

Załącznik Nr 1.9
do uchwały Nr 1626/33a/2025
Krajowej Rady Biegłych Rewidentów
z dnia 21 grudnia 2025 r.

KRAJOWY STANDARD BADANIA 315 (ZMIENIONY W 2019 R.)
w brzmieniu
MIĘDZYNARODOWEGO STANDARDU BADANIA 315 (ZMIENIONEGO W 2019 R.)

IDENTYFIKACJA I OSZACOWANIE RYZYK ISTOTNEGO ZNIEKSZTAŁCENIA

MIĘDZYNARODOWY STANDARD BADANIA 315 (ZMIENIONY W 2019 R.)

IDENTYFIKACJA I OSZACOWANIE RYZYK ISTOTNEGO ZNIEKSZTAŁCENIA

(Stosuje się do badań sprawozdań finansowych za okresy sprawozdawcze
rozpoczynające się 15 grudnia 2021 r. lub później)

SPIS TREŚCI

	Paragraf
Wprowadzenie	
Zakres niniejszego MSB.....	1
Kluczowe pojęcia w niniejszym MSB.....	2-8
Skalowalność	9
Data wejścia w życie	10
Cel	11
Definicje	12
Wymogi	
Procedury oszacowania ryzyka i związane z tym czynności	13–18
Uzyskanie zrozumienia jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej oraz systemu kontroli wewnętrznej jednostki	19–27
Identyfikacja i oszacowanie ryzyk istotnego zniekształcenia	28–37
Dokumentacja	38
Zastosowanie i inny materiał objaśniający	
Definicje.....	A1–A10
Procedury oszacowania ryzyka i związane z tym czynności	A11–A47
Uzyskanie zrozumienia jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej oraz systemu kontroli wewnętrznej jednostki	A48–A183
Identyfikacja i oszacowanie ryzyk istotnego zniekształcenia.....	A184–A236
Dokumentacja.....	A237–A241
Załącznik 1: Rozważania dotyczące zrozumienia jednostki i jej modelu biznesowego	
Załącznik 2: Zrozumienie czynników ryzyka nieodłącznego	
Załącznik 3: Zrozumienie systemu kontroli wewnętrznej jednostki	
Załącznik 4: Rozważania dotyczące zrozumienia funkcji audytu wewnętrznego jednostki	
Załącznik 5: Rozważania dotyczące zrozumienia technologii informacyjnej (IT)	
Załącznik 6: Rozważania dotyczące zrozumienia ogólnych kontroli IT	

Międzynarodowy Standard Badania (MSB) 315 (zmieniony w 2019 r.) *Identyfikacja i oszacowanie ryzyk istotnego zniekształcenia*, należy odczytywać w połączeniu z MSB (PL) 200 *Ogólne cele niezależnego audytora oraz przeprowadzanie badania zgodnie z Międzynarodowymi Standardami Badania*.

Wprowadzenie

Zakres niniejszego MSB

1. Niniejszy Międzynarodowy Standard Badania (MSB) dotyczy odpowiedzialności audytora dotyczącej identyfikacji i oszacowania ryzyk istotnego zniekształcenia sprawozdania finansowego.

Kluczowe pojęcia w niniejszym MSB

2. MSB (PL) 200 dotyczy ogólnych celów audytora podczas przeprowadzania badania sprawozdania finansowego¹, w tym uzyskania wystarczających i odpowiednich dowodów badania, aby zmniejszyć ryzyko badania do akceptowalnie niskiego poziomu². Ryzyko badania jest funkcją ryzyk istotnego zniekształcenia i ryzyka przeoczenia³. MSB (PL) 200 wyjaśnia, że ryzyka istotnego zniekształcenia mogą występować na dwóch poziomach:⁴ na poziomie ogólnym sprawozdania finansowego; oraz na poziomie stwierdzeń dla grup transakcji, sald kont i ujawnień.
3. MSB (PL) 200 wymaga od audytora zastosowania zawodowego osądu podczas planowania i wykonywania badania oraz zaplanowania i wykonania badania z zawodowym sceptycyzmem, uznając, że mogą zaistnieć okoliczności, które powodują, że sprawozdanie finansowe jest istotnie zniekształcone⁵.
4. Ryzyka na poziomie sprawozdania finansowego odnoszą się w sposób rozległy do sprawozdania finansowego jako całości i potencjalnie wpływają na wiele stwierdzeń. Ryzyka istotnego zniekształcenia na poziomie stwierdzeń składają się z dwóch elementów – ryzyka nieodłącznego i ryzyka kontroli:
 - Ryzyko nieodłączne jest określane jako podatność stwierdzeń dotyczących grupy transakcji, salda konta lub ujawnienia na zniekształcenie, które może być istotne, pojedynczo lub w połączeniu z innymi zniekształceniami, przed rozważeniem jakichkolwiek powiązanych kontroli.
 - Ryzyko kontroli jest określane jako ryzyko, że kontrole w jednostce nie zapobiegają lub nie wykryją i nie skorygują w odpowiednim czasie zniekształcenia, które mogłyby wystąpić w stwierdzeniu dotyczącym grupy transakcji, salda konta lub ujawnienia i które mogłyby być istotne, pojedynczo lub w połączeniu z innymi zniekształceniami.
5. MSB (PL) 200 wyjaśnia, że ryzyka istotnego zniekształcenia są szacowane na poziomie stwierdzeń w celu określenia rodzaju, rozłożenia w czasie i zakresu dalszych procedur badania niezbędnych dla uzyskania wystarczających odpowiednich dowodów badania⁶. Dla zidentyfikowanych ryzyk istotnego zniekształcenia na poziomie stwierdzeń, odrębne oszacowanie ryzyka nieodłącznego i ryzyka kontroli jest wymagane przez niniejszy MSB. Stopień różnicowania ryzyka nieodłącznego, jest określany w niniejszym MSB jako „zakres ryzyka nieodłącznego”.
6. Ryzyka istotnego zniekształcenia zidentyfikowane i oszacowane przez audytora obejmują zarówno te wynikające z błędu, jak i te wynikające z oszustwa. Chociaż do obu odnosi się

¹ MSB (PL) 200 *Ogólne cele niezależnego audytora oraz przeprowadzanie badania zgodnie z Międzynarodowymi Standardami Badania.*

² MSB (PL) 200, paragraf 17.

³ MSB (PL) 200, paragraf 13(c).

⁴ MSB (PL) 200, paragraf A37.

⁵ MSB (PL) 200, paragrafy 15-16.

⁶ MSB (PL) 200, paragraf A46 i MSB 330 *Reakcje audytora na oszacowane ryzyka*, paragraf 6.

niniejszy MSB, znaczenie oszustwa jest takie, że w MSB 240⁷ są zawarte dalsze wymogi i wytyczne dotyczące procedur oszacowania ryzyka i związanych z nimi działań w celu uzyskania informacji, które są wykorzystywane do identyfikacji, oszacowania i reakcji na ryzyka istotnego zniekształcenia wynikające z oszustwa.

