

- Obiektywne – Wolne od uprzedzeń,
- Mierzalne – Dostarczające spójnych pomiarów
- Kompletnie – Obejmujące wszystkie powiązane czynniki niezbędne do wyprowadzenia wniosków
- Stosowne – Odnoszące się do tematu

1.2.7 Zadanie raportowania bezpośredniego jest zadaniem, gdzie kierownictwo nie spisuje opinii na temat skuteczności swoich procedur kontrolnych i gdzie audytor SI dostarcza opinii, takiej jak skuteczność procedur kontrolnych, bezpośrednio o przedmiotowej sprawie.

1.2.8 System kontroli wewnętrznej (kontrola wewnętrzna) jest dynamiczny, zintegrowany procesowo, wywiera na niego wpływ ciała nadzorcze, kierownictwo i pozostały personel, i jest zaprojektowany by dostarczać względne zapewnienia odnośnie osiągania następujących celów ogólnych:

- Skuteczność, sprawność i oszczędność działań
- Rzetelność zarządzania
- Zgodność z właściwym prawem, regulacjami i wewnętrznymi politykami

1.2.9 Strategie kierownictwa dla osiągania tych ogólnych celów zależą od budowy i działania następujących komponentów:

- Środowiska kontroli
- Systemów informacyjnych
- Procedur kontrolnych

1.3 Potrzeba wytycznej

1.3.1 Niniejsza wytyczna wskazuje jak audytor SI powinien stosować standardy audytu SI ISACA i COBIT, gdy raportuje na temat mechanizmów kontrolnych systemów informatycznych organizacji i związanych z nimi celów kontrolnych.

2. WPROWADZENIE

2.1 Cel niniejszej wytycznej

2.1.1 Celem niniejszej wytycznej jest wskazanie kierunku audytorom SI mającym zadanie raportować, czy procedury kontrolne dla

określonego obszaru działalności są skuteczne z punktu widzenia każdego z poniższych:

- Kierownictwa organizacji na poziomie nadzorczym i/lub operacyjnym
- Określonych stron trzecich, na przykład regulatora lub innego audytora

2.1.2 Audytor SI może mieć za zadanie raportować na temat skuteczności budowy lub skuteczności operacyjnej.

3. WERYFIKACJA

3.1 Rodzaje usług

3.1.1 Audytor SI może realizować każde z poniższych:

- Audyt (bezpośredni lub pośredni)
- Przegląd (bezpośredni lub pośredni)
- Wykonanie uzgodnionych procedur

3.2 Audyt i przegląd

3.2.1 Audyt dostarcza umiarkowanego zapewnienia na temat skuteczności procedur kontrolnych. Zwykle jest wyrażany jako względne zapewnienie z powodu faktu, że absolutne zapewnienie jest rzadko osiągalne z powodu takich czynników jak konieczność osądu, wykorzystanie testowania, wbudowane ograniczenia kontroli wewnętrznej oraz, że większość dowodów dostępnych audytorowi SI jest w swej naturze raczej przekonująca niż rozstrzygająca.

3.2.2 Przegląd dostarcza umiarkowanego zapewnienia na temat skuteczności procedur kontrolnych. Dostarczany poziom zapewnienia jest mniejszy niż w przypadku audytu, ponieważ zakres prac jest mniej rozległy, a natura, czas trwania i obszar wykonywanych procedur nie zapewniają wystarczających dowodów audytowych, by umożliwić audytorowi wyrażenie pozytywnej opinii. Celem przeglądu jest umożliwienie audytorowi wyrażenia, czy, na podstawie procedur, coś zwróciło uwagę audytora SI, co pozwala audytorowi SI wierzyć, że w oparciu o określone kryteria procedury kontrolne nie były skuteczne (wyrażenie negatywnego zapewnienia).

3.2.3 Zarówno audyty jak i przeglądy pociągają za sobą:

- Planowanie zadania
- Ocenę skuteczności budowy procedur kontrolnych
- Testowanie skuteczności operacyjnej procedur kontrolnych (natura, okres i obszar testowania będą się różniły pomiędzy audytami i przeglądami)
- Formułowanie wniosków o, oraz raportowanie, skuteczności budowy i operacyjnej procedur kontrolnych w oparciu o następujące kryteria:
 - Wniosek z audytu jest wyrażony jako pozytywne wyrażenie opinii i dostarcza wysokiego poziomu zapewnienia.
 - Wniosek z przeglądu jest wyrażony jako oświadczenie negatywnego zapewnienia i dostarcza jedynie umiarkowanego poziomu zapewnienia.

3.3 Uzgodnione procedury

3.3.1 Zadanie wykonania uzgodnionych procedur nie skutkuje wyrażeniem przez audytora SI jakiegokolwiek zapewnienia. Audytor SI ma za zadanie wykonać określone procedury by zaspokoić potrzebę informacji tych stron, które uzgodniły wykonanie procedur. Audytor SI wydaje stronom, które uzgodniły procedury raport spostrzeżeń opartych na faktach. Odbiorcy wyciągają swoje własne wnioski z tego raportu, ponieważ audytor SI nie określał natury, czasu i obszaru procedur i nie jest w stanie wyrazić jakiegokolwiek zapewnienia. Raport jest ograniczony do tych stron (na przykład ciała regulującego), które uzgodniły procedury do wykonania, podczas gdy inie nie są świadome powodów realizacji procedur i mogą źle interpretować ich rezultaty.

3.4 Raportowanie uzgodnionych procedur

3.4.1 Raport z wykonania uzgodnionych procedur powinien posiadać formę procedur i spostrzeżeń. Raport powinien zawierać następujące elementy:

- Tytuł, który zawiera słowo „niezależny”
- Identyfikację określonych stron
- Identyfikację tematu (lub jego pisemne wyrażenie) i typu zadania
- Identyfikację odpowiedzialnych stron
- Oświadczenie, że temat jest w zakresie obowiązków strony odpowiedzialnej
- Oświadczenie, że wykonywane procedury są tymi, które zostały uzgodnione przez strony zidentyfikowane w raporcie
- Oświadczenie, że dostateczność procedur stanowi wyłączną odpowiedzialność określonych stron oraz zastrzeżenie o ograniczeniu odpowiedzialności za dostateczność tych procedur
- Listę wykonanych procedur (lub odnośnik do niej) i powiązanych spostrzeżeń
- Oświadczenie, że audytor SI nie miał za zadanie przeprowadzić badania tematu i nie wykonał tego
- Jeżeli audytor SI wykonał dodatkowe procedury, to oświadczenie, że inne tematy mogły zwrócić uwagę audytora i mogą być zaraportowane
- Oświadczenie o ograniczeniu wykorzystania raportu, ponieważ zamierzonym jest jego używanie wyłącznie przez określone strony

3.5 Mandat zadaniowy

3.5.1 W przypadku, gdy zadanie audytowe jest podejmowane by spełnić wymagania regulatora lub podobne, narzucone wymagania, ważnym jest, aby audytor SI był zapewniony, że typ zadania jest czysty z punktu widzenia odpowiedniej legislacji lub innych źródeł dających mandat audytowy. Jeżeli występują wątpliwości (brak przewidywalności), zaleca się audytorowi SI i/lub mianowanej grupie skomunikować z odpowiednim regulatorem lub inną stroną odpowiedzialną za ustanawianie lub regulowanie wymagania i wyrażanie zgody na typ zadania i dostarczany typ zapewnienia.

3.5.2 Audytor S, który przed zakończeniem zadania jest proszony o zmianę zadania z audytu na przegląd lub wykonanie uzgodnionych procedur powinien rozważyć stosowność wykonania tego i nie może się zgodzić na taką zmianę, jeżeli nie ma

przekonyującego uzasadnienia dla zmiany. Przykładowo zmiana nie jest odpowiednia dla uniknięcia modyfikacji raportu.

4. OPINIA AUDYTU SI

4.1 Ograniczenia

4.1.1 Opinia audytora SI jest oparta na procedurach określonych jako niezbędne do zebrania dostatecznych i stosownych dowodów, które powinny być w swojej naturze raczej przekonujące niż rozstrzygające. Zapewnienie audytora SI na temat skuteczności mechanizmów kontroli wewnętrznej jest jednakże ograniczone ze względu na charakter mechanizmów kontrolnych i wbudowanych ograniczeń każdego zbioru mechanizmów kontroli wewnętrznej i ich działania. Te ograniczenia obejmują:

- Ogólnie przyjęte wymaganie kierownictwa, że koszty mechanizmów kontroli wewnętrznej nie przekraczają oczekiwanych korzyści
- Większość mechanizmów kontroli wewnętrznej ma tendencję do ukierunkowania raczej na rutynowe niż nierutynowe transakcje/zdarzenia
- Potencjalne błędy ludzkie wynikłe z niedbałości, roztargnienia lub zmęczenia, niezrozumienia instrukcji i pomyłek w osądzie
- Prawdopodobieństwo omijania mechanizmów kontroli wewnętrznej w ramach porozumienia pracownika z innym pracownikiem lub stronami spoza organizacji
- Prawdopodobieństwo, że osoba odpowiedzialna za sprawowanie kontroli wewnętrznej może nadużyć swych obowiązków, np. członek kierownictwa obchodzi procedurę kontrolną
- Prawdopodobieństwo, że kierownictwo może nie być poddawane tym samym mechanizmom kontroli wewnętrznej, które są stosowane wobec innego personelu
- Prawdopodobieństwo, że mechanizmy kontroli wewnętrznej mogą stać się nieodpowiednie z powodu zmian warunków, wówczas zgodność z procedurami może pogarszać działanie

4.1.2 Systemy zwyczajów, kultury i ładu (korporacyjnego i IT) mogą powstrzymywać nieprawidłowości popełniane przez kierownictwo, ale nie w sposób całkowicie niezawodny. Skuteczne środowisko kontrolne może pomóc zmniejszyć prawdopodobieństwo takich nieprawidłowości. Czynniki środowiska kontrolnego, takie jak skuteczne ciało nadzorcze, komitet audytowy, i instytucjonalna kontrola wewnętrzna mogą ograniczać niewłaściwe zachowanie kierownictwa. Alternatywnie, nieskuteczne środowisko kontrolne może negować skuteczność procedur kontrolnych wewnątrz struktury kontroli wewnętrznej. Dla przykładu, chociaż organizacja ma odpowiednie procedury kontrolne dotyczące zgodności z regulacjami środowiskowymi, kierownictwo może mieć silną skłonność zatajenia każdej wykrytej niezgodności, która mogłoby wpływać niekorzystnie na publiczny odbiór organizacji. Skuteczność lub stosowność mechanizmów kontroli wewnętrznej może znajdować się także pod wpływem takich czynników jak zmiana własności lub kontroli, zmiany w kierownictwie lub innym personelu albo postępy na rynku lub w przemyśle, do którego należy organizacja.

4.2 Zdarzenia wynikłe

4.2.1 Czasami mają miejsce zdarzenia, późniejsze od czasu lub okresu czasu badanego tematu, ale powstałe przed datą wydania raportu audytora SI, które mają poważny wpływ na temat i dlatego wymagają dopasowania lub ujawnienia w prezentacji tematu lub zapewnieniu. Takie zdarzenia nazywane są zdarzeniami wynikłymi. Wykonując zadanie poświadczające, audytor SI powinien rozważyć informacje o zdarzeniach wynikłych, które zwróciły jego uwagę.

Jednakże, audytor SI nie ma obowiązku wykrywania takich zdarzeń.

4.2.2 Audytor SI powinien zasięgnąć u kierownictwa informacji na temat, czy są świadomi jakichkolwiek zdarzeń wynikłych do daty raportu audytora SI, które mogłyby mieć poważny wpływ na przedmiotową sprawę lub zapewnienie.

4.3 Wnioski i raportowanie

4.3.1 Audytor SI powinien w oparciu o określone kryteria przejrzeć i ocenić wnioski wyciągnięte z pozyskanych dowodów stanowiących podstawę formułowania opinii na temat skuteczności procedur kontrolnych.

4.3.2 Raport audytora SI na temat skuteczności procedur kontrolnych powinien zawierać następujące:

- Tytuł
- Adresatów
- Opis zakresu audytu, włączając w to:
 - Identyfikację lub opis obszaru działalności
 - Kryteria wykorzystane jako podstawa dla wniosków audytora SI
 - Stwierdzenie, że utrzymanie skutecznej struktury kontroli wewnętrznej, włączając w to procedury dla przedmiotowego obszaru działalności jest obowiązkiem kierownictwa
- Jeżeli zadanie jest zadaniem poświadczającym, stwierdzenie identyfikujące źródło twierdzeń kierownictwa o skuteczności procedur kontrolnych
- Stwierdzenie, że audytor SI wykonał zadanie, by wyrazić opinię na temat skuteczności procedur kontrolnych
- Określenie celu dla którego został przygotowany raport audytora SI i upoważnionych do posługiwania się nim oraz zastrzeżenie odpowiedzialności za wykorzystanie go do jakiegokolwiek innego celu lub przez jakąkolwiek inną osobę
- Opis kryteriów lub ujawnienie źródła kryteriów
- Stwierdzenie, że audyt został wykonany zgodnie ze ISACA-owskimi standardami audytu SI lub innymi właściwymi standardami zawodowymi
- Dalsze szczegółowe wyjaśnienia na temat czynników wpływających na dostarczane zapewnienie oraz, w razie potrzeby, inne informacje
- W razie potrzeby, oddzielny raport powinien zawierać rekomendacje działań korygujących i zawierać odpowiedź kierownictwa

- Paragraf stwierdzający, że ze względu na wbudowane ograniczenia każdej kontroli wewnętrznej, mogą wystąpić i nie być wykryte nieprawidłowości wynikające z błędów lub oszustw. Dodatkowo, paragraf powinien stwierdzać, że rzutowanie jakiegokolwiek oceny mechanizmów kontrolnych na sprawozdania finansowe przyszłych okresów jest narażone na ryzyko, że kontrola wewnętrzna może stać się nieadekwatna z powodu zmian w warunkach, lub z powodu pogorszenia poziomu zgodności z politykami lub procedurami
 - Audyt nie jest przeznaczony do wykrywania wszystkich słabości w procedurach kontrolnych i nie jest wykonywany w sposób ciągły w danym przedziale czasu, a testy wykonane na procedurach kontrolnych oparte są na próbach
 - Kiedy opinia audytora SI jest z zastrzeżeniami wówczas powinien być zawarty paragraf określający zastrzeżenia
 - Wyrażenie opinii, czy, we wszystkich istotnych aspektach, budowa i działanie procedur kontrolnych w odniesieniu do obszaru działalności były skuteczne
 - Podpis audytora SI
 - Adres audytora SI
 - Datę raportu audytora SI. W większości przypadków, datowanie raportu opiera się na stosownych standardach zawodowych. W pozostałych przypadkach, data raportu powinna być oparta na wnioskach z pracy w terenie.
- 4.3.3** W zadaniu raportowania bezpośredniego, audytor SI raportuje raczej bezpośrednio o przedmiotowej sprawie niż o twierdzeniach na jej temat. Raport powinien odnosić się jedynie do tematu zadania i nie powinien zawierać jakichkolwiek odniesień do twierdzeń kierownictwa na przedmiotową sprawę.
- 4.3.4** Jeżeli audytor SI podejmuje się zadania przeglądu, wówczas raport wskazuje, że wnioski audytora SI odnoszą się do skuteczności budowy i działania oraz, że praca audytora w odniesieniu do skuteczności operacyjnej była ograniczona głównie do pytań, inspekcji, obserwacji i minimalnych testów działania mechanizmów kontroli wewnętrznej. Raport zawiera stwierdzenie, że nie wykonano audytu, że podjęte procedury dają mniejszą pewność niż audyt i w związku z tym nie wyrażono opinii audytowej. Wyrażenie negatywnego zapewnienia oznacza, że nic nie zwróciło uwagi co powoduje, że audytor SI wierzy, że organizacyjne procedury kontroli były, we wszystkich istotnych kwestiach, nieskuteczne w odniesieniu do obszaru działalności, w oparciu o określone kryteria.
- 4.3.5** Podczas przebiegu zadania audytor SI może stać się świadomym słabości kontroli. Audytor SI powinien terminowo raportować odpowiedniemu poziomowi kierownictwa każdą zidentyfikowaną słabość kontroli. Procedury związane z zadaniem są zaprojektowane do zbierania wystarczająco odpowiednich dowodów by sformułować wnioski zgodnie z warunkami zadania. W przypadku braku specjalnych wymagań w warunkach zadania, audytor SI nie ma obowiązku konstruować procedur do zidentyfikowania rzeczy, które mogą być odpowiednie do raportowania kierownictwu.

5. OBOWIĄZYWANIE

5.1 Niniejsza wytyczna obowiązuje wszystkie audyty systemów informatycznych rozpoczęte począwszy od 1 stycznia 2003 roku.

Procedury audytowania SI

Procedura 1 Ocena ryzyka IS

1. INFORMACJE OGÓLNE

1.1 Powiązanie ze standardami I wytycznymi

- 1.1.1 Standard 050.010 – planowanie audytu: „audytor systemów informatycznych **ma (proponuję: „powinien”)** tak planować prace audytu informatycznego aby sprostać obowiązującym standardom i zrealizować określone cele audytu”.
- 1.1.2 Standard 060.020 – dowody: „podczas przeprowadzania audytu, audytor systemów informatycznych jest zobowiązany do tego, aby uzyskać wystarczające, wiarygodne i odpowiednie dowody, aby w efektywny sposób osiągnąć cel audytu. Konkluzje i wyniki audytu powinny być wsparte przez odpowiednie analizy i interpretacje zidentyfikowanych dowodów.
- 1.1.3 Wytyczna 050.010.030 – ocena ryzyka podczas planowania audytu.

1.2 Potrzeba procedury

- 1.2.1 Procedura została zaprojektowana w celu zapewnienia:
 - Definicji oceny ryzyka audytu IS
 - Wskazówek dla audytu wewnętrznego w jaki sposób używać metodologii oceny ryzyka audytu IS
 - Wskazówek na temat wyboru kryteriów rangowania ryzyka oraz stosowania wag.

2. Ryzyko IS

- 2.1.1 Ryzyko to możliwość wystąpienia zdarzenia lub działania, które będzie miało niepożądany wpływ na daną organizację i jej systemy informatyczne. **Ryzykiem może również być możliwość, że dane zagrożenie z powodu słabości aktywa czy grupy aktywów spowoduje stratę lub uszkodzenie (zniszczenie) aktywów.** To jest w sposób prosty mierzony poprzez połączenie wpływu zdarzenia i prawdopodobieństwa jego wystąpienia.
- 2.1.2 Ryzyko wewnętrzne odnosi się do ryzyka wystąpienia zdarzenia w przypadku braku odpowiednich mechanizmów kontrolnych.
- 2.1.3 Ryzyko pozostałe odnosi się do ryzyka wystąpienia zdarzenia w przypadku gdy istnieją odpowiednie mechanizmy kontrolne redukujące wpływ lub prawdopodobieństwo wystąpienia zdarzenia.

3. OCENA RYZYKA IS

- 3.1 **Ocena ryzyka to proces identyfikacji i szacowania ryzyk i ich potencjalnych skutków.**

4. METODOLOGIA OCENY RYZYKA IS

- 4.1.1 Ocena ryzyka IS to metodologia służąca budowie modelu ryzyka w celu optymalizowania przydzielania (wykorzystania) zasobów audytu IS poprzez dogłębne zrozumienie środowiska IS organizacji i ryzyk związanych z każdą **audytowalną jednostką**. Patrz pkt. 9 – **jednostka audytowalna**.
- 4.1.2 Celem modelu ryzyka jest optymalizowanie przydziału zasobów audytu IS poprzez dogłębne zrozumienie **zbioru audytowalnych jednostek (audit universe)** i ryzyk związanych z każdym jego elementem.

5. PODEJŚCIE DO AUDYTU IS OPARTE NA RYZYKU

- 5.1.1** Coraz więcej organizacji przechodzi do audytu opartego na analizie ryzyka, który może być stosowany do rozwijania i poprawy procesu audytu. To podejście jest stosowane do oceny ryzyka oraz wspiera audytora IS w procesie decyzyjnym odnośnie stosowania odpowiednio testów zgodności lub testów istotności. W podejściu do audytu bazującym na ryzyku audytorzy IS nie opierają się wyłącznie na ryzyku. Również polegają na kontrolach wewnętrznych i operacyjnych oraz znajomości organizacji. Taki rodzaj oceny ryzyka pozwala na praktyczne wybory poprzez powiązanie analizy kosztów/korzyści wynikających z kontroli z rozpoznanymi ryzykami.
- 5.1.2** Poprzez zrozumienie prowadzonej działalności, audytor IS może zidentyfikować i skategoryzować rodzaje ryzyka, które będą lepiej określały model ryzyka i podejście stosowane w trakcie wykonywania przeglądu. Model oceny ryzyka może być prosty i sprowadzać się do stworzenia wag dla różnych rodzajów ryzyka związanego z prowadzoną działalnością i **opisywać ryzyko w formie równania. (and identifying risk in an equation)**. Z drugiej strony ocena ryzyka może być projektem, w którym ryzyku przyporządkowano złożone wagi bazujące na znajomości prowadzonej działalności lub istotności konsekwencji.
- 5.1.3** Audytor IS interesuje się niekontrolowanymi ryzykami i krytycznymi kontrolami. Tak więc, w podejściu do audytu opartym o ryzyko audytor IS będzie zainteresowany systemami bazującymi na technologii, które zapewniają kontrolę dla funkcji biznesowych o wysokim ryzyku własnym i funkcjach bazujących na technologii, w których ryzyko pozostałe jest większe niż akceptowalne.
- 5.1.4** Zdefiniowanie **zbioru audytowalnych jednostek** jest warunkiem wstępnym do rangowania ryzyka. Określanie **zbioru audytowalnych jednostek** będzie bazowało na znajomości strategicznych planów organizacji w zakresie IS, operacji, przeglądzie regulaminów organizacyjnych, opisów stanowisk i zakresów czynności wszystkich jednostek zależnych i przedyskutowania z odpowiedzialną kadrami kierowniczą.
- 5.1.5** Cykle planowania audytu są skorelowane z cyklami planowania biznesowego. Często wybierany jest roczny cykl planowania, w oparciu o rok kalendarzowy lub inny dwunastomiesięczny okres. Niektóre organizacje planują w cyklach innych niż dwunastomiesięczne, np. na sześć czy osiemnaście miesięcy. Niektóre organizacje zamiast sztywnego okresu planowania wolą **planowanie kroczące (rolling planning cycles)** na ustalony okres do przodu. Dla spójności w tej procedurze zakładamy roczny cykl planowania audytu.
- 5.1.6** Jednym z najważniejszych problemów przed jakim stoi kierownictwo audytu IS jest dobór zagadnień (projektów) które będą uwzględnione w planie audytu. Proces planowania audytu daje możliwość skwantyfikowania i ocenienia zasobów audytu IS niezbędnych do realizacji rocznego planu audytu. Błędy w wyborze zagadnień skutkują niewykorzystaniem możliwości w zakresie wzmocnienia kontroli i **wydajności (efficiency)** operacyjnej.
- 5.1.7** U podstaw planu audytu IS leży założenie, że ocena planowanych przeglądów/projektów audytu będzie bardziej **skuteczna (effective)** jeżeli przestrzegany jest formalny proces zbierania informacji koniecznych do dokonania wyboru przeglądów/projektów. Podejścia opisane w tym dokumencie są podstawowymi ramami, w których stosuje się zasady zdrowego rozsądku i profesjonalnego osądu.
- 5.1.8** Prezentowana metodologia jest bardzo prosta. Pomimo tego w większości przypadków powinna być wystarczająca do osiągnięcia rozsądnych, rozsądnych i możliwych do obrony decyzji wyboru przeglądów/projektów audytowych. Ramy przeprowadzenia analizy ryzyka i przygotowania priorytetów przeglądów/projektów zostały zaprezentowane w niniejszej procedurze.
- 5.1.9** Ocena ryzyka w tym ujęciu jest techniką wykorzystywaną do zweryfikowania **jednostek audytowalnych** oraz wyboru przeglądów/projektów, które mają największą ekspozycję na ryzyko. Zastosowanie oceny ryzyka do wyboru audytu /projektów jest ważne ponieważ jest środkiem pozwalającym w rozsądny sposób zapewnić, że zasoby audytu IS są wykorzystane w optymalny sposób, tzn. że plan audytu IS alokuje zasoby w sposób, który powinien przynieść największe efekty. **To this end**, ocena ryzyka zapewnia jasne kryteria do systematycznego wyboru projektów audytu. Plan audytu IS jest często dołączony do planu audytu finansowego i operacyjnego w celu uszczegółowienia pełnego planowanego zakresu audytu IS.

6. TECHNIKI OCENY RYZYKA IS

- 6.1.1** Określając, które obszary funkcjonalne powinny zostać poddane audytowi, audytor IS może spotkać się z całą różnorodnością przedmiotów audytu. Jeśli to możliwe wszystkie obszary IS organizacji powinny zostać ujęte w procesie oceny ryzyka. Niektóre organizacje oceniają tylko projekty IT. Inne oceniają każdy obszar/system, który może podlegać audytowi IS. Każde z powyższych podejść może reprezentować różne rodzaje ryzyka audytowego. Audytor IS powinien oszacować te różne ryzyka w celu zdecydowania, które obszary są obszarami wysokiego ryzyka i stąd powinny być audytowane. Celem tego procesu jest:
- Zidentyfikowanie obszarów w których ryzyko pozostałe jest nieakceptowalnie wysokie
 - Zidentyfikowanie krytycznych systemów kontrolnych, które zabezpieczają wysokie ryzyko własne
 - Oszacowanie niepewności istniejącej w stosunku do krytycznych systemów kontrolnych.
- 6.1.2** Wykorzystywanie oceny ryzyka do określania obszarów IS, które powinny zostać poddane audytowi:
- Umożliwienie kierownictwu efektywnej alokacji ograniczonych zasobów audytu IS
 - Dostarczenie rozsądnego zapewnienia, że uzyskano odpowiednie informacje od wszystkich szczebli zarządzania włącznie z zarządem i kierownictwem jednostek funkcjonalnych. Ogólnie rzecz biorąc informacje obejmują zagadnienia, które pomogą kierownictwu w efektywnym wykonaniu obowiązków i dostarczą rozsądnego zapewnienia, że działalność audytu IS jest nakierowana na obszary wysokiego ryzyka biznesowego i będzie wносить wartość dodaną dla kierownictwa.
 - Stanowi bazę do efektywnego zarządzania funkcją audytu IS.
 - Daje podsumowanie jak poszczególne przeglądane obszary są powiązane z całą organizacją oraz z planami biznesowymi.