7. Proces identyfikacji i oszacowania ryzyka przez audytora jest iteratywny i dynamiczny. Zrozumienie jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej oraz systemu kontroli wewnętrznej jednostki przez audytora są współzależne z pojęciami w ramach wymogów, aby zidentyfikować i oszacować ryzyka istotnego zniekształcenia. Podczas uzyskiwania zrozumienia wymaganego przez niniejszy MSB, mogą zostać opracowane wstępne oczekiwania dotyczące ryzyk, które mogą być dalej dopracowywane w miarę postępów audytora w procesie identyfikacji i oszacowania ryzyka. Ponadto, niniejszy MSB oraz MSB 330 wymagają od audytora dokonywania zmian oszacowań ryzyka oraz modyfikowania dalszych ogólnych reakcji i dalszych procedur badania w oparciu o dowody badania uzyskane z wykonania dalszych procedur badania zgodnie z MSB 330 lub jeżeli zostały uzyskane nowe informacje.
8. MSB 330 wymaga, aby audytor zaprojektował i wdrożył ogólne reakcje w odpowiedzi na oszacowane ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego⁸. MSB 330 dalej wyjaśnia, że na oszacowanie ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego przez audytora oraz na ogólne reakcje audytora wpływa zrozumienie przez audytora środowiska kontroli. MSB 330 wymaga również, aby audytor zaprojektował i wykonał dalsze procedury badania, których rodzaj, rozłożenie w czasie i zakres są oparte na oszacowanych ryzykach istotnego zniekształcenia na poziomie stwierdzeń i stanowią reakcję na nie⁹.

Skalowalność

9. MSB (PL) 200 stwierdza, że niektóre MSB zawierają rozważania dotyczące skalowalności, które ilustrują zastosowanie wymogów do wszystkich jednostek, niezależnie od tego, czy ich charakter i okoliczności są mniej złożone, czy bardziej złożone¹⁰. Niniejszy MSB jest przeznaczony do badania wszystkich jednostek, bez względu na ich wielkość lub złożoność, a zatem materiały dotyczące stosowania obejmują tam, gdzie to odpowiednie, szczególne rozważania specyficzne zarówno dla jednostek mniej, jak i bardziej złożonych. Podczas gdy wielkość jednostki może być wskaźnikiem jej złożoności, niektóre mniejsze jednostki mogą być złożone, a niektóre większe jednostki mogą być mniej złożone.

Data wejścia w życie

10. Niniejszy MSB stosuje się do badań sprawozdań finansowych za okresy sprawozdawcze rozpoczynające się 15 grudnia 2021 r. lub później.

Cel

11. Celem audytora jest identyfikacja i oszacowanie ryzyk istotnego zniekształcenia, niezależnie od tego, czy zostało ono spowodowane oszustwem, czy błędem, na poziomach sprawozdania finansowego i stwierdzeń, co zapewnia podstawę do zaprojektowania i wdrożenia reakcji na oszacowane ryzyka istotnego zniekształcenia.

⁷ MSB 240 *Obowiązki audytora podczas badania sprawozdania finansowego dotyczące oszustw*.

⁸ MSB 330, paragraf 5.

⁹ MSB 330, paragraf 6.

¹⁰ MSB (PL) 200, paragraf A69.

Definicje

12. Dla celów MSB następujące pojęcia mają znaczenia przypisane poniżej:

- (a) *Stwierdzenia* – oświadczenia, wyrażone wprost lub w inny sposób, dotyczące ujmowania, wyceny, prezentacji i ujawniania informacji w sprawozdaniu finansowym, które są nieodłączne w oświadczeniu kierownictwa, że sprawozdanie finansowe zostało sporządzone zgodnie z mającymi zastosowanie ramowymi założeniami sprawozdawczości finansowej. Stwierdzenia są wykorzystywane przez audytora, aby rozważyć różne rodzaje potencjalnych zniekształceń, które mogą wystąpić podczas identyfikowania, szacowania i reagowania na ryzyka istotnego zniekształcenia. (Zob. par. A1)
- (b) *Ryzyko biznesowe* – ryzyko wynikające ze znaczących warunków, zdarzeń, okoliczności, działań lub zaniechań, które mogłyby ujemnie wpływać na zdolność jednostki do osiągnięcia jej celów i realizowania jej strategii lub z określenia niewłaściwych celów i strategii.
- (c) *Kontrole* – polityki lub procedury, które jednostka ustanawia, aby osiągnąć cele kontroli kierownictwa lub osób sprawujących nadzór. W tym kontekście: (zob. par. A2–A5)
 - (i) polityki stanowią oświadczenia określające, co powinno, a co nie powinno być robione w jednostce w celu sprawowania kontroli. Takie oświadczenia mogą być udokumentowane, wyraźnie stwierdzone w komunikacjach lub domyślnie wyrażone poprzez działania i decyzje,
 - (ii) procedury są działaniami w celu wdrożenia polityki.
- (d) *Ogólne kontrole technologii informacyjnych (IT)* – kontrole procesów IT jednostki, które wspierają utrzymanie właściwego działania środowiska IT, w tym ciągłe skuteczne funkcjonowanie kontroli przetwarzania informacji oraz integralność informacji (tj. kompletność, dokładność i aktualność informacji) w systemie informacyjnym jednostki. Zobacz również definicję *Środowiska IT*.
- (e) *Kontrole przetwarzania informacji* – kontrole odnoszące się do przetwarzania informacji w aplikacjach IT lub ręcznych procesach informacyjnych w systemie informacyjnym jednostki, które odpowiadają bezpośrednio na ryzyka związane z integralnością informacji (tj. kompletności, dokładności i ważności transakcji i innych informacji). (Zob. par. A6)
- (f) *Czynniki ryzyka nieodłącznego* – cechy zdarzeń lub warunków, które wpływają na podatność na zniekształcenie, niezależnie od tego, czy zostało ono spowodowane oszustwem, czy błędem, stwierdzenia dotyczące grupy transakcji, salda konta lub ujawnienia przed rozważeniem kontroli. Czynniki takie mogą być jakościowe lub ilościowe i obejmują złożoność, subiektywność, zmianę, niepewność lub podatność na zniekształcenie wynikające ze stronniczości kierownictwa lub innych czynników ryzyka oszustwa¹¹, o ile mają one wpływ na ryzyko nieodłączne. (Zob. par. A7–A8)
- (g) *Środowisko IT* – aplikacje IT i wspierająca infrastruktura IT, a także procesy IT i personel zaangażowany w te procesy, które jednostka wykorzystuje w celu wspierania działalności gospodarczej i osiągnięcia strategii gospodarczych. Dla celów niniejszego MSB:
 - (i) aplikacja IT jest programem lub zestawem programów, które są wykorzystywane podczas inicjowania, przetwarzania, rejestrowania i raportowania transakcji lub informacji. Aplikacje IT obejmują hurtownie danych i edytory raportów,
 - (ii) infrastruktura IT składa się z sieci, systemów operacyjnych i baz danych oraz związanego z nimi sprzętu i oprogramowania,

¹¹ MSB 240, paragrafy A24–A27.