7. METODY OCENY RYZYKA IS

- 7.1.1** Obecnie stosowanych jest kilka metod przeprowadzania oceny ryzyka IS. Jednym z podejść jest system punktowy użyteczny przy ustalaniu priorytetów audytów IS na podstawie szacowania czynników ryzyka z uwzględnieniem takich zmiennych jak techniczna złożoność, zakres zmian systemów i procesów oraz istotność. Te zmienne mogą być ważone. Wartości ryzyka są następnie porównane wzajemnie i na tej podstawie w prosty sposób przygotowany jest plan audytu. Często plan audytu IS jest zatwierdzany przez Komitet Audytu i/lub Prezesa Zarządu. Przeglądy są następnie harmonogramowane zgodnie z planem audytu IS. Inną formą oceny ryzyka jest osąd. Zakłada podjęcie niezależnej decyzji na podstawie wytycznych kierownictwa (członków zarządu), danych historycznych i podejścia biznesowego.

8. ZBIERANIE DANYCH

- 8.1.1** Informacje opisujące wszystkie aspekty operacji organizacji zostaną wykorzystane do zdefiniowania różnych **audytowalnych jednostek** i do modelowania ryzyka własnego operacji danej jednostki. Źródła danych obejmują:
- Wywiady z kierownictwem wyższego szczebla przeprowadzane w celu zebrania danych na potrzeby modelu ryzyka IS
 - Odpowiedzi na ankietę zawierającą zestrukturyzowaną listę pytań, wysłaną do kierownictwa w celu ułatwienia zbierania danych do modelu ryzyka IS
 - Ostatnie raporty z przeglądów
 - Plan strategiczny IT
 - Użytecznym źródłem informacji może być proces budżetowania
 - Problemy podniesione przez audytorów zewnętrznych
 - Wiedza audytu IS i świadomość istotnych problemów zebranych z wszystkich innych źródeł
 - Specyficzne metody wykorzystywane do zbierania danych pod warunkiem że będą efektywne uwzględniając czas i zasoby dostępne do realizacji tego zadania.

9. AUDYTOWALNE JEDNOSTKI IS

- 9.1.1** Model jest pomyślany w ten sposób by zawierał i dostarczał ocenę ryzyka dla każdej **audytowalnej** pod względem IS jednostki w organizacji (**ze zbioru audytowalnych jednostek**). **Audytoralna jednostka** może być zdefiniowana jako każda samodzielna część organizacji i jej systemów. Nie ma specyficznych zasad określających lub różnicujących poszczególne **audytowalne jednostki**. Niemniej poniżej są wytyczne do zastosowania w tym modelu ryzyka audytu dla każdej jednostki/tematu/funkcji:
- Możliwe do zaudytowania w rozsądnych ramach czasowych
 - System - tj. ma określone wejścia, procesy, wyjścia i wynik
 - Oddzielne tj. możliwe do zaudytowania w sposób minimalnie powiązany z innymi systemami (to może być trudne jeśli audytowana aplikacja ma wiele interfejsów z innymi systemami)

10. PRZYKŁADY

- 10.1** Jest wiele różnych metod przeprowadzania oceny ryzyka IS. Punkty 11 do 14 opisują kilka rodzajów oceny ryzyka IS.

11. PRZYKŁAD I

- 11.1** **PRZYKŁAD I** prezentuje ocenę ryzyka IS z ośmioma **kluczowymi zmiennymi**. Każda jednostka/obszar w zbiorze audytowalnych jednostek IS (IS audit universe) będzie oceniana na podstawie tych ośmiu zmiennych z wykorzystaniem liczbowych wartości ryzyka z przedziału od 1 (niski) do 5 (wysoki). **Wyniki tego rankingu są następnie mnożone przez wagi z przedziału od 1 (niski) do 10 (wysoki) dając wartość zwiększoną**. Przykładowe wagi są zawarte w przykładzie I. **Zwiększone wartości dodaje się do siebie by uzyskać wartość łączną**. Kiedy mamy wartości łączne dla każdej **audytowalnej jednostki/obszaru**, **audytowalne jednostki/obszary** są szeregowane wg ryzyka. Na podstawie tego rankingu budowana jest struktura rocznego planu audytu. **Osiem kluczowych zmiennych jest wyspecyfikowanych w punktach od 11.1.1 do 11.1.3 wraz z krótkim objaśnieniem każdej z nich**.

11.1.1 Miary wpływu

- **Charakter działalności**—krytyczność czynności i części organizacji, która wykorzystuje daną czynność. Rzadkie lub niezwykle czynności lub projekty mogą z większym prawdopodobieństwem skutkować błędami lub **nieefektywnością (inefficiency)** i w większym stopniu podlegają zainteresowaniu audytu.
- **Zabezpieczenie powrotu (Fall back arrangements)**—ten czynnik odnosi się do działań które zostały przewidziane w celu kontynuowania działalności na wypadek gdy nowy system ma problemy. Czynniki, które należy uwzględnić to plany kontynuacji działalności, plany przywracania działalności po katastrofie, procedury pracy ręcznej i stary system.

Ogólnie rzecz ujmując, jeżeli powyższe kwestie zostały rozważone, rozwiązania są osiągalne **lub** (w oryginale jest „or” co nie ma dla mnie za bardzo sensu, wg mnie powinno być „i”) efektywne kosztowo to ryzyko jest najmniejsze.

- **Wrażliwość funkcji dla kierownictwa wyższego szczebla**—ten czynnik odnosi się do tego jak ważna jest dana jednostka, funkcja lub obszar dla kierownictwa wyższego szczebla.
- **Istotność**—to koncepcja dotycząca ważności przedmiotu lub informacji z punktu widzenia wpływu na funkcjonowanie organizacji. Wyrażenie względnych konsekwencji lub ważności konkretnej sprawy w kontekście organizacji jako całości.

11.1.2 Miary prawdopodobieństwa

- **Zakres zmian systemów lub procesów**—Dynamiczne środowisko w kontekście zmian systemów lub procesów zwiększa prawdopodobieństwo błędów i w konsekwencji zwiększa zainteresowanie audytu. Może mieć miejsce znacząca ilość reinżynierii procesów. Zmiany systemów lub procesów zwykle okazują się przynosić korzyści w długim okresie czasu lecz często w krótkim okresie mają odmienne skutki, które wymagają zwiększonej uwagi audytu.
- **Złożoność**—Ten czynnik ryzyka odzwierciedla możliwość zaistnienia błędów lub oszustw niewykrytych ze względu na skomplikowane środowisko. Ocena złożoności zależy od wielu czynników. Zakresu automatyzacji, złożoności obliczeń, powiązanych i współzależnych działań, ilości produktów lub usług, **okresu czasu na jaki prognozujemy (the time spans of estimates)**, zależności od stron trzecich, popytu klientów, czasu przetwarzania, odpowiednich przepisów prawa i regulacji, i wielu innych czynników, z których niektóre są nierozpoznane, mających wpływ na osąd na temat złożoności określonego audytu.
- **Zarządzanie projektami**—oceniając zarządzanie projektami powinno się rozważyć:
 - Czy projekty są robione wewnętrznie czy przez firmy zewnętrzne
 - Strukturę projektu
 - Umiejętności personelu
 - Ramy czasowe projektu

Ogólnie mówiąc ryzyko jest dzielone jeśli projekt jest outsourcowany.

11.1.3 Miary niepewności w odniesieniu do kontroli

- **Okres od ostatniego przeglądu**—Jeśli czas od ostatniego przeglądu się wydłuża wartość nowego przeglądu prawdopodobnie rośnie. Najkorzystniejsze efekty nowego przeglądu są bezpośrednio przed lub po wdrożeniu systemu.

PRZYKŁAD I—OCENA RYZYKA IS

KLUCZOWE ZMIENNE	LICZBOWA WARTOŚĆ RYZYKA 1 (niska) to 5 (wysoka)	WAGA KONSEKWENCJI 1 (niskie) to 10 (wysokie)	WARTOŚĆ ZWIĘKSZO NA
1. Charakter działalności	Rozważyć: Działalność podstawowa = 4 to 5 Jednostka biznesowa = 2 to 3 System lokalny = 1	8*	
2. Przygotowanie do powrotu	Rozważyć: Plany kontynuowania działalności Plany przywracania działalności po katastrofie Stary system	5*	
Wrażliwość funkcji dla kierownictwa wyższego szczebla	Duże zainteresowanie = 4 to 5 Umiarkowane zainteresowanie = 2 to 3 Małe zainteresowanie = 1	6*	
4. Istotność	Wartość generowanych wydatków lub przychodów lub konsumowanych zasobów Budżet projektu >\$500,000 = 4 to 5 Budżet projektu \$100,000 to \$500,000 = 2 to 3 Budżet projektu <\$100,000 = 1 Przychody/wydatki >\$500,000 = 4 to 5 Przychody/wydatki \$100,000 to \$500,000 = 2 to 3 Przychody/wydatki <\$100,000 = 1	5*	
5. Zakres zmian systemów, procedur i procesów	Rozważyć: Zakres reinżynierii. Duża reinżynieria = 4 do 5 Umiarkowana reinżynieria = 2 do 3 Mała reinżynieria = 1 lub Brak procedur = 4 lub 5 Lokalne procedury = 3 lub 2 Korporacyjne procedury = 1	8*	
6. Złożoność	Rozważyć: Wolumen transakcji Ilość użytkowników Scentralizowane lub zdecentralizowane Ilość interfejsów Bardzo złożone = 4 to 5 Umiarkowanie złożone = 2 to 3 Proste = 1	7*	
7. Zarządzanie projektami	Rozważyć: Projektanci wewnętrzni lub zewnętrzni Struktura projektu Umiejętności personelu Ramy czasowe projektu	7*	
8. Okres od ostatniego przeglądu	Ocena 5 wskazuje okres 5 lat lub więcej od ostatniego audytu lub że nigdy audytu nie było	1*	
	Razem		

* Zastosowano przykładowe wagi konsekwencji

12. PRZYKŁAD II

- 12.1** Przykład II rozszerza ocenę ryzyka IS wykorzystaną w przykładzie I poprzez włączenie ryzyka biznesowego jak również ośmiu kluczowych zmiennych audytu IS użytych w przykładzie I. **Czynnik rangowania ryzyka audytu IS (z przykładu I) jest pomnożony przez ryzyko biznesowe w tym przykładzie. Czynniki ryzyka biznesowego (finansowe, strategiczne, operacyjne i zgodności prawnej) są rozważone pod względem ich ważności (odpowiedniości) dla każdej audytowalnej jednostki/obszaru.**
- 12.2** Każda jednostka/obszar w zbiorze audytowalnych jednostek/obszarów IS będzie oceniona pod względem tych ośmiu kluczowych zmiennych z zastosowaniem oceny liczbowej od 1 (niski) do 5 (wysoki). Wyniki tej oceny są następnie przemnożone przez **czynnik ważący konsekwencje**, z zakresu od 1 (niskie) do 10 (wysokie) jak w przykładzie I. Te rozszerzone wartości dodane do siebie dają sumę (stosuje się **wagi konsekwencji** użyte w przykładzie I) Ta suma jest wskaźnikiem ryzyka audytu IS.
- 12.3** Cztery czynniki ryzyka biznesowego są zdefiniowane poniżej.
- **Ryzyko finansowe**—ponieważ większość systemów ma pewien potencjalny wpływ na wyniki finansowe organizacji , poziom i prawdopodobieństwo takiego wpływu powinno zostać rozważone. Jeżeli przewidywany efekt nie jest bezpośredni i relatywnie mały w porównaniu do innych wpływów i celów systemu i/lub w porównaniu z innymi audytowalnymi obszarami/systemami wtedy prawdopodobnie wycenimy wskaźnik ryzyka finansowego na 0 raczej niż na 1.
 - **Ryzyko strategiczne** —system może mieć bezpośredni, strategiczny wpływ na organizację. Oczekuje się , że te czynniki ryzyka wskazane przez kierownictwo wyższego szczebla zostaną ocenione na 1
 - **Ryzyko operacyjne** —ryzyko operacyjne zostanie z większym prawdopodobieństwem ocenione na 1 niż inne ryzyka biznesowe ponieważ większość systemów jest zaprojektowanych w ten sposób, że wpływają na sposób i **skuteczność (effectiveness)** z jaką organizacje prowadzą swoją codzienna działalność
 - **Zgodność z prawem** —Systemy mogą mieć bezpośredni wpływ na stopień w jakim organizacje spełniają wymogi prawne .
- 12.4** **Wstaw cyfrę 1 (ważne, odpowiednie) lub 0 (nieistotne) dla każdego czynnika ryzyka biznesowego. Następnie pomnóż każdy wynik przez odpowiednią wagę i zsumuj by uzyskać sumaryczny wskaźnik ryzyka biznesowego dla każdego tematu.**
- 12.5** **Przypisując punkty rozważ trzy poniższe kwestie:**
- Jaki jest przewidywany **cel** systemu, który ma być audytowany?
 - Jaki jest przewidywany zakres i cel audytu?
 - Czy system w sposób bezpośredni wpływa na wyniki finansowe/strategiczne/operacyjne lub zgodność z prawem? Np. Jeżeli system nie działa zgodnie z oczekiwaniami czy jest prawdopodobnym, że organizacja poniesie straty finansowe, doświadczy niekorzystnych efektów strategicznych, będzie miała problemy operacyjne lub naruszy odpowiednie wymogi prawne.?
- 12.6** **Ostatnim krokiem w tym przykładzie jest pomnożenie oceny ryzyka audytu (audit risk ranking factor) przez czynnik ryzyka biznesowego by otrzymać łączną ocenę ryzyka . Patrz przykład w tabeli poniżej.. Kiedy mamy łączną ocenę ryzyka (total risk rankings) dla każdej audytowalnej jednostki/obszaru otrzymujemy jednostki/obszary zręgowane wg ryzyka. Na podstawie tego rankingu jest budowana struktura rocznego planu audytu IS.**

PRZYKŁAD II—OCENA RYZYKA IS Z UWZGLĘDNIENIEM CZYNNIKÓW RYZYKA BIZNESOWEGO

JEDNOSTKA AUDYTO-WALNA	OCENA RYZYKA AUDYTU (z przykładu I)	CZYNNIK RYZYKA BIZNESOWEGO (0 lub 1)				CZYNNIK RYZYKA BIZNESOWEGO	ŁĄCZNA OCENA RYZYKA
		FINANSOWE	STRATEGICZNE	OPERACYJNE	ZGODNOŚCI Z PRAWEM		
Rodzaj działalności	Risk weighting	5*	4*	3*	2*		
System dla Skarbu	158	1	1	1	0	12	1896
Ciągłość działania	162	0	0	1	1	5	810
Place	165	0	0	1	0	3	495
Sieć lokalna (LAN)	159	0	0	1	0	3	477
Computer operations	146	0	0	1	0	3	438
Licencjon-	123	0	0	0	1	2	246

Wanie Oprogramowania							
RACF	152	0	0	1	0	3	456

Na przykładzie systemu skarbowego: $158 * (5*1+4*1+3*1+2*0) = 158*(5+4+3) = 158*12 = 1896$

13. PRZYKŁAD III

13.1 Część audytorów IS preferuje ocenianie projektów, a nie całego zbioru audytowalnych jednostek (IS auditable universe). Przykład III prezentuje metodologię do oceniania projektów IT. Każdy projekt IS znajdujący się w zbiorze audytowalnych jednostek IS (IS audit universe) będzie oceniany na podstawie tych ośmiu kluczowych zmiennych z wykorzystaniem liczbowych wartości ryzyka od 1 (niskie) do 5 (wysokie). Wyniki tych ocen (ranking judgments) są potem mnożone przez wagę z zakresu od 1 (niski) do 10 (wysoki) i daje to wartość zwiększoną (extended value). Wartości zwiększone (extended values) dodane do siebie dając sumę. Kiedy mamy sumę dla każdego projektu, projekty są rangowane wg ryzyka. Na podstawie tego rankingu tworzona jest struktura rocznego planu audytu. Kategorie zastosowane w przykładzie III są wyspecyfikowane w pkt. 13.2 i 13.3.

13.2 Miary wpływu

- **Budżet projektu** —ważnym czynnikiem do rozważenia jest łączny budżet projektu IS. Wskazówką może być, że niektóre organizacje szacują projekty o budżecie ponad US\$500,000 jako ryzyko na poziomie 4 lub 5. Te organizacje szacują ryzyko budżetów pomiędzy US \$100,000 to US\$ 500,000 na poziomie 2 lub 3 i budżety poniżej US \$100,000 jako ryzyko 1.
- **Wolumen transakcji**—łączny wolumen transakcji przewidywanych, że będą przetwarzane przez system w określonym okresie.
- **Charakter czynności (działalności)** —krytyczność czynności i części organizacji, która wykorzystuje daną czynność. Rzadkie lub niezwykle czynności lub projekty mają większe prawdopodobieństwo skutkowania błędem lub nieefektywnością i nieeficyjnością i znajdują się w kręgu szczególnego zainteresowania audytora.
- **Zainteresowanie wyższego kierownictwa** —Ten czynnik odnosi się do tego jak w opinii kierownictwa wyższego szczebla ważną jest jednostka, funkcja lub obszar.
- **Przygotowania do powrotu (Fall back arrangements)**—ten czynnik odnosi się do działań które zostały przewidziane w celu kontynuowania działalności na wypadek gdy nowy system ma problemy. Czynniki, które należy uwzględnić to:
 - plany kontynuacji działalności,
 - plany przywracania działalności po katastrofie,
 - procedury pracy ręcznej
 - stary system.

Ogólnie mówiąc, jeżeli powyższe kwestie zostały rozważone, są osiągalne lub (w oryginale jest „or” moim zdaniem powinno być „and”) są efektywne kosztowo, to ryzyko jest najmniejsze.

13.3 Miary prawdopodobieństwa

- **Zmiany w procedurach**—zakres zmian proceduralnych lub reinżynierii towarzyszących implementacji systemu.
- **Złożoność systemu** —powinny być rozważone takie czynniki jak liczba użytkowników, ilość modułów systemów, środowisko mainframe wersus klient-srewer (zcentralizowane wersus zdecentralizowane) i liczba interfejsów.
- **Zarządzanie projektami**—Rangując zarządzanie projektami powinno się rozważyć:
 - Projekty robione wewnątrz lub przez firmy zewnętrzne
 - Strukturę projektu
 - Umiejętności personelu
 - Ramy czasowe projektu

Ogólnie mówiąc ryzyko jest dzielone jeśli projekt jest outsourcowany.

PRZYKŁAD III—OCENA RYZYKA PROJEKTU IT

Kategoria	Poziom ryzyka 1(niski do 5(wysoki)	Waga konsekwencji 1(małe) to 10(wysokie)	Razem
1. Budżet projektu >\$500,000 = 4 do 5 \$100,000 do \$500,000 = 2 do 3 <\$100,000 = 1		5	
2. Wolumen transakcji		2	
3. Charakter działalności			
Kluczowa (Core council) 4 do 5 Jednostka biznesowa 2 do 3		8	

System lokalny 1			
4. Zainteresowanie kierownictwa wyższego szczebla Duże zainteresowanie = 4 do 5 Umiarkowane zainteresowanie = 2 do 3 Niewielkie zainteresowanie = 1		6	
5. Procedury powrotu Plany kontynuacji działania/przywracania działania po katastrofie Procedury manualne Stary system		7	
6. Zmiany w procedurach (Zakres reinżynieringu) Duży reinżyniering = 4 do 5 Umiarkowany reinżyniering = 2 do 3 Niewielki reinżyniering = 1		8	
7. Złożoność systemu Ilość użytkowników Ilość modułów Zcentralizowany czy zdecentralizowany (mainframe v. Klient-serwer) Interfejsy		7	
8. Zarządzanie projektem Wewnętrzne Zewnętrzni developers Struktura Umiejętności Ramy czasowe		7	
		Razem	

14. PRZYKŁAD IV—Ocena ryzyka jednostki audytowalnej

14.1 Przykład 4 ocenia różne kategorie audytowalnych jednostek w zbiorze audytowalnych jednostek IS po ich zidentyfikowaniu. Kategorie są specyfikowane na podstawie natury ryzyka na jakie są narażone te jednostki. Odpowiednie informacje takie jak: ekspozycja finansowa, wpływ na biznes, zakres, są zbierane. Kategorie są następujące:

- Operacje centrum przetwarzania danych
- Aplikacje (produkcyjne)
- Aplikacje (rozwój)
- **IS procurement (ludzie i sprzęt) (manpower and material)**
- Zakupy oprogramowania
- Inne funkcje IS

14.2 W każdej kategorii są wymienione istotne elementy ryzyka. W zależności od rodzaju ryzyka, każdemu z elementów ryzyka przypisywana jest waga. Scoring ryzyka dla określonego elementu ryzyka jest wynikiem oceny punktowej i jej wagi. Ogólny scoring ryzyka funkcji to suma scoringów poszczególnych elementów ryzyka. Dla ułatwienia porównań ryzyko jest mierzone na skali do 100. Oddzielne arkusze oceny ryzyka mogą być przygotowane dla każdej audytowalnej jednostki. Na końcu scoringi otrzymane dla każdej audytowalnej jednostki są konsolidowane i ustalane są priorytety audytu.

PRZYKŁAD IV—OCENA RYZYKA—AUDYT IS
i. DZIAŁNOŚĆ CENTRUM PRZETWARZANIA DANYCH

	Czynnik ryzyka	Waga	Punkty	Przyznane punkty
1.	Liczba personelu centrum przetwarzania danych Bardzo mała poniżej 2 Mała 3—7 Umiarkowana 7—15 Duża 16—25 Bardzo duża ponad 25	1	1 2 3 4 5	5
2.	Wpływ na działalność biznesową grupy Bez wpływu Mały Umiarkowany Wysoki Może uniemożliwić Grupie działalność biznesową	5	1 2 3 4 5	25
3.	Liczba aplikacji Pojedyncza Poniżej 5 5—15 16—25 Ponad 25	5	1 2 3 4 5	25
4.	Liczba użytkowników Poniżej 25 26—50 51—100 100—250 Powyżej 250	2	1 2 3 4 5	10
5.	Nieprawidłowości stwierdzone podczas poprzedniego audytu Brak znaczących nieprawidłowości Kilka znaczących nieprawidłowości Wiele mało istotnych nieprawidłowości Niewiele istotnych nieprawidłowości Wiele istotnych nieprawidłowości	1	1 2 3 4 5	5
6.	Złożoność przetwarzania Batch Batch/w czasie rzeczywistym Batch/w czasie rzeczywistym/on-line Klient/serwer Równoległe/rozproszone	2	1 2 3 4 5	10
7.	Zmiany w sprzęcie/platformie/personelu Baz zmian Umiarkowane zmiany/niska fluktuacja Zmiana platformy/mała fluktuacja Wysoka fluktuacja Zmiana platformy I wysoka fluktuacja	1	1 2 3 4 5	5
8.	Ilość platform 1 2 3 4 5+	3	1 2 3 4 5	15
	Łączny scoring		100	100

PRZYKŁAD IV—OCENA RYZYKA—AUDYT IS
ii. APLIKACJA (PRODUKCJA)

	Czynnik ryzyka	Waga	Punktu	Przyznane punkty
1.	Wpływ błędu systemu (krytyczność) Brak natychmiastowego wpływu Niedogodność dla użytkowników Utrata reputacji Utrata przychodów Utrata biznesu/przychodów/reputacji	5	1 2 3 4 5	25
2.	Ekspozycja finansowa(AED) Brak Mała (<100,000) Umiarkowana (100,000—1 m) Wysoka (1m—10 m) Bardzo wysoka (>10 m)	5	1 2 3 4 5	25
3.	Zakres systemu Część departamentu Cały departament Wielodepartamentowy Dla całej organizacji Dla całej organizacji i na zewnątrz	2	1 2 3 4 5	10
4.	Wiek aplikacji Ponad 10 lat 7—10 lat 4—6 lat 1—3 lat Mniej niż 1 rok	1	1 2 3 4 5	5
5.	Nieprawidłowości stwierdzone podczas poprzednich audytów Poprzedni audyt – brak słabości Poprzedni audyt – nieznaczące słabości Audyt—kilka słabości Audyt—wiele słabości Nie było audytu	2	1 2 3 4 5	10
6.	Wielkość aplikacji (ilość programów) Poniżej 25 25—50 50—100 100—250 Ponad 250	3	1 2 3 4 5	15
7.	Zmiany w śodowisku/personelu Bez zmian Umiarkowane zmiany/niska fluktuacja Znaczące zmiany/mała fluktuacja Wysoka fluktuacja Znaczące zmiany i wysoka fluktuacja	1	1 2 3 4 5	5
8.	Ilość wdrożonych lokalizacji 1 2 3 4 5+	1	1 2 3 4 5	5
	Łączny scoring		100	100

PRZYKŁAD IV—OCENA RYZYKA—AUDYT IS
iii. APLIKACJA (ROZWÓJ)