- (iii) procesy IT to procesy jednostki służące zarządzaniu dostępem do środowiska IT, zarządzaniu zmianami programów lub zmianami w środowisku IT oraz zarządzaniu operacjami IT.
- (h) *Stosowne stwierdzenia* – stwierdzenie dotyczące grupy transakcji, salda konta lub ujawnienia jest stosowne, gdy odnosi się do zidentyfikowanego ryzyka istotnego zniekształcenia. Ustalenie, czy dane stwierdzenie jest stosownym stwierdzeniem, jest dokonywane przed rozważeniem wszelkich powiązanych kontroli (tj. ryzyko nieodłączne). (Zob. par. A9)
- (i) *Ryzyko powstające z wykorzystania IT* – Podatność kontroli przetwarzania informacji na nieefektywne zaprojektowanie lub działanie, lub ryzyko dla integralności informacji (tj. kompletności, dokładności i aktualności transakcji oraz innych informacji) w systemie informacyjnym jednostki, wynikające z nieefektywnego zaprojektowania lub działania kontroli w procesach IT jednostki (zobacz środowisko IT).
- (j) *Procedury oszacowania ryzyka* – procedury badania zaprojektowane i wykonywane, aby zidentyfikować i oszacować ryzyka istotnego zniekształcenia, niezależnie od tego, czy zostało spowodowane oszustwem, czy błędem, na poziomach sprawozdania finansowego i stwierdzeń.
- (k) *Znacząca grupa transakcji, saldo konta lub ujawnienie* – grupa transakcji, saldo konta lub ujawnienie, w odniesieniu do których występuje jedno lub więcej stosownych stwierdzeń.
- (l) *Znaczące ryzyko* – zidentyfikowane ryzyko istotnego zniekształcenia: (zob. par. A10)
 - (i) w przypadku, którego oszacowanie ryzyka nieodłącznego jest zbliżone do górnej granicy zakresu ryzyka nieodłącznego ze względu na stopień, w jakim czynniki ryzyka nieodłącznego wpływają na połączenie prawdopodobieństwa wystąpienia zniekształcenia i wielkości potencjalnego zniekształcenia w przypadku wystąpienia tego zniekształcenia, lub
 - (ii) które należy to traktować jako znaczące ryzyko zgodnie z wymogami innych MSB¹².
- (m) *System kontroli wewnętrznej* – system zaprojektowany, wdrożony i utrzymywany przez osoby sprawujące nadzór, kierownictwo i innych pracowników, aby zapewnić racjonalną pewność dotyczącą osiągnięcia celów jednostki w odniesieniu do wiarygodności sprawozdawczości finansowej, skuteczności i efektywności działania oraz zgodności z mającymi zastosowanie przepisami prawa i regulacją. Dla celów MSB, system kontroli wewnętrznej składa się z pięciu wzajemnie powiązanych elementów:
 - (i) środowiska kontroli,
 - (ii) procesu oszacowania ryzyka przez jednostkę,
 - (iii) procesu monitorowania systemu kontroli wewnętrznej przez jednostkę,
 - (iv) systemu informacyjnego i komunikacji oraz
 - (v) czynności kontrolnych

Wymogi

Procedury oszacowania ryzyka i związane z tym czynności

¹² MSB 240, paragraf 27 oraz MSB 550 *Strony powiązane*, paragraf 18.

13. Audytor projektuje* i wykonuje procedury oszacowania ryzyka w celu uzyskania dowodów badania, które zapewniają odpowiednią podstawę dla: (zob. par. A11–A18)
 - (a) identyfikacji i oszacowania ryzyk istotnego zniekształcenia, niezależnie od tego, czy zostało ono spowodowane oszustwem, czy błędem, na poziomach sprawozdania finansowego i stwierdzeń, oraz
 - (b) zaprojektowania dalszych procedur badania zgodnie z MSB 330.

Audytor projektuje i wykonuje procedury oszacowania ryzyka w sposób, który nie jest stronniczy w kierunku uzyskiwania dowodów badania, które mogą być potwierdzające lub w kierunku wykluczania dowodów badania, które mogą być sprzeczne. (Zob. par. A14)
14. Procedury oszacowania ryzyka obejmują następujące elementy: (zob. par. A19–A21)
 - (a) zapytania do kierownictwa oraz innych odpowiednich osób w jednostce, w tym osób w funkcji audytu wewnętrznego (jeżeli funkcja taka istnieje), (zob. par. A22–A26)
 - (b) procedury analityczne, (zob. par. A27–A31)
 - (c) obserwacja i inspekcja. (Zob. par. A32–A36)

Informacje z innych źródeł

15. Uzyskując dowody badania zgodnie z paragrafem 13, audytor rozważa informacje pochodzące z: (zob. par. A37–A38)
 - (a) procedur audytora dotyczących akceptacji lub kontynuacji relacji z klientem lub zlecenia badania, oraz
 - (b) gdy ma to zastosowanie, innych zleceń wykonywanych dla jednostki przez partnera odpowiedzialnego za zlecenie.
16. Gdy audytor zamierza wykorzystać informacje uzyskane ze swoich poprzednich doświadczeń z jednostką i z procedur badania wykonanych podczas poprzednich badań, audytor ocenia, czy takie informacje pozostają stosowne i wiarygodne jako dowody badania dla bieżącego badania. (Zob. par. A39–A41)

Dyskusja w ramach zespołu wykonującego zlecenie

17. Partner odpowiedzialny za zlecenie i inni kluczowi członkowie zespołu wykonującego zlecenie omawiają zastosowanie mających zastosowanie ramowych założeń sprawozdawczości finansowej oraz podatność sprawozdania finansowego jednostki na istotne zniekształcenie. (Zob. par. A42–A47)
18. Gdy istnieją członkowie zespołu wykonującego zlecenie nieuczestniczący w dyskusji w ramach zespołu wykonującego zlecenie, partner odpowiedzialny za zlecenie określa, jakie sprawy należy zakomunikować tym członkom.

* *Uw. tłum.* – Stosowane w standardzie w części określającej wymogi sformułowanie *auditor shall + czynność* przetłumaczono na język polski za pomocą czasu teraźniejszego, *audytor wykonuje czynność*, zgodnie z konwencją tłumaczeniową przyjętą w Unii Europejskiej. Niezastosowanie formy nakazowej poprzez użycie słów *musi, ma, powinien* itp. nie zmienia faktu, że wyrażona w ten sposób czynność wskazuje na zobowiązanie audytora do jej wykonania, a zwolnienie od tego wymogu może nastąpić jedynie w sposób przewidziany w standardzie.