	Czynnik ryzyka	Waga	Punkty	Przyznane punkty
1.	Wielkość, organizacja i doświadczenie zespołu Mały, bedykowany i doświadczony zespół Przeciętna wielkość, scentralizowany i doświadczony zespół Przeciętny, doświadczony, różne priorytety Przeciętny, w większości zcentralizowany z innymi priorytetami Wielki, zdecentralizowany, niedoświadczony i z niejasną podległością służbową	3	1 2 3 4 5	15
2.	Wielkość systemu Mała ilość programów dla 1 departamentu Umiarkowana ilość programów dla 1 departamentu Duża ilość programów dla wielu departamentów Umiarkowana liczba programów dla całej organizacji Wielka liczba programów dla całej organizacji	3	1 2 3 4 5	15
3.	Długość cyklu rozwoju Mniej niż 3 miesiące 3—6 miesięcy 6—12 miesięcy 1—1 ¹ / ₂ roku 2 lub więcej lat	2	1 2 3 4 5	10
4.	Platforma, aplikacji Sprawdzona i powszechnie używana Dość nowa ale akceptowana powszechnie na świecie Dość nowa ale nieakceptowana powszechnie na świecie Wypróbowana i markowa (trade name, brand name) Nowa, nie wypróbowana, markowa	3	1 2 3 4 5	15
5.	Poprzednie zaangażowanie audytu Doświadczenia w budowaniu mechanizmów kontrolnych Faza analizowania wymogów Monitorowanie harmonogramu projektu Monitorowanie kosztów projektu Brak	2	1 2 3 4 5	10
6.	Metodologia rozwoju systemu Standardowa metodologia z udokumentowanymi standardami i procedurami Standardowa metodologia bez udokumentowanych standardów i procedur Brak standardowej metodologii ale doświadczony zespół Eksperymentalna, nie sprawdzona metodologia Brak użycia jakiegokolwiek metodologii rozwoju, brak udokumentowanych standardów rozwoju i wytycznych	3	1 2 3 4 5	15
7.	Doświadczenie w zarządzaniu projektami Bardzo duże Powyżej przeciętnej Przeciętne Poniżej przeciętnej Brak doświadczenia/ multiproject	1	1 2 3 4 5	5
8.	Outsorsowanie personelu Mała ilość, pojedynczy dostawca Mała ilość, zróżnicowani dostawcy Znacząca ilość, pojedynczy dostawca Znacząca ilość, zróżnicowani dostawcy 100%	1	1 2 3 4 5	5
	Łączny scoring		100	90

PRZYKŁAD IV—OCENA RYZYKA AUDYT IS
iv. IS PROCUREMENT (MANPOWER AND MATERIAL)

	Czynnik ryzyka	Waga	Punkty	Przyznane punkty
1.	Wpływ Brak natychmiastowego wpływu Niedogodność dla użytkowników Utrata reputacji Utrata przychodów Utrata biznesu/przychodów/reputacji	5	1 2 3 4 5	25
2.	Ekspozycja finansowa (AED) Brak Mała (<100,000) Umiarkowana (100,000—1 m) Wysoka (1m—10 m) Bardzo wysoka (>10 m)	5	1 2 3 4 5	25
3.	Procedury i wytyczne Udokumentowane i sprawdzone procedury Procedury nieudokumentowane Procedury ale nie w pełni zaimplementowane Brak ustalonych procedur ale kontrolowane Brak ustalonych procedur I niekontrolowane	5	1 2 3 4 5	25
4.	Nieprawidłowości stwierdzone podczas poprzednich audytów Poprzedni audyt – brak słabości Poprzedni audyt – nieznaczące słabości Audyt—kilka słabości Audyt—wiele słabości Nie było audytu	2	1 2 3 4 5	10
5.	Złożoność Lokalne zasoby dla jednego departamentu Lokalne zasoby dla całej organizacji Międzynarodowe zasoby dla jednej technologii Międzynarodowe zasoby dla wielu technologii Międzynarodowe i lokalne zasoby dla wielu technologii	3	1 2 3 4 5	15
	Łączny scoring		100	100

**PRZYKŁAD IV—OCENA RYZYKA —AUDYT IS
v. ZAKUPY OPROGRAMOWANIA**

	Czynnik ryzyka	Waga	Punkty	Przyznane punkty
1.	Zakres systemu Część departamentu Cały departament Wielodepartamentowy Dla całej organizacji Dla całej organizacji i na zewnątrz	5	1 2 3 4 5	25
2.	Ekspozycja finansowa (AED) związana z systemem Brak Mała (<100,000) Umiarkowana (100,000—1 m) Wysoka (1m—10 m) Bardzo wysoka (>10 m)	5	1 2 3 4 5	25
3.	Charakter pakietu (oprogramowania) Produkt z "półki" Zaadaptowany (Skastomizowany) przez dostawcę, utrzymywany przez dostawcę Wykonany przez dostawcę, utrzymywany wewnętrznie Stworzony wspólnie, utrzymywany przez dostawcę Stworzony wspólnie, utrzymywany wewnętrznie	2	1 2 3 4 5	10
4.	Typ oceny Przez departament użytkownika/IS/konsultanta Przez IS/użytkownika Przez konsultanta Przez IS Przez departament użytkownika	1	1 2 3 4 5	5
5.	Koszt i złożoność pakietu Nieznaczące Małe Umiarkowane Znaczące Bardzo wysokie	2	1 2 3 4 5	10
6.	Metodologia oceny Oceniany produkt/dostawca Oceniany tylko produkt Oceniany tylko dostawca Nie oceniany, kupiony warunkowo Nie oceniany, kupiony bezwarunkowo	3	1 2 3 4 5	15
7.	Wybór Wybrany spośród wielu kandydatów Wybrany spośród kilku reputowanych dostawców Wybrany spośród kilku znanych systemów Wybrany znany system Wybrany nieznan system	1	1 2 3 4 5	5
8.	Wpływ na działalność biznesową Brak natychmiastowego wpływu Niedogodność dla użytkowników Utrata reputacji Utrata przychodów Utrata biznesu/reputacji/przychodów	1	1 2 3 4 5	5
	Łączny scoring		100	100

**PRZYKŁAD IV – OCENA RYZYKA- AUDYT IS
vi. INNE FUNKCJE IS**

	Czynnik ryzyka	Waga	Punkty	Przyznane punkty
1.	Wpływ błędu funkcji (krytyczność) Brak natychmiastowego wpływu Niedogodność dla użytkowników Utrata reputacji Utrata przychodów Utrata biznesu/przychodów/reputacji	5	1 2 3 4 5	25
2.	Ekspozycja finansowa (AED) Brak Mała (<100,000) Umiarkowana (100,000—1 m) Wysoka (1m—10 m) Bardzo wysoka (>10 m)	5	1 2 3 4 5	25
3.	Zakres funkcji Część departamentu Cały departament Wielodepartamentowa Dla całej organizacji Dla całej organizacji i na zewnątrz	2	1 2 3 4 5	10
4.	Wiek funkcji Ponad 10 lat 7—10 lat 4—6 lat 1—3 lat Mniej niż 1 rok	1	1 2 3 4 5	5
5.	Nieprawidłowości stwierdzone podczas poprzednich audytów Poprzedni audyt – brak słabości Poprzedni audyt – nieznaczące słabości Audyt—kilka słabości Audyt—wiele słabości Nie było audytu	2	1 2 3 4 5	10
6.	Złożoność funkcji Bardzo mała Mała Umiarkowana Wysoka Bardzo wysoka	3	1 2 3 4 5	15
7.	Ilość personelu 1 Mniej niż 5 6—10 (gdzieś w oryginale zginęło im = 5) 11—25 Ponad 25	1	1 2 3 4 5	5
8.	Liczba lokalizacji 1 2 3 4 5+	1	1 2 3 4 5	5
	Łączny scoring		100	100

15. OBOWIĄZYWANIE

15.1 Powyższa procedura obowiązuje w stosunku do wszystkich audytów systemów informatycznych począwszy od 1 lipca 2002r.

Procedura 1 Ocena ryzyka IS

BIBLIOGRAFIA

Infrastruktura Klucza Publicznego

AICPA/CICA WebTrust Principles and Criteria for CAs

Department of Energy Records Schedule (DOERS), <http://ardor.nara.gov/doi/index.html>

Digital Signatures Security & Control, ISACF, 2002, Rolling Meadows, IL, USA

DOE IT standards repository and program-related information, <http://cio.doe.gov> Select Standards Records Management General Records Schedules (GRS), <http://gopher.nara.gov:70/1/managers/federal/schedule>

National Institute of Standards and Technology Computer Security Division, PKI Specifications to support the DOE Travel Manager Program, August 15, 1996, <http://cio.doe.gov> and select Computer Security Standards

Telecommunications Security Manual, DOE M 200.1-1, chapter 9

Prawo

ABA-PKI Assessment Guidelines (currently only draft)

American Bar Association Digital Signature Guidelines, www.abanet.org/scitech/ec/isc/dsg.html

ANSI X9.79 and the AICPA/CICA WebTrust for Certification Authorities, www.cpawebtrust.org/CertAuth_fin.htm

ESSI – Final report of the ESSI Expert Team

EU Directive on the matter can be found at http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399L0093.html

IETF PKIX

ITU X.509

McBride, Baker & Coles, Summary of Electronic Commerce and Digital Signature Legislation, www.mbc.com/ds_sum.html

PKI assessment guidelines of the American Bar Association. Available at www.abanet.org/scitech/ec/isc

Software Industry Issues: Digital Signatures, www.SoftwareIndustry.org/issues/1digsig.html#s1

Aplikacje

Entrust ISVs, www.entrust.com/ kliknij na *search* i wpisz ISV.

Domowa strona Netscape, www.netscape.com.

NIST Special Publication 800-2, Public Key Cryptography.

NIST: Public key infrastructure program (as of July 1998), <http://csrc.nist.gov/pki/>.

Domowa strona OMG, www.omg.org.

S/MIME Editor. S/MIME message specification PKCS security services for MIME.

Standardy kontroli systemów informatycznych

Wydane przez Information Systems Audit and Control Association (Stowarzyszenie do spraw audytu i kontroli systemów informatycznych)

510 Zakres

510.010 Obowiązki, uprawnienia i odpowiedzialność

Obowiązki, uprawnienia i odpowiedzialność funkcji kontrolowania systemów informatycznych mają być odpowiednio udokumentowane i zatwierdzone przez odpowiedni szczebel kierownictwa.

520 Niezależność

520.010 Niezależność zawodowa

We wszystkich sprawach związanych z kontrolą systemów informatycznych, kontroler systemów informatycznych musi być niezależny, zarówno jeśli chodzi o postawę wewnętrzną, jak i wizerunek.

520.020 Powiązania organizacyjne

Funkcja kontroli systemów informatycznych ma być wystarczająco niezależna od kontrolowanego obszaru, aby zapewnić obiektywne pełnienie obowiązków kontrolerów systemów informatycznych.

530 Standardy i etyka zawodowa

530.010 Kodeks etyki zawodowej

Kontroler systemów informatycznych jest zobowiązany do stosowania się do Kodeksu Etyki Zawodowej Stowarzyszenia do spraw audytu i kontroli systemów informatycznych (ISACA - Information Systems Audit and Control Association).

530.020 Należyta staranność zawodowa

We wszelkich aspektach pracy kontrolera systemów informatycznych obowiązuje należyta staranność zawodowa oraz przestrzeganie odpowiednich standardów zawodowych.

540 Kompetencje

540.010 Umiejętności i wiedza

Kontroler systemów informatycznych ma być kompetentny w zagadnieniach technicznych, posiadając [równocześnie] umiejętności i wiedzę niezbędne do wykonywania pracy audytorskiej.

540.020 Ustawiczne szkolenie zawodowe

Kontroler systemów informatycznych jest zobowiązany utrzymywać na odpowiednim poziomie swoje kompetencje dotyczące zagadnień technicznych poprzez właściwe i ustawiczne szkolenie zawodowe.

550 Planowanie

550.010 Planowanie kontroli

Kontroler systemów informatycznych ma wykorzystywać analizę ryzyka i inne, stosowne narzędzia w planowaniu i priorytetyzowaniu prac kontrolnych by odzwierciedlić cele kontrolne.

560 Wykonywanie prac audytowych

560.010 Nadzór

Kontroler systemów informatycznych ma podlegać odpowiedniemu nadzorowi, w celu zapewnienia, że zostaną spełnione cele kontroli oraz odpowiednie standardy zawodowe audytu.

560.020 Dowody

Kontroler systemów informatycznych jest zobowiązany uzyskać wystarczające, wiarygodne, stosowne i użyteczne dowody, tak aby skutecznie zrealizować cele kontroli. Oceny kontroli mają być poparte odpowiednią analizą i interpretacją tychże dowodów.

560.030 Effectiveness

In carrying out their duties, information systems control professionals are to establish appropriate measures of the effectiveness of their activities in achieving both the objectives of their role and the objectives defined in the Statement of Scope.

570 Raportowanie

570.010 Okresowe raportowanie

Kontroler systemów informatycznych raportuje odpowiedniemu szczeblowi zarządzania w zakresie, w którym zostały osiągnięte cele kontrolne.

080 Dalszy ciąg działań

080.010 Dalszy ciąg działań

Kontroler systemów informatycznych ma monitorować wydajność procedur kontrolnych i przegląda informacje zwrotne dotyczące skuteczności i wydajności działań kontrolnych oraz, jeżeli zachodzi taka potrzeba, upewnia się czy zostały podjęte działania naprawcze.

OBOWIĄZYWANIE

Niniejsze standardy zostały wydane 1 maja 1999 i obowiązują w stosunku do wszystkich działań kontrolnych systemów informatycznych rozpoczynających się począwszy od dnia 1 września 1999 roku.

Historia

Postanowienia o standardach audytowania SI (SISAS)

Documents withdrawn

Tytuł	Withdrawal date
SISAS 3 (Evidence Requirement)	19 June 1998
SISAS 7 (Audit Reports)	19 June 1998
SISAS 9 (Use of Audit Software Tools)	19 June 1998
SISAS 4 (Due Professional Care)	1 October 1999
SISAS 6 (Audit Documentation)	1 October 1999
SISAS 2 (Involvement in the System Development Process)	1 March 2000
SISAS 8 (Audit Considerations for Irregularities)	1 March 2000
SISAS 1 (Attitude & Appearance - Organisational Relationship)	1 September 2000
SISAS 5 (The Use of Risk Assessment in Audit Planning)	1 September 2000

Dodatek-Słownik/indeks

Zachowanie

akt tworzenia wyobrażenia czy stwarzania wrażenia, odnośnie tego kim lub jakim się jest, lub też co się robi

020.010 Niezależność zawodowa

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

020.020.010 Powiązania organizacyjne i niezależność

Błąd! Nie można odnaleźć źródła odsyłacza.

Wyrażanie niezależności

zachowanie właściwe dla sprostania sytuacjom pojawiającym się podczas wykonywania prac związanych z audytem (wywiadów, spotkań, raportowania, itd.). Audytor SI powinien być świadomy, że wyrażanie niezależności w postępowaniu zależy od sposobu postrzegania przez innych, i że mogą mieć na to wpływ niewłaściwe działania lub związki.

020.020.010 Powiązania organizacyjne i niezależność

Przegląd nabywania aplikacji

ocena aplikacji, która ma zostać nabyta lub jest przedmiotem analizy, obejmująca takie zagadnienia, jak: - zaplanowanie w systemie odpowiednich mechanizmów kontrolnych, - kompletność, dokładność i niezawodność procesu przetwarzania informacji, - funkcjonowanie aplikacji zgodnie z zamierzeniami, - funkcjonowanie aplikacji w zgodzie z dowolnymi wymogami prawnymi (ustawowymi itp.) - zgodność działań nabywania danego systemu z ustaloną procedurą (procesem) nabywania systemów

Mechanizmy kontrolne aplikacji

odnoszą się do transakcji i parametrów związanych z każdą aplikacją komputerową i z tego powodu są charakterystyczne dla każdej aplikacji. Celem mechanizmów kontrolnych (manualnych lub programowych) aplikacji jest zapewnienie kompletności i dokładności rekordów oraz poprawności i ważności zapisów w nich zawartych, będących wynikiem zarówno manualnego jak i programowego przetwarzania. Przykładem mechanizmów kontrolnych aplikacji może być: sprawdzanie poprawności i ważności danych wejściowych, uzgadnianie sum przetwarzania wsadowego i szyfrowanie transmitowanych danych

060.020.020 Przegląd systemów aplikacyjnych

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Przegląd rozwoju aplikacji

Ocena aplikacji będącej na etapie rozwoju, obejmująca takie zagadnienia, jak: - zaplanowanie w systemie odpowiednich mechanizmów kontrolnych, - kompletność, dokładność i niezawodność procesu przetwarzania informacji, - funkcjonowanie aplikacji zgodnie z zamierzeniami, - funkcjonowanie aplikacji w zgodzie z dowolnymi wymogami prawnymi (ustawowymi itp.) - zgodność działań rozwoju systemu z ustaloną procedurą (procesem) cyklu rozwoju systemów.

Przegląd wdrożenia aplikacji

Ocena dowolnego fragmentu przedsięwzięcia (projektu) wdrożeniowego (np. zarządzania przedsięwzięciem (projektem), planów testów, procedur testowania dotyczących akceptacji przez użytkowników).

Przegląd utrzymania (pielęgnacji) aplikacji

Ocena dowolnego fragmentu przedsięwzięcia (projektu) dotyczącego utrzymania (pielęgnacji) aplikacji (np. zarządzania przedsięwzięciem (projektem), planów testów, procedur testowania dotyczących akceptacji przez użytkowników).

Oprogramowanie użytkowe do śledzenia i mapowania

Specjalistyczne narzędzia, które mogą być używane do analizy przepływu danych poprzez badanie logiki przetwarzania oprogramowania oraz dokumentowanie organizacji, ścieżek logicznych, warunków sterujących i ciągów procesów. Analizie mogą być poddane zarówno język rozkazów, jak i wyrażenia sterujące zadaniami oraz język programowania. Techniki te obejmują: mapowanie, śledzenie, tworzenie obrazów wyników pośrednich symulacje równoległe oraz porównywanie kodów programów/systemów..

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Aplikacja (system aplikacyjny)

Zintegrowany zbiór programów komputerowych zaprojektowanych pod kątem realizacji danej funkcji, które wykonują określone działania związane z wejściem, przetwarzaniem i wyjściem danych (np. księga główna, planowanie zasobów produkcyjnych, zarządzanie personelem).

010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.020 Przegląd systemów aplikacyjnych

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

070.010.010 Raportowanie

Procedura 1 Ocena ryzyka IS

ASP/MSP (Dostawca usług aplikacyjnych, Dostawca usług zarządzanych)

trzecia strona, która dostarcza usług informatycznych (usługi aplikacyjne i sprzętowe) oraz zarządza nimi, i które obejmują usługi związane z zapewnieniem bezpieczeństwa dla wielu użytkowników poprzez Internet lub sieci prywatne.

050.010.040 Effect of Third Parties on an Organisation's IT Controls Guideline

Dodatek-Słownik/indeks c.d.

Stanowisko

sposób myślenia , zachowania, odczuwania , itp.

020.010 Niezależność zawodowa

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

020.020.010 Powiązania organizacyjne i niezależność

030.010.010 Nieprawidłowości i akty bezprawne

Błąd! Nie można odnaleźć źródła odsyłacza.

Odpowiedzialność audytu (rozliczanie wykonania prac audytu)

Pomiary wydajności podczas dostarczania usług, włączając w to koszty, zgodność z terminarzem oraz jakość, względem uzgodnionych poziomów usług.

010.010.010 Prawa i powinności audytu - statut audytu

Uprawnienia audytu

Oficjalne określenie zajmowanej pozycji w ramach organizacji, obejmujące ścieżki raportowania oraz prawa dostępu (wstępu, wglądu, itp.).

010.010.010 Prawa i powinności audytu - statut audytu

Statut audytu

Dokument określający obowiązki, uprawnienia i odpowiedzialność obszaru (funkcji) audytu SI..

010.010 Obowiązki, uprawnienia i odpowiedzialność

010.010.010 Prawa i powinności audytu - statut audytu

010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

020.020.010 Powiązania organizacyjne i niezależność

030.020.010 Rozważania audytowe na temat nieprawidłowości

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

060.020.080 Wykorzystanie prac innych audytorów i ekspertów

Dowody audytu

Audytor Systemów Informatycznych (Audytor SI) gromadzi informacje w trakcie przeprowadzania audytu IT. Informacje użyte przez Audytora IT, dla spełnienia cele celów audytu nazywane są dowodami audytu (dowodami).

010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

020.020.010 Powiązania organizacyjne i niezależność

030.020.010 Rozważania audytowe na temat nieprawidłowości

030.020.020 Należyta staranność zawodowa

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.010 Dokumentacja audytu

060.020.020 Przegląd systemów aplikacyjnych

060.020.030 Wymóg dowodów audytu

060.020.040 Próbkiwanie audytowe

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

060.020.080 Wykorzystanie prac innych audytorów i ekspertów

Eksperskie systemy audytowe

Systemy wspomagające ekspertyzy lub decyzje, które poprzez automatyzację przetwarzania zgromadzonej wiedzy ekspertów mogą być stosowane w pracy Audytora SI jako pomocnicze w procesach podejmowania decyzji. Technika ta obejmuje pakiety do automatycznej analizy ryzyka, oprogramowania systemowego oraz oprogramowania do celów kontrolnych.

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Plan audytu

ogólny opis prac audytowych, które mają być wykonane w określonym czasie (zwykle jeden rok). Obejmuje obszary, które mają być audytowane, cele ogólne i zakres prac, jak również inne zagadnienia, takie jak budżet, alokacja zasobów, harmonogram, rodzaj raportu i jego potencjalni odbiorcy, oraz inne ogólne aspekty prac.

050.010 Planowanie audytu

010.010.010 Prawa i powinności audytu - statut audytu

020.020.010 Powiązania organizacyjne i niezależność

030.020.010 Rozważania audytowe na temat nieprawidłowości

050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych

050.010.020 Planowanie

050.010.030 Ocena ryzyka podczas planowania audytu

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Procedura 1 Ocena ryzyka IS

Program audytu

seria kroków niezbędnych do osiągnięcia celu audytu.

050.010.020 Planowanie

Dodatek-Słownik/indeks c.d.

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji
060.020.010 Dokumentacja audytu
060.020.080 Wykorzystanie prac innych audytorów i ekspertów

Obowiązki audytu

Rola, zakres działań oraz zadania udokumentowane w umowie dotyczącej poziomu usług pomiędzy kierownictwem a audytem.

010.010.010 Prawa i powinności audytu - statut audytu

Ryzyko Audytowe

ryzyko wydania błędnej opinii audytowej.

030.020.020 Należyta staranność zawodowa

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.040 Próbkowanie audytowe

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Procedura 1 Ocena ryzyka IS

Próbkowanie audytowe

zastosowanie procedury audytowej dla mniej niż 100% obserwacji z danej populacji, by uzyskać dowód audytowy potwierdzający określoną charakterystykę populacji.

060.020.040 Próbkowanie audytowe

Authentication

Determining that a person or computer system trying to access information is really the entity they say they are.

070.010.010 Raportowanie

Procedura 1 Ocena ryzyka IS

Dostawca usług biznesowych (BSP ang. skrót)

Dostawca usług aplikacyjnych (ASP), który zapewnia również outsourcing procesów biznesowych takich jak obsługa płatności, obsługa zleceń sprzedaży czy rozwój aplikacji..

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

CAATs - Techniki komputerowego wspomaganie audytu

dowolna z technik zautomatyzowanego audytu, taka jak: oprogramowanie audytowe ogólnego stosowania, oprogramowanie narzędziowe, dane testowe, oprogramowanie śledzące i mapujące oraz audytowe systemy eksperckie.

060.020.020 Przegląd systemów aplikacyjnych

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Cadbury

Raport stworzony przez Committee on the Financial Aspects of Corporate Governance (kierowany przez Sir Adriana Cadbury, a powołany w 1991 roku przez brytyjską radę Financial Reporting Council, giełdę London Stock Exchange oraz brytyjskie środowisko księgowych), w Wielkiej Brytanii powszechnie znany jako "Raport Cadbury".

Certificate authority (CA)

A trusted third party that serves authentication infrastructures or organisations and registers entities and issues them certificates.

Procedura 1 Ocena ryzyka IS

Certificate revocation list

A list of retracted certificates.

Procedura 1 Ocena ryzyka IS

COBIT

Control Objectives for Information and Related Technology (Cele Kontrolne Technologii Informatycznych i Technologii Pokrewnych), międzynarodowy zbiór celów kontrolnych dla IT opublikowany przez fundację ISACAF w 1996..

010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

020.020.010 Powiązania organizacyjne i niezależność

050.010.020 Planowanie

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

060.020.020 Przegląd systemów aplikacyjnych

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

070.010.010 Raportowanie

COCO

Kryteria kontroli (Criteria Of Control), opublikowane w 1995 roku przez Canadian Institute of Chartered Accountants

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Combined Code on Corporate Governance (Skonsolidowane Przepisy odnośnie Nadzoru Korporacyjnego)

Przeprowadzona w 1998 konsolidacja Raportów "Cadbury", "Greenbury" i "Hampel". Raporty te, nazwane tak od nazwisk przewodniczących komisji, były sponsorowane przez UK Financial Reporting Council, the London Stock Exchange, the Confederation of British Industry, the Institute of Directors, the Consultative Committee of Accountancy Bodies, the National Association of Pension

Dodatek-Słownik/indeks c.d.

Funds oraz the Association of British Insurers, i miały na celu odniesienie się do "Finansowych Aspektów Nadzoru Korporacyjnego, Wynagrodzenia Dyrektorów" oraz wdrożenie rekomendacji Cadbury i Greenbury.