Uzyskanie zrozumienia jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej oraz systemu kontroli wewnętrznej jednostki (Zob. par. A48–A49)

Zrozumienie jednostki i jej otoczenia oraz mających zastosowanie ramowych założeń sprawozdawczości finansowej (Zob. par. A50–A55)

19. Audytor wykonuje procedury oszacowania ryzyka, ab uzyskać zrozumienie:

- (a) następujących aspektów jednostki i jej otoczenia:
 - (i) struktury organizacyjnej, struktury właścicielskiej i ładu korporacyjnego jednostki oraz jej modelu biznesowego, w tym zakresu, w jakim model biznesowy włącza wykorzystanie IT, (zob. par. A56–A67)
 - (ii) branżowych, regulacyjnych i innych czynników zewnętrznych (zob. par. A68–A73) oraz
 - (iii) wskaźników wykorzystywanych, wewnątrz i zewnątrz, do oceny wyników finansowych jednostki, (zob. par. A74–A81)
- (b) mających zastosowanie ramowych założeń sprawozdawczości finansowej i zasad (polityk) rachunkowości jednostki oraz przyczyn wszelkich zmian do nich (zob. par. A82–A84) oraz
- (c) w jaki sposób oraz w jakim stopniu czynniki ryzyka nieodłącznego wpływają na podatność stwierdzeń na zniekształcenia podczas sporządzania sprawozdania finansowego zgodnie z mającymi zastosowanie ramowymi założeniami sprawozdawczości finansowej, w oparciu o zrozumienie uzyskane w punktach (a) i (b). (Zob. par. A85–A89)

20. Audytor ocenia, czy zasady (polityki) rachunkowości jednostki są odpowiednie i spójne z mającymi zastosowanie ramowymi założeniami sprawozdawczości finansowej.

Zrozumienie elementów systemu kontroli wewnętrznej jednostki (Zob. par. A90–A95)

Środowisko kontroli, proces oszacowania ryzyka jednostki oraz proces monitorowania systemu kontroli wewnętrznej przez jednostkę (Zob. par. A96–A98)

Środowisko kontroli

21. Audytor uzyskuje zrozumienie środowiska kontroli stosownego dla sporządzania sprawozdania finansowego wykonując procedury oszacowania ryzyka poprzez: (zob. par. A99–A100)	
(a) zrozumienie zestawu kontroli, procesów i struktur, które odnoszą się do: (zob. par. A101–A102) (i) sposobu, w jaki wykonywane są obowiązki nadzorcze kierownictwa, takie jak kultura jednostki oraz zobowiązanie kierownictwa do uczciwości i wartości etycznych, (ii) gdy osoby sprawujące nadzór są oddzielone od kierownictwa, niezależności i nadzoru nad systemem kontroli wewnętrznej jednostki przez osoby sprawujące nadzór, (iii) przydzielenia uprawnień i odpowiedzialności w jednostce,	i (b) dokonanie oceny, czy: (zob. par. A103–A108) (i) kierownictwo, pod nadzorem osób sprawujących nadzór, stworzyło i utrzymało kulturę uczciwości i etycznego zachowania, (ii) środowisko kontroli zapewnia odpowiednią podstawę dla innych elementów systemu kontroli wewnętrznej jednostki, biorąc pod uwagę charakter i złożoność jednostki, oraz (iii) słabości kontroli zidentyfikowane w środowisku kontroli osłabiają inne

(iv) sposobu, w jaki jednostka przyciąga, rozwija i zatrzymuje kompetentne osoby, oraz (v) sposobu, w jaki jednostka rozlicza osoby odpowiedzialne z ich odpowiedzialności za realizację celów systemu kontroli wewnętrznej.	elementy systemu kontroli wewnętrznej jednostki.
--	---

Proces oszacowania ryzyka przez jednostkę

22. Audytor uzyskuje zrozumienie procesu oszacowania ryzyka przez jednostkę stosownego dla sporządzania sprawozdania finansowego wykonując procedury oszacowania ryzyka poprzez:	
(a) zrozumienie procesu jednostki dla: (zob. par. A109–A110) (i) identyfikowania ryzyk gospodarczych stosownych dla celów sprawozdawczości finansowej, (zob. par. A62) (ii) oszacowania znaczenia tych ryzyk, w tym prawdopodobieństwa ich wystąpienia oraz (iii) reakcji na te ryzyka,	i (b) dokonanie oceny, czy proces oszacowania ryzyka przez jednostkę jest odpowiedni do okoliczności jednostki, biorąc pod uwagę charakter i złożoność jednostki. (Zob. par. A111–A113)

23. Jeżeli audytor identyfikuje ryzyka istotnego zniekształcenia, których kierownictwo nie zidentyfikowało, audytor:

- (a) określa, czy którekolwiek z takich ryzyk jest tego rodzaju, iż audytor oczekuje, że zostałyby zidentyfikowane w procesie oszacowania ryzyka przez jednostkę, i jeżeli tak, to uzyskuje zrozumienie, dlaczego proces oszacowania ryzyka w jednostce nie zidentyfikował takich ryzyk istotnego zniekształcenia, oraz
- (b) rozważa konsekwencje dla oceny audytora, o której mowa w paragrafie 22(b).

Proces monitorowania systemu kontroli wewnętrznej przez jednostkę

24. Audytor uzyskuje zrozumienie procesu monitorowania systemu kontroli wewnętrznej przez jednostkę stosownego dla sporządzania sprawozdania finansowego wykonując procedury oszacowania ryzyka, poprzez: (zob. par. A114–A115)	
(a) zrozumienie tych aspektów procesu jednostki, które odnoszą się do: (i) ciągłych i odrębnych ocen w celu monitorowania skuteczności kontroli oraz identyfikacji i korygowania zidentyfikowanych słabości kontroli, (zob. par. A116–A117) oraz (ii) funkcji audytu wewnętrznego jednostki, jeżeli jakakolwiek istnieje, w tym jej charakteru, obowiązków i działań, (zob. par. A118)	i (c) dokonanie oceny czy proces monitorowania systemu kontroli wewnętrznej przez jednostkę jest odpowiedni do okoliczności jednostki, biorąc pod uwagę charakter i złożoność jednostki. (Zob. par. A121–A122)

(b) zrozumienie źródeł informacji wykorzystywanych w procesie monitorowania systemu kontroli wewnętrznej w jednostce oraz podstaw uznawania przez kierownictwo informacji za wystarczająco wiarygodne dla danego celu, (zob. par. A119–A120)	
---	--

System informacyjny i komunikacja oraz czynności kontrolne (Zob. par. A123–A130)

System informacyjny i komunikacja

25. Audytor uzyskuje zrozumienie systemu informacyjnego i komunikacji jednostki stosownych dla sporządzania sprawozdania finansowego wykonując procedury oszacowania ryzyka, poprzez: (zob. par. A131)	
(a) zrozumienie działań jednostki w zakresie przetwarzania informacji, w tym jej danych i informacji, zasobów do wykorzystania podczas takich działań oraz polityk określających, dla znaczących grup transakcji, sald kont i ujawnień: (zob. par. A132–A143) (i) w jaki sposób informacje przepływają przez system informacyjny jednostki, w tym jak: a. transakcje są inicjowane i w jaki sposób informacje o nich są rejestrowane, przetwarzane, w razie potrzeby poprawiane, włączane do księgi głównej i raportowane w sprawozdaniu finansowym, oraz b. informacje o zdarzeniach i warunkach, innych niż transakcje, są ujmowane, przetwarzane i ujawniane w sprawozdaniu finansowym, (ii) zapisy księgowe, poszczególne konta w sprawozdaniu finansowym oraz inne zapisy pomocnicze odnoszące się do przepływu informacji w systemie informacyjnym, (iii) proces sprawozdawczości finansowej wykorzystywany do sporządzania sprawozdania finansowego jednostki, w tym ujawnień oraz (iv) zasoby jednostki, w tym środowisko IT, stosowne dla powyższych punktów (a)(i) do (a)(iii),	i (c) dokonanie oceny czy system informacyjny i komunikacja jednostki odpowiednio wspierają sporządzanie sprawozdania finansowego jednostki zgodnie z mającymi zastosowanie ramowymi założeniami sprawozdawczości finansowej. (Zob. par. A146)

(b) zrozumienie, w jaki sposób jednostka komunikuje znaczące sprawy, które wspomagają sporządzanie sprawozdania finansowego i związane z tym obowiązki sprawozdawcze w systemie informacyjnym oraz inne elementy systemu kontroli wewnętrznej: (zob. par. A144–A145) (i) pomiędzy osobami w jednostce, w tym w jaki sposób komunikowane są role i obowiązki w zakresie sprawozdawczości finansowej, (ii) pomiędzy kierownictwem, a osobami sprawującymi nadzór oraz (iii) ze stronami zewnętrznymi, takimi jak te z organami regulacyjnymi.	
---	--

Czynności kontrolne.

26. Audytor uzyskuje zrozumienie elementu czynności kontrolnych wykonując procedury oszacowania ryzyka, poprzez: (zob. par. A147–A157)	
(a) identyfikowanie kontroli, które odnoszą się do ryzyk istotnego zniekształcenia na poziomie stwierdzeń w elemencie czynności kontrolnych, w następujący sposób: (i) kontrole, które odnoszą się do ryzyka określonego jako będące znaczącym ryzykiem, (zob. par. A158–A159) (ii) kontrole dotyczące zapisów dziennika, w tym nietypowych zapisów dziennika używanych do rejestrowania niepowtarzalnych, nietypowych transakcji lub korekt, (zob. par. A160–A161) (iii) kontrole, których skuteczność działania audytor planuje przetestować podczas określania rodzaju, rozłożenia w czasie i zakresu testów wiarygodności, które obejmują kontrole odnoszące się do ryzyk, dla których same procedury wiarygodności nie dostarczają wystarczających odpowiednich dowodów badania, oraz (zob. par. A162–A164) (iv) inne kontrole, które audytor uznaje za odpowiednie, aby umożliwić audytorowi osiągnięcie celów	i (d) dla każdej kontroli zidentyfikowanej w punktach (a) lub (c)(ii): (zob. par. A175–A181) (i) dokonanie oceny czy kontrola została zaprojektowana skutecznie, aby odpowiedzieć na ryzyko istotnego zniekształcenia na poziomie stwierdzeń lub czy została skutecznie zaprojektowana, aby wspierać działanie innych kontroli, oraz (ii) określenie czy kontrola została wdrożona poprzez wykonanie dodatkowych procedur, poza zapytaniem personelu jednostki.

określonych w paragrafie 13 w odniesieniu do ryzyk na poziomie stwierdzeń, na podstawie zawodowego osądu audytora, (zob. par. A165)	
(b) na podstawie kontroli zidentyfikowanych w punkcie (a), identyfikację aplikacji IT i innych aspektów środowiska IT jednostki, które podlegają ryzykom powstającym z wykorzystania IT, (zob. par. A166–A172)	
(c) dla takich aplikacji IT i innych aspektów środowiska IT zidentyfikowanych w punkcie (b), identyfikację: (zob. par. A173–A174)	
(i) powiązanych ryzyk powstających z wykorzystania IT oraz	
(ii) ogólnych kontroli IT jednostki, które odnoszą się do takich ryzyk,	

Słabości kontroli w systemie kontroli wewnętrznej jednostki

27. Na podstawie dokonanej przez audytora oceny każdego z elementów systemu kontroli wewnętrznej jednostki, audytor ustala, czy zidentyfikowano jedną lub wiele słabości kontroli. (Zob. par. A182–A183)

Identyfikacja i oszacowanie ryzyk istotnego zniekształcenia (Zob. par. A184–A185)

Identyfikacja ryzyk istotnego zniekształcenia

28. Audytor identyfikuje ryzyka istotnego zniekształcenia i określa, czy istnieją one: (zob. par. A186–A192)
- (a) na poziomie sprawozdania finansowego, (zob. par. A193–A200) lub
 - (b) na poziomie stwierdzeń dla grup transakcji, sald kont i ujawnień. (Zob. par. A201)
29. Audytor określa stosowne stwierdzenia i związane z nimi znaczące grupy transakcji, salda kont i ujawnienia. (Zob. par. A202–A204)

Oszacowanie ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego

30. Dla zidentyfikowanych ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego audytor dokonuje oszacowania ryzyk oraz: (zob. par. A193–A200)
- (a) określa, czy takie ryzyka wpływają na oszacowanie ryzyk na poziomie stwierdzeń oraz
 - (b) ocenia charakter i zakres ich rozległego wpływu na sprawozdanie finansowe.

Oszacowanie ryzyk istotnego zniekształcenia na poziomie stwierdzeń

Oszacowanie ryzyka nieodłącznego (Zob. par. A205–A217)

31. Dla zidentyfikowanych ryzyk istotnego zniekształcenia na poziomie stwierdzeń, audytor dokonuje oszacowania ryzyka nieodłącznego poprzez ocenę prawdopodobieństwa wystąpienia

i wielkości zniekształcenia. Postępując w ten sposób, audytor bierze pod uwagę sposób i stopień, w jakim:

- (a) czynniki ryzyka nieodłącznego wpływają na podatność stosownych stwierdzeń na zniekształcenia oraz
 - (b) ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego wpływają na oszacowanie ryzyka nieodłącznego dla ryzyk istotnego zniekształcenia na poziomie stwierdzeń. (Zob. par. A215–A216)
32. Audytor ustala, czy którekolwiek z oszacowanych ryzyk istotnego zniekształcenia są ryzykami znaczącymi. (Zob. par. A218–A221)
33. Audytor ustala, czy same procedury wiarygodności nie mogą dostarczyć wystarczających odpowiednich dowodów badania w odniesieniu do jakichkolwiek ryzyk istotnego zniekształcenia na poziomie stwierdzeń. (Zob. par. A222–A225)

Oszacowanie ryzyka kontroli

34. Jeżeli audytor planuje testować operacyjną skuteczności kontroli, dokonuje on oszacowania ryzyka kontroli. Jeżeli audytor nie planuje testować operacyjnej skuteczności kontroli, jego oszacowanie ryzyka kontroli jest takie, że oszacowanie ryzyka istotnego zniekształcenia jest identyczne, jak oszacowanie ryzyka nieodłącznego. (Zob. par. A226–A229)

Ocena dowodów badania uzyskanych w ramach procedur oszacowania ryzyka

35. Audytor ocenia, czy dowody badania uzyskane w ramach procedur oszacowania ryzyka zapewniają odpowiednią podstawę do identyfikacji i oszacowania ryzyk istotnego zniekształcenia. Jeżeli nie, audytor wykonuje dodatkowe procedury oszacowania ryzyka do czasu uzyskania dowodów badania zapewniających taką podstawę. Identyfikując i dokonując oszacowania ryzyk istotnego zniekształcenia, audytor bierze pod uwagę wszystkie dowody badania uzyskane w ramach procedur oszacowania ryzyka, niezależnie od tego, czy są one potwierdzające stwierdzenia kierownictwa, czy sprzeczne z nimi. (Zob. par. A230–A232)

Grupy transakcji, salda kont i ujawnienia, które nie są znaczące, ale są istotne

36. Dla istotnych grup transakcji, sald kont lub ujawnień, które nie zostały określone jako będące znaczącymi grupami transakcji, saldami kont lub ujawnieniami, audytor ocenia, czy ustalenie audytora pozostaje odpowiednie. (Zob. par. A233–A235)

Weryfikacja oszacowania ryzyka

37. Jeżeli audytor uzyskuje nowe informacje, które są niespójne z dowodami badania, na których audytor pierwotnie oparł identyfikację lub oszacowanie ryzyk istotnego zniekształcenia, audytor weryfikuje taką identyfikację lub oszacowanie. (Zob. par. A236)

Dokumentacja

38. Audytor włącza do dokumentacji badania¹³: (zob. par. A237–A241)
- (a) omówienie w gronie zespołu wykonującego zlecenie oraz podjęte znaczące decyzje,

¹³ MSB 230 *Dokumentacja badania*, paragrafy 8-11 i A6-A7.

- (b) kluczowe elementy zrozumienia przez audytora zgodnie z paragrafami 19, 21, 22, 24 i 25; źródła informacji, z których zrozumienie przez audytora zostało uzyskane; oraz wykonane procedury oszacowania ryzyka,
- (c) ocenę zaprojektowania zidentyfikowanych kontroli oraz ustalenie, czy takie kontrole zostały wdrożone, zgodnie z wymogami określonymi w paragrafie 26, oraz
- (d) zidentyfikowane i oszacowane ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego oraz na poziomie stwierdzeń, w tym znaczące ryzyka i ryzyka, dla których same procedury wiarygodności nie są w stanie zapewnić wystarczających odpowiednich dowodów badania, a także uzasadnienie dla dokonanych znaczących osądów.

Zastosowanie i inny materiał objaśniający

Definicje (Zob. par. 12)

Stwierdzenia (Zob. par. 12(a))

- A1. Kategorie stwierdzeń są wykorzystywane przez audytorów do rozważenia różnych rodzajów potencjalnych zniekształceń, które mogą wystąpić podczas identyfikowania, oszacowania i reagowania na ryzyka istotnego zniekształcenia. Przykłady tych kategorii stwierdzeń są opisane w paragrafie A190. Stwierdzenia te różnią się od pisemnych oświadczeń wymaganych przez MSB 580¹⁴, które mają na celu potwierdzenie pewnych spraw lub wsparcie innych dowodów badania.

Kontrole (Zob. par. 12(c))

- A2. Kontrole są wbudowane w elementy systemu kontroli wewnętrznej jednostki.
- A3. Polityki są wdrażane poprzez działania personelu w jednostce lub poprzez powstrzymywanie personelu od podejmowania działań, które byłyby sprzeczne z takimi politykami.
- A4. Procedury mogą być nakazane poprzez formalną dokumentację lub inne komunikowanie przez kierownictwo lub osoby sprawujące nadzór lub mogą wynikać z zachowań, które nie są nakazane, ale raczej są uwarunkowane przez kulturę jednostki. Procedury mogą być egzekwowane poprzez działania dozwolone przez aplikacje IT wykorzystywane przez jednostkę lub inne aspekty środowiska IT jednostki.
- A5. Kontrole mogą być bezpośrednie lub pośrednie. Kontrole bezpośrednie to kontrole, które są wystarczająco precyzyjne, aby odnosić się do ryzyk istotnego zniekształcenia na poziomie stwierdzeń. Kontrole pośrednie to kontrole, które wspierają kontrole bezpośrednie.

Kontrole przetwarzania informacji (Zob. par. 12(e))

- A6. Ryzyka dla integralności informacji powstają z względu na podatność na nieefektywne wdrażanie polityk informacyjnych jednostki, które są politykami określającymi przepływy informacji, zapisy i procesy sprawozdawczości w systemie informacyjnym jednostki. Kontrole przetwarzania informacji są procedurami, które wspierają skuteczne wdrożenie polityk informacyjnych jednostki. Kontrole przetwarzania informacji mogą być zautomatyzowane (tj. wbudowane

¹⁴ MSB 580 *Pisemne oświadczenia*.

w aplikacje IT) lub ręczne (np. kontrole wejścia lub wyjścia) i mogą opierać się na innych kontrolach, w tym na innych kontrolach przetwarzania informacji lub ogólnych kontrolach IT.

Czynniki ryzyka nieodłącznego (Zob. par. 12(f))

Załącznik 2 przedstawia dalsze rozważania związane ze zrozumieniem czynników ryzyka nieodłącznego.

- A7. Czynniki ryzyka nieodłącznego mogą mieć charakter jakościowy lub ilościowy i mogą wpływać na podatność stwierdzeń na zniekształcenie. Jakościowe czynniki ryzyka nieodłącznego związane ze sporządzeniem informacji wymaganych przez mające zastosowanie ramowe założenia sprawozdawczości finansowej obejmują:
- złożoność,
 - subiektywizm,
 - zmianę,
 - niepewność lub
 - podatność na zniekształcenie spowodowane stronniczością kierownictwa lub innymi czynnikami ryzyka oszustwa, o ile mają one wpływ na ryzyko nieodłączne.
- A8. Inne czynniki ryzyka nieodłącznego, które wpływają na podatność na zniekształcenie stwierdzeń o danej grupie transakcji, saldzie konta lub ujawnieniu mogą obejmować:
- ilościowe lub jakościowe znaczenie grupy transakcji, salda konta lub ujawnienia, lub
 - wielkość lub brak jednolitości w składzie pozycji, które mają być przetwarzane w ramach danej grupy transakcji lub salda konta, lub które mają być odzwierciedlone w ujawnieniu.

Stosowne stwierdzenia (Zob. par. 12(h))

- A9. Ryzyko istotnego zniekształcenia może odnosić się do więcej niż jednego stwierdzenia i w takim przypadku wszystkie stwierdzenia, do których odnosi się takie ryzyko, są stosownymi stwierdzeniami. Jeżeli stwierdzenie nie wiąże się ze zidentyfikowanym ryzykiem istotnego zniekształcenia, to nie jest to stosowne stwierdzenie.

Znaczące ryzyko (Zob. par. 12(l))

- A10. Znaczenie może być opisane jako względna ważność sprawy i jest oceniane przez audytora w kontekście, w którym sprawa jest rozważana. Dla ryzyka nieodłącznego, znaczenie może być rozważane w kontekście sposobu i stopnia, w jakim czynniki ryzyka nieodłącznego wpływają na połączenie prawdopodobieństwa wystąpienia zniekształcenia i wielkości potencjalnego zniekształcenia w przypadku wystąpienia tego zniekształcenia.

Procedury oszacowania ryzyka i związane z tym czynności (Zob. par. 13–18)

- A11. Ryzyka istotnego zniekształcenia, które należy zidentyfikować i oszacować, obejmują zarówno te wynikające z oszustwa, jak i te wynikające z błędu, i oba są objęte niniejszym MSB. Jednakże, znaczenie oszustwa jest takie, że w MSB 240 zawarte zostały dalsze wymogi i wytyczne dotyczące procedur oszacowania ryzyka i związanych z nimi działań mających na celu uzyskanie informacji, które są wykorzystywane w celu identyfikacji i oszacowania ryzyka istotnego zniekształcenia spowodowanego oszustwem¹⁵. Ponadto, poniższe MSB dostarczają dalszych

¹⁵ MSB 240, paragrafy 12-27.

wymogów i wytycznych dotyczących identyfikowania i szacowania ryzyk istotnego zniekształcenia w odniesieniu do poszczególnych spraw lub okoliczności:

- MSB 540 (zmieniony)¹⁶ w odniesieniu do szacunków księgowych,
- MSB 550 w odniesieniu do powiązań i transakcji z podmiotami powiązanymi,
- MSB 570 (zmieniony)¹⁷ w odniesieniu do kontynuacji działalności oraz
- MSB 600 (zmieniony)¹⁸ w odniesieniu do sprawozdania finansowego grupy.

A12. Zawodowy sceptycyzm jest niezbędny do krytycznej oceny dowodów badania zebranych podczas wykonywania procedur oszacowania ryzyka i pomaga audytorowi w zachowaniu czujności w odniesieniu do dowodów badania, aby nie były stronnice w kierunku potwierdzania istnienia ryzyk, lub które mogą być sprzeczne z występowaniem ryzyk. Zawodowy sceptycyzm jest postawą przyjmowaną przez audytora podczas dokonywania zawodowych osądów, które następnie zapewniają podstawę działań audytora. Audytor stosuje zawodowy osąd podczas ustalania, czy audytor dysponuje dowodami badania, które zapewniają odpowiednią podstawę dla oszacowania ryzyka.

A13. Stosowanie zawodowego sceptycyzmu przez audytora może obejmować:

- kwestionowanie sprzecznych informacji i wiarygodności dokumentów,
- rozważenie reakcji na zapytania i inne informacje uzyskane od kierownictwa i osób sprawujących nadzór,
- zachowanie czujności w odniesieniu do warunków, które mogą wskazywać na możliwe zniekształcenie spowodowane oszustwem lub błędem, oraz
- rozważenie, czy uzyskane dowody badania wspierają identyfikację i oszacowanie przez audytora ryzyk istotnego zniekształcenia w świetle charakteru jednostki i okoliczności.

Dlaczego ważne jest uzyskanie dowodów badania w sposób bezstronny (Zob. par. 13)

A14. Zaprojektowanie i wykonanie procedur oszacowania ryzyka, aby uzyskać dowody badania wspierające identyfikację i oszacowanie ryzyk istotnego zniekształcenia w sposób bezstronny może pomóc audytorowi w identyfikowaniu potencjalnie sprzecznych informacji, co może pomóc audytorowi w zastosowaniu zawodowego sceptycyzmu podczas identyfikowania i oszacowania ryzyk istotnego zniekształcenia.

Źródła dowodów badania (Zob. par. 13)

A15. Projektowanie i wykonywanie procedur oszacowania ryzyka, aby uzyskać dowody badania w sposób bezstronny może obejmować uzyskiwanie dowodów z wielu źródeł wewnątrz jednostki i poza jednostką. Od audytora nie jest jednak wymagane wykonywanie wyczerpujących poszukiwań w celu identyfikacji wszystkich możliwych źródeł dowodów badania. Oprócz

¹⁶ MSB 540 (zmieniony) *Badanie szacunków księgowych i powiązanych ujawnień.*

¹⁷ MSB 570 (zmieniony) *Kontynuacja działalności.*

¹⁸ MSB 600 (zmieniony) *Szczególne rozważania – badania sprawozdań finansowych grupy (w tym praca audytorów części składowych grupy).*

informacji z innych źródeł¹⁹, źródła informacji dla procedur oszacowania ryzyka mogą obejmować:

- interakcje z kierownictwem, osobami sprawującymi nadzór i innymi kluczowymi pracownikami jednostki, takimi jak audytorzy wewnętrzni,
- pewne strony trzecie, takie jak regulatorzy, niezależnie od tego, czy informacje zostały uzyskane bezpośrednio, czy pośrednio,
- publicznie dostępne informacje o jednostce, na przykład komunikaty prasowe wydane przez jednostkę, materiały dla analityków lub spotkania grupy inwestorów, raporty analityków lub informacje o działalności handlowej.

Bez względu na źródło informacji, audytor rozważa stosowność i wiarygodność informacji, które mają zostać wykorzystane jako dowody badania zgodnie z MSB 500²⁰.

Skalowalność (Zob. par. 13)

- A16. Rodzaj i zakres procedur oszacowania ryzyka będą się różnić w zależności od charakteru i okoliczności jednostki (np. sformalizowania polityk i procedur oraz procesów i systemów jednostki). Audytor wykorzystuje zawodowy osąd, aby określić rodzaj i zakres procedur oszacowania ryzyka, które mają zostać wykonane, aby spełnić wymogi niniejszego MSB.
- A17. Pomimo, że zakres, w jakim polityki i procedury oraz procesy i systemy jednostki są sformalizowane, może być różny, od audytora nadal wymagane jest, aby uzyskać zrozumienie zgodnie z paragrafami 19, 21, 22, 24, 25 i 26.

Przykłady:

Niektóre jednostki, w tym jednostki mniej złożone, a w szczególności jednostki zarządzane przez właściciela, mogły nie ustanowić ustrukturyzowanych procesów i systemów (np. procesu oszacowania ryzyka lub procesu monitorowania systemu kontroli wewnętrznej) lub mogły ustanowić procesy lub systemy o ograniczonej dokumentacji lub braku spójności w sposobie ich realizacji. Gdy takie systemy i procesy nie są sformalizowane, audytor może nadal być w stanie wykonywać procedury oszacowania ryzyka poprzez obserwację i zapytanie.

Od innych jednostek, zazwyczaj bardziej złożonych jednostek, oczekiwane jest, że będą miały bardziej sformalizowane i udokumentowane polityki i procedury. Audytor może korzystać z takiej dokumentacji podczas wykonywania procedur oszacowania ryzyka.

- A18. Rodzaj i zakres procedur oszacowania ryzyka, które mają zostać wykonane podczas podjęcia się zlecenia po raz pierwszy, może być bardziej rozległy niż procedury dla zlecenia powtarzalnego. W kolejnych okresach audytor może skupić się na zmianach, jakie nastąpiły od poprzedniego okresu.

Rodzaje procedur oszacowania ryzyka (Zob. par. 14)

- A19. MSB 500²¹ wyjaśnia rodzaje procedur badania, które mogą być wykonane podczas uzyskiwania dowodów badania z procedur oszacowania ryzyka i dalszych procedur badania. Na rodzaj, rozłożenie w czasie i zakres procedur badania może mieć wpływ fakt, że niektóre dane księgowe i inne dowody mogą być dostępne tylko w formie elektronicznej lub tylko w pewnych momentach

¹⁹ Zobacz paragrafy A37 i A38.

²⁰ MSB 500 *Dowody badania*, paragraf 7.

²¹ MSB 500, paragrafy A14–A17 i A21–A25.

w czasie²². Audytor może wykonać procedury wiarygodności lub testy kontroli, zgodnie z MSB 330, równoległe z procedurami oszacowania ryzyka, gdy jest to efektywne. Uzyskane dowody badania, które wspierają identyfikację i oszacowanie ryzyk istotnego zniekształcenia, mogą również wspierać wykrywanie zniekształceń na poziomie stwierdzeń lub w ocenę skuteczności działania kontroli.

- A20. Pomimo, że od audytora wymagane jest wykonanie wszystkich procedur oszacowania ryzyka opisanych w paragrafie 14 w trakcie uzyskiwania wymaganego zrozumienia jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej oraz systemu kontroli wewnętrznej jednostki (zobacz paragrafy 19-26), od audytora nie jest wymagane wykonanie wszystkich z nich dla każdego aspektu tego zrozumienia. Inne procedury mogą być wykonywane, gdy informacje, które mają zostać uzyskane, mogą być pomocne w identyfikowaniu ryzyk istotnego zniekształcenia. Przykłady takich procedur mogą obejmować kierowanie zapytań do zewnętrznego doradcy prawnego jednostki lub zewnętrznych organów nadzoru, lub do ekspertów w zakresie wyceny, z których usług jednostka korzystała.

Zautomatyzowane narzędzia i techniki (Zob. par. 14)

- A21. Wykorzystując zautomatyzowane narzędzia i techniki, audytor może wykonać procedury oszacowania ryzyka w odniesieniu do dużych ilości danych (z księgi głównej, ksiąg pomocniczych lub innych danych operacyjnych), w tym do analizy, ponownych obliczeń, ponownego wykonania lub uzgodnień.

Zapytania do kierownictwa i innych osób w jednostce (Zob. par. 14(a))

Dlaczego zapytania kierowane są do kierownictwa i innych osób w jednostce

- A22. Informacje uzyskane przez audytora w celu wsparcia odpowiedniej podstawy identyfikacji i oszacowania ryzyk oraz zaprojektowania dalszych procedur badania, mogą zostać uzyskane poprzez zapytania kierowane do kierownictwa i osób odpowiedzialnych za sprawozdawczość finansową.
- A23. Zapytania kierowane do kierownictwa i osób odpowiedzialnych za sprawozdawczość finansową oraz innych odpowiednich osób w jednostce i innych pracowników o różnych poziomach uprawnień mogą zaoferować audytorowi różne perspektywy podczas identyfikowania i oszacowania ryzyk istotnego zniekształcenia.

²² MSB 500, paragraf A16.

Przykłady:

- Zapytania kierowane do osób sprawujących nadzór mogą pomóc audytorowi zrozumieć zakres nadzoru sprawowanego przez osoby sprawujące nadzór nad sporządzaniem sprawozdania finansowego przez kierownictwo. MSB 260 (zmieniony)²³ identyfikuje znaczenie skutecznej dwustronnej komunikacji we wspomaganiu audytora w uzyskaniu informacji od osób sprawujących nadzór w tym zakresie.
- Zapytania kierowane do pracowników odpowiedzialnych za inicjowanie, przetwarzanie lub rejestrowanie złożonych lub nietypowych transakcji mogą pomóc audytorowi ocenić prawidłowość doboru i zastosowania pewnych zasad (polityk) rachunkowości.
- Zapytania kierowane do doradców prawnych wewnątrz jednostki mogą dostarczyć informacji na temat takich zagadnień, jak: spory sądowe, zgodność z przepisami prawa i regulacją, wiedza o oszustwach lub podejrzewanych oszustwach wpływających na jednostkę, gwarancje, zobowiązania posprzedażne, porozumienia (takie jak wspólne przedsięwzięcia) z partnerami biznesowymi oraz znaczenie warunków umownych.
- Zapytania kierowane do personelu ds. marketingu lub sprzedaży mogą dostarczać informacji o zmianach w strategiach marketingowych jednostki, trendach sprzedaży lub ustaleniach umownych z jej odbiorcami.
- Zapytania kierowane do funkcji zarządzania ryzykiem (lub zapytania kierowane do osób wykonujących takie role) mogą dostarczyć informacji o ryzykach operacyjnych i regulacyjnych, które mogą wpływać na sprawozdawczość finansową.
- Zapytania kierowane do personelu związanego z IT mogą dostarczyć informacji o zmianach systemu, niedociągnięciach systemu lub kontroli, lub o innych ryzykach związanych z IT.

Szczególne rozważania dla jednostek sektora publicznego

A24. Kierując zapytania do osób mogących posiadać informacje, które prawdopodobnie pomogą w identyfikowaniu ryzyk istotnego zniekształcenia, audytorzy jednostek sektora publicznego mogą uzyskać informacje z dodatkowych źródeł, takich jak audytorzy, którzy są zaangażowani w audyty działalności lub inne badania związane z daną jednostką.

Zapytania kierowane do funkcji audytu wewnętrznego

Załącznik 4 przedstawia rozważania dotyczące zrozumienia funkcji audytu wewnętrznego jednostki.

Dlaczego do funkcji audytu wewnętrznego kierowane są zapytania (jeżeli funkcja ta istnieje)

A25. Jeżeli jednostka posiada funkcję audytu wewnętrznego, zapytania kierowane do odpowiednich osób wewnątrz tej funkcji mogą pomóc audytorowi w zrozumieniu jednostki i jej otoczenia oraz systemu kontroli wewnętrznej jednostki, w identyfikacji i oszacowaniu ryzyk.

Szczególne rozważania dla jednostek sektora publicznego

A26. Audytorzy jednostek sektora publicznego często mają dodatkowe obowiązki w odniesieniu do kontroli wewnętrznej oraz zgodności z mającymi zastosowanie przepisami prawa i regulacją. Zapytania kierowane do odpowiednich osób z funkcji audytu wewnętrznego mogą pomóc

²³ MSB 260 (zmieniony) *Komunikowanie się z osobami sprawującymi nadzór*, paragraf 4(b).

audytorom w identyfikowaniu ryzyka istotnej niezgodności z mającymi zastosowanie przepisami prawa i regulacją oraz ryzyka słabości kontroli związanych ze sprawozdawczością finansową.

Procedury analityczne (Zob. par. 14(b))

Dlaczego procedury analityczne są wykonywane jako procedury oszacowania ryzyka

A27. Procedury analityczne pomagają identyfikować niespójności, nietypowe transakcje lub zdarzenia oraz kwoty, wskaźniki i trendy, które wskazują na sprawy, które mogą mieć wpływ na badanie. Nietypowe lub nieoczekiwane powiązania, które zostają zidentyfikowane, mogą pomóc audytorowi w identyfikowaniu ryzyk istotnego zniekształcenia, w szczególności ryzyk istotnego zniekształcenia spowodowanych oszustwem.

A28. Procedury analityczne wykonywane jako procedury oszacowania ryzyka mogą zatem pomóc w identyfikowaniu i oszacowaniu ryzyk istotnego zniekształcenia poprzez zidentyfikowanie aspektów jednostki, których audytor nie