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Testowanie Zgodności

test kontroli zaprojektowany w celu uzyskania dowodów, obrazujących zarówno efektywność jak i funkcjonowanie kontroli w okresie poddanym audytowi.

050.010.020 Planowanie

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.030 Wymóg dowodów audytu

060.020.040 Próbkowanie audytowe

Procedura 1 Ocena ryzyka IS

Techniki komputerowego wspomaganie audytu patrz CAATs

Cele Kontrolne Nadzoru Przedsiębiorstw (Control Objectives for Enterprise Governance)

Opublikowany w 1999 przez the Information Systems Audit and Control Foundation dokument do dyskusji, proponujący "Model Nadzoru Przedsiębiorstw" ("Enterprise Governance Model"), silnie koncentrujący się zarówno na celach biznesowych jak i na tzw. "czynnikach umożliwiających" IT, ułatwiających prawidłowy nadzór w przedsiębiorstwach.

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Ryzyko Kontroli

ryzyko, że błąd, który mógłby powstać w audytowanym obszarze, i który mógłby być istotny, samodzielnie lub w połączeniu z innymi błędami, nie zostanie uniknięty lub wykryty i skorygowany, we właściwym czasie przez system kontroli wewnętrznej.

010.010.010 Prawa i powinności audytu - statut audytu

050.010.030 Ocena ryzyka podczas planowania audytu

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

060.020.040 Próbkowanie audytowe

Nadzór Korporacyjny (Corporate Governance)

"... struktury za pomocą których ustalane są cele organizacji i środki ich osiągnięcia, oraz określane są wytyczne, jak zrealizować monitorowanie. Prawidłowy nadzór korporacyjny powinien zapewniać właściwe zachęty dla zarządu i kierownictwa, aby dążyli do celów leżących w interesie firmy i udziałowców, oraz powinien ułatwiać skuteczne monitorowanie, i w ten sposób pobudzać firmy do bardziej wydajnego wykorzystania zasobów." (Źródło: Zasady Nadzoru Korporacyjnego, wydane przez Organisation for Economic Cooperation and Development (OECD) w 1999 roku)

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Raport COSO

Stworzony w 1992 roku raport pt. "Kontrola wewnętrzna - zintegrowana struktura ramowa" ("Internal Control - Integrated Framework") przez Committee of Sponsoring Organisations of the Treadway Commission. Podaje wytyczne oraz obszerną strukturę ramową kontroli wewnętrznej dla wszystkich organizacji.

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Cross-certification

A certificate issued by one certification authority to a second certification authority so that users of the first certification authority are able to obtain the public key of the second certification authority and verify the certificates it has created. Often cross certification refers specifically to certificates issued to each other by two CAs at the same level in a hierarchy.

Procedura 1 Ocena ryzyka IS

Cryptography

The art of designing, analysing and attacking cryptographic schemes.

Procedura 1 Ocena ryzyka IS

Szczegółowe mechanizmy kontrolne

mechanizmy kontrolne dotyczące nabywania, wdrażania, dostarczania i wspierania systemów i usług SI. Składają się z mechanizmów kontrolnych aplikacji i tych ogólnych mechanizmów kontrolnych, które nie są zawarte w skrótnych mechanizmach kontrolnych.

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

Ryzyko Detekcji

ryzyko polegającym na tym, iż analityczne procedury audytowe nie ujawnią błędu, który sam lub w połączeniu z innymi błędami będzie miał istotny wpływ na analizowany obszar

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.040 Próbkowanie audytowe

Digital signature

An electronic signature formed using an asymmetric cryptographic scheme.

Procedura 1 Ocena ryzyka IS

Należyta staranność

Dbłość, z jaką osoba może wykonywać zadanie w określonych okolicznościach.

030.020.020 Należyta staranność zawodowa

Dodatek-Słownik/indeks c.d.

Należyta staranność zawodowa

Dbałość, z jaką osoba posiadająca specjalne umiejętności, może wykonywać zadanie w określonych okolicznościach.

Kodeks Etyki Zawodowej

030.020 Należyta staranność zawodowa

030.010.010 Nieprawidłowości i akty bezprawne

030.020.010 Rozważania audytowe na temat nieprawidłowości

030.020.020 Należyta staranność zawodowa

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Błąd! Nie można odnaleźć źródła odsyłacza.

Electronic signature

Any technique designed to provide the electronic equivalent of a handwritten signature to demonstrate the origin and integrity of specific data. Digital signatures are an example of electronic signatures.

Procedura 1 Ocena ryzyka IS

Wbudowany moduł audytowy (rewizyjny)

integralny składnik aplikacji, zaprojektowany w celu rozpoznawania i raportowania określonych transakcji lub innych informacji w oparciu o wcześniej zdefiniowane kryteria. Rozpoznawanie elementów (pozycji), które mają być zaraportowane, odbywa się w ramach przetwarzania w czasie rzeczywistym. Raportowanie może odbywać się bezpośrednio (interakcyjnie) w trybie czasu rzeczywistego, lub może wykorzystywać metody typu zapamiętaj i prześlij. Moduł ten znany jest również jako Zintegrowany System Testowy lub Moduł Kontroli (Rewizji) Ciągłej.

Umowa - zlecenie (na przeprowadzenie audytu)

Formalny dokument definiujący obowiązki, uprawnienia oraz odpowiedzialność (rozliczenie wykonanych prac) Audytora SI w ramach określonego przypisanego zadania do wykonania.

010.010 Obowiązki, uprawnienia i odpowiedzialność

010.010.010 Prawa i powinności audytu - statut audytu

010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

060.020.080 Wykorzystanie prac innych audytorów i ekspertów

Nadzór na Przedsiębiorstwach i Przedsięwzięciach (Enterprise governance)

Obszerne, mające szeroki zakres pojęcie z dziedziny nadzoru korporacyjnego, obejmujące stowarzyszone organizacje takie jak np. partnerzy globalnego porozumienia strategicznego (global strategic alliance partners) (Źródło: Control Objectives for Enterprise Governance Discussion Document opublikowany w 1999 roku przez Information Systems Audit and Control Foundation).

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Błąd

odchylenia w kontroli (w przypadku testowania zgodności) lub jej brak (w przypadku testowania dowodowego).

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

030.010.010 Nieprawidłowości i akty bezprawne

050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.030 Wymóg dowodów audytu

060.020.040 Próbki audytowe

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Procedura 1 Ocena ryzyka IS

Ryzyko Błędu

ryzyko wystąpienia błędu w audytowanym obszarze

050.010.030 Ocena ryzyka podczas planowania audytu

Narażenie

potencjalne straty w danym obszarze z powodu wystąpienia niepożądanych okoliczności.

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.020 Przegląd systemów aplikacyjnych

Procedura 1 Ocena ryzyka IS

Procedura 1 Ocena ryzyka IS

Ogólne mechanizmy kontrolne

mechanizmy kontrolne różne od mechanizmów kontrolnych aplikacji, związane ze środowiskiem, w którym aplikacje komputerowe działają oraz są rozwijane i zarządzane, a z tego powodu stosują się (ogólne mechanizmy kontrolne - przyp. tłum.) do wszystkich aplikacji. Celem ogólnych mechanizmów kontrolnych jest zapewnienie właściwego rozwoju i wdrażania aplikacji oraz integralności programów, zbiorów danych oraz operacji komputerowych. Podobnie jak aplikacyjne mechanizmy kontrolne, mogą być manualne i programowe. Przykładem ogólnych mechanizmów kontrolnych może być: rozwój i wdrażanie strategii SI, polityki bezpieczeństwa SI, odpowiednia organizacja personelu SI w celu eliminacji konfliktu obowiązków oraz planowanie prewencji przed katastrofą i odtwarzania po katastrofie.

060.020.020 Przegląd systemów aplikacyjnych

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Oprogramowanie audytowe ogólnego stosowania

Dodatek-Słownik/indeks c.d.

Program komputerowy lub zestaw programów przeznaczonych do automatycznego wykonywania określonych funkcji. Funkcje te obejmują odczyt plików komputerowych, wybieranie, obróbkę, sortowanie i sumowanie danych, wykonywanie obliczeń, wybieranie próbek, drukowanie raportów lub specjalnie sformatowanych przez Audytora SI pism. Stosowane techniki zawierają zarówno oprogramowanie nabyte lub napisane z przeznaczeniem dla audytu, jak też oprogramowanie wbudowane w systemy produkcyjne.
060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Hash function

An algorithm that maps or translates one set of bits into another (generally smaller) so that: a message yields the same result every time the algorithm is executed using the same message as input. It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm. It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

Procedura 1 Ocena ryzyka IS

Niezależność

Samorządność, brak konfliktów interesów i wolność od nacisków (wpływów zewnętrznych). Audytor SI powinien mieć swobodę w podejmowaniu swoich własnych decyzji, na które nie będzie wywierał wpływu audytowana organizacja oraz ludzie z nią związani (kierownictwo i pracownicy).

Kodeks Etyki Zawodowej

020.010 Niezależność zawodowa

010.010.010 Prawa i powinności audytu - statut audytu

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

020.020.010 Powiązania organizacyjne i niezależność

030.010.010 Nieprawidłowości i akty bezprawne

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

060.020.020 Przegląd systemów aplikacyjnych

060.020.030 Wymóg dowodów audytu

060.020.040 Próbki audytowe

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

060.020.080 Wykorzystanie prac innych audytorów i ekspertów

Błąd! Nie można odnaleźć źródła odsyłacza.

Stwarzanie wrażenia niezależności

wrażenie stwarzane na zewnątrz odnośnie samorządności, braku konfliktu interesów i wolności od nacisków (wpływów zewnętrznych).

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

Niezależna postawa

Bezstronny punkt widzenia który pozwala Audytorowi SI działać obiektywnie i sprawiedliwie.

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

Ryzyko inherentne (wewnętrzne)

jest to podatność na wystąpienie istotnego błędu, który sam lub w połączeniu z innymi błędami będzie miał istotny wpływ na analizowany obszar, przy braku odpowiednich wewnętrznych mechanizmów kontrolnych

050.010.020 Planowanie

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.040 Próbki audytowe

Procedura 1 Ocena ryzyka IS

Integralność

Completeness, accuracy and consistency.

030.020.020 Należyta staranność zawodowa

050.010.030 Ocena ryzyka podczas planowania audytu

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

060.020.020 Przegląd systemów aplikacyjnych

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Procedura 1 Ocena ryzyka IS

Kontrola wewnętrzna

"Polityki, procedury, praktyki i struktury organizacyjne, zaprojektowane w celu dostarczania rozsądnego zapewnienia, że cele biznesowe będą osiągnięte i, że będzie się zapobiegać niepożądanym zdarzeniom oraz je wykrywać i korygować." (Źródło: COBIT "Struktura ramowa")

020.020.010 Powiązania organizacyjne i niezależność

030.010.010 Nieprawidłowości i akty bezprawne

030.020.010 Rozważania audytowe na temat nieprawidłowości

050.010.020 Planowanie

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.010 Dokumentacja audytu

060.020.040 Próbki audytowe

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

060.020.080 Wykorzystanie prac innych audytorów i ekspertów

Nieprawidłowości

świadome naruszenie ustalonej polityki zarządzania lub wymagań regulacyjnych (wymagań organów nadzorczych), rozmyślne

Dodatek-Słownik/indeks c.d.

zniekształcenie lub pominięcie informacji dotyczącej obszaru audytowanego lub organizacji jako całości, poważne zaniedbanie lub niezamierzony czyn nielegalny.

030.010.010 Nieprawidłowości i akty bezprawne

030.020.010 Rozważania audytowe na temat nieprawidłowości

050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Dostawca usług internetowych (ang. skrót ISP))

trzecia strona, która dostarcza innym organizacjom różnorodne usługi związane z Internetem.

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

Nadzór nad IT (IT Governance)

Struktura zależności [powiązań] i procesów mająca na celu takie pokierowanie przedsiębiorstwem (przedsięwzięciem) i jego kontrolę, aby zrealizować cele tego przedsiębiorstwa, wypracowując wartość dodaną a równocześnie równoważąc ryzyko z dochodami z IT i powiązanych procesów.

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Istotność (ważność)

Wyrażenie względnego znaczenia lub ważności danej sprawy (zagadnienia) w kontekście organizacji jako całości.

030.010.010 Nieprawidłowości i akty bezprawne

050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych

050.010.020 Planowanie

060.020.040 Próbkowanie audytowe

Procedura 1 Ocena ryzyka IS

Nonrepudiation

The assurance that a party cannot later deny originating data, that it is the provision of proof of the integrity and origin of the data which can be verified by a third party. Nonrepudiation may be provided by a digital signature.

Procedura 1 Ocena ryzyka IS

Obiektywność

Zdolność do bezstronnej oceny, oraz bezstronnego wyrażania opinii i przedstawiania rekomendacji.

Kodeks Etyki Zawodowej

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

060.020.080 Wykorzystanie prac innych audytorów i ekspertów

Outsourcing (przekazanie, zlecenie usług do realizacji na zewnątrz)

formalna umowa (porozumienie) ze stroną zewnętrzną (tzw. stroną trzecią) w celu realizacji pewnych usług informatycznych na rzecz danej organizacji.

010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

030.010.010 Nieprawidłowości i akty bezprawne

050.010.020 Planowanie

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

060.020.080 Wykorzystanie prac innych audytorów i ekspertów

070.010.010 Raportowanie

Procedura 1 Ocena ryzyka IS

Wskaźniki Wydajności

Zbiór miar stworzonych w celu pomiaru stopnia w jakim cele wydajnościowe są spełniane w bieżącej działalności. Mogą one obejmować porozumienia dotyczące poziomów usług (SLA), krytyczne czynniki sukcesu, oceny zadowolenia klientów, wskaźniki (wartości) wzorcowe (benchmarki) wewnętrzne i zewnętrzne, najlepsze praktyki branżowe oraz standardy międzynarodowe.

010.010.010 Prawa i powinności audytu - statut audytu

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Skośne mechanizmy kontrolne SI

ogólne mechanizmy kontrolne zaprojektowane do zarządzania i monitorowania środowiska SI i z tego powodu wpływające na wszystkie działania związane z SI.

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.060 Wpływ skośnych mechanizmów kontrolnych SI

Populacja

cały zbiór danych, z których jest wybierana próbka i o której audytor systemów informatycznych ma zamiar wyciągać wnioski.

060.020.040 Próbkowanie audytowe

060.020.060 Wpływ skośnych mechanizmów kontrolnych SI

Private key

a mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Procedura 1 Ocena ryzyka IS

Dodatek-Słownik/indeks c.d.

Kompetencje zawodowe

Udokumentowany poziom umiejętności, potwierdzony przez odpowiednie organizacje i instytucje oraz zgodność z ustalonymi przez nich standardami i zasadami działania.

Kodeks Etyki Zawodowej

060.020.080 Wykorzystanie prac innych audytorów i ekspertów

Sponsor przedsięwzięcia (projektu)

wziąwszy pod uwagę proces nabywania (zakupów), osoba odpowiedzialna za decyzje na najwyższym szczeblu, takie jak decyzje dotyczące zmiany zakresu i/lub budżetu przedsięwzięcia, a także realizacji wdrożenia.

Zespół realizujący przedsięwzięcie (projekt)

Grupa osób odpowiedzialnych za przedsięwzięcie (projekt), której pole działania może obejmować rozwój, nabywanie, wdrażanie lub utrzymanie aplikacji (systemu aplikacyjnego). W skład zespołu mogą wchodzić członkowie kierownictwa operacyjne (liniowego), pracownicy operacyjni, zewnątrzni podwykonawcy i audytorzy SI.

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

Public key

In an asymmetric cryptographic scheme, the key which may be widely published to enable the operation of the scheme.

Procedura 1 Ocena ryzyka IS

Public key infrastructure

A system which authentically distributes users' public keys using certificates.

Procedura 1 Ocena ryzyka IS

Rozsądne (Względne, Umiarkowane) Zapewnienie (Poświadczenie)

Poziom satysfakcji daleki od (stuprocentowego) zagwarantowania, ale uznany za adekwatny biorąc pod uwagę koszty kontroli i możliwe do uzyskania korzyści.

010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

030.010.010 Nieprawidłowości i akty bezprawne

030.020.010 Rozważania audytowe na temat nieprawidłowości

050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych

050.010.020 Planowanie

050.010.030 Ocena ryzyka podczas planowania audytu

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Procedura 1 Ocena ryzyka IS

Procedura 1 Ocena ryzyka IS

Stosowne (relewantne) dowody audytu

Audit evidence is relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support.

060.020.030 Wymóg dowodów audytu

Wiarygodne dowody audytu

Dowody audytu są wiarygodne, jeśli, w opinii Audytora IT, są one prawdziwe (ważne), oparte na faktach, obiektywne i możliwe do zaakceptowania.

030.020.010 Rozważania audytowe na temat nieprawidłowości

060.020.030 Wymóg dowodów audytu

Residual risk

The risk associated with an event when the controls in place to reduce the effect or likelihood of that event are taken into account.

Procedura 1 Ocena ryzyka IS

Ryzyko

możliwość wystąpienia zdarzenia lub działania, które będzie miało niepożądany wpływ na daną organizację i jej systemy informatyczne

010.010.010 Prawa i powinności audytu - statut audytu

010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI

030.010.010 Nieprawidłowości i akty bezprawne

030.020.010 Rozważania audytowe na temat nieprawidłowości

030.020.010 Rozważania audytowe na temat nieprawidłowości

030.020.020 Należyta staranność zawodowa

050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych

050.010.020 Planowanie

050.010.030 Ocena ryzyka podczas planowania audytu

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

060.020.020 Przegląd systemów aplikacyjnych

060.020.040 Próbkowanie audytowe

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Dodatek-Słownik/indeks c.d.

060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI
060.020.070 Stosowanie technik komputerowego wspomaganie audytu
070.010.010 Raportowanie

Błąd! Nie można odnaleźć źródła odsyłacza.

Procedura 1 Ocena ryzyka IS
Procedura 1 Ocena ryzyka IS

Szacowanie Ryzyka

proces identyfikacji i oceny ryzyk i ich potencjalnych skutków
010.010.010 Prawa i powinności audytu - statut audytu
030.010.010 Nieprawidłowości i akty bezprawne
030.020.010 Rozważania audytowe na temat nieprawidłowości
050.010.020 Planowanie
050.010.030 Ocena ryzyka podczas planowania audytu
060.020.060 Wpływ skrótnych mechanizmów kontrolnych SI

Błąd! Nie można odnaleźć źródła odsyłacza.

Procedura 1 Ocena ryzyka IS
Procedura 1 Ocena ryzyka IS

Ryzyko próbkowania

prawdopodobieństwo, że audytor systemów informatycznych wyciągnął niewłaściwe wnioski dlatego, że nie została przebadana cała populacja, a tylko próbka audytowa. Chociaż ryzyko audytowe może być zredukowane do akceptowalnie niskiego poziomu poprzez użycie odpowiednio wielkiej próbki, to jednak nigdy nie może być wyeliminowane.

060.020.040 Próbkowanie audytowe

Umowa dotycząca Poziomu Usług

określone minimalne miary wydajności na poziomie lub powyżej których dostarczane usługi uznaje się za możliwe do przyjęcia.
010.010.010 Prawa i powinności audytu - statut audytu
010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji
050.010.010 Pojęcie istotności w audytowaniu systemów informatycznych
050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

Usługodawca

organizacja dostarczająca przekazane na zewnątrz usługi.
010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji
050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji

Użytkownik Usług

organizacja korzystająca z przekazanych na zewnątrz usług.
010.010.020 Outsourcing (przekazanie) działań SI do innych organizacji

Smart card

A hardware token that incorporates one or more integrated-circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.
Procedura 1 Ocena ryzyka IS

Testowanie dowodowe

testy szczegółowych działań i transakcji, lub testy polegające na przeglądzie analitycznym, zaprojektowane w celu uzyskania dowodów audytowych odnośnie kompletności, dokładności lub zaistnienia tych działań lub transakcji podczas trwania audytu.
050.010.030 Ocena ryzyka podczas planowania audytu
060.020.030 Wymóg dowodów audytu
060.020.040 Próbkowanie audytowe
Procedura 1 Ocena ryzyka IS

Wystarczające dowody audytu

Dowody audytu są wystarczające, jeśli są kompletne, adekwatne, przekonywujące oraz spowodowałyby, że inny Audytor SI sformułowałby takie same wnioski.
030.020.010 Rozważania audytowe na temat nieprawidłowości
060.020.020 Przegląd systemów aplikacyjnych
060.020.030 Wymóg dowodów audytu

Proces nabywania systemów

Procedury określone w celu nabycia lub zmodernizowania aplikacji, obejmujące ocenę stabilności finansowej dostawcy, wyników jego pracy (osiągnięć), zasobów, a także referencji udzielonych przez innych klientów

Proces Cyklu Rozwoju Systemu

Podejście zastosowane do planowania, projektowania, rozwoju (budowy), testowania i wdrażania aplikacji (systemu aplikacyjnego) lub jej większej modyfikacji.

Specyfikacja warunków działania (zakres uprawnień, działań) – Terms of reference

dokument, który potwierdza zaakceptowanie przez klienta i Audytora SI zlecenia przeprowadzenia przeglądu.
010.010.010 Prawa i powinności audytu - statut audytu

Dodatek-Słownik/indeks c.d.

020.010.010 Wpływ pozaaudytowych zadań na niezależność audytora SI
030.010.010 Nieprawidłowości i akty bezprawne
050.010.020 Planowanie
050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji
060.020.020 Przegląd systemów aplikacyjnych
060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)
060.020.080 Wykorzystanie prac innych audytorów i ekspertów

Dane testowe

Symulowane transakcje służące do testowania poprawności procesów i formuł obliczeniowych oraz do kontroli aktualnie użytkowanych programów. Testowane mogą być poszczególne programy lub całe systemy. Do technik tych zalicza się Integrated Test Facilities (ITFs) – zintegrowany zestaw narzędzi testowych - oraz Base Case System Evaluations (BCSEs).

050.010.020 Planowanie
060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Najwyższe Kierownictwo

Najwyższy poziom kierownictwa w danej organizacji, odpowiedzialny za kierunki działania i kontrolę organizacji jako całości (np. dyrektor, dyrektor generalny, partner, naczelnik, kierownik, dyrektor wykonawczy)

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Trust

Generally, the assumption that an entity will behave substantially as expected. Trust may apply only for a specific function. The key role of this term in an authentication framework is to describe the relationship between an authenticating entity and a certificate authority (CA). An authenticating entity must be certain that it can trust the CA to create only valid and reliable certificates, and users of those certificates rely upon the authenticating entity's determination of trust.

060.020.050 IT Governance - Nadzór nad Technologiami Informatycznymi (IT)

Procedura 1 Ocena ryzyka IS

Użyteczne dowody audytu

Dowody audytu są użyteczne, jeśli pomagają Audytorom IT spełnić ich cele audytów.

060.020.030 Wymóg dowodów audytu
060.020.040 Próbkowanie audytowe
060.020.080 Wykorzystanie prac innych audytorów i ekspertów

Oprogramowanie narzędziowe

Programy komputerowe dostarczone przez wytwórcę sprzętu komputerowego lub przez dostawcę oprogramowania, używane podczas pracy systemu. Techniki te mogą mieć zastosowanie w badaniu aktywności procesów, testowaniu programów, monitorowaniu czynności systemu i procedur operacyjnych, określaniu wykorzystania zbiorów danych oraz analizie danych do rozliczenia zadań.

050.010.040 Wpływ stron trzecich (usługodawców, usługodawców zewnętrznych) na mechanizmy kontrolne IT w organizacji
060.020.070 Stosowanie technik komputerowego wspomaganie audytu

Formularz uwag do standardów ISACA

W naszych nieustających wysiłkach lepszego działania potrzebujemy Twojej opinii na temat standardów
In our continuing efforts to serve you better, your feedback is requested on standards documents.

Twoja odpowiedź może być przekazana e-mailem (research@isaca.org), faksem (+1.847. 253 .1443) albo listownie (Information Systems Audit and Control Association, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008 USA) dyrektorom odpowiedzialnym w kwaterze głównej ISACA za badania, standardy i związki z uczelniami.
Your responses can be returned by e-mail (research@isaca.org), fax (+1.847. 253 .1443) or mail (Information Systems Audit and Control Association, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008 USA) to the ISACA International Headquarters to the attention of the director of research, standards and academic relations.

Prosimy o dołączenie dowolnych komentarzy . O ile to możliwe, to prosimy o zwięzłe komentarze. Prosimy o wskazanie konkretnego numeru paragrafu oraz sugerowanych słów w przypadku rekomendacji dodania lub usunięcia. Prosimy mieć na uwadze, że wskazanie podstaw lub referencji w Twojej opinii pozwoli nam lepiej zrozumieć Twój punkt widzenia.
Please attach any additional comments, typed or legibly written. In commenting please be as concise as possible. When recommending additions or deletions, we ask that you refer to the specific paragraph number to which your comment applies and provide suggested wording where appropriate. Please indicate the basis or rationale for your opinion to help us in understanding your point of reference.

Prosimy o wskazanie tematów (takich jak pilne zagadnienia lub obszary problemowe) lub innych standardów, które Twoim zdaniem byłyby warte rozważenia i pomocne w przyszłości dla Komitetu Standaryzującego.
Please indicate below any topics (such as emerging issues or problem areas) or other bodies' standards that you believe would be helpful for the Standards Board to consider in the future.

Optional Information for Internal Use Only

It is used to acknowledge receipt of your response, clarify any of your comments, and summarise the geographic areas from which comments were received.

Name _____ E-mail, Fax or Phone _____

Organisation _____ Title _____

Address _____ Country _____

Dziękujemy za Twój udział w procesie weryfikacyjnym. Twoje uwagi są nieocenione w pomocy kodyfikowania wytycznych zawodowych przez ISACA.
Thank you for your participation in the exposure process. Your comments are invaluable in helping ISACA codify professional guidance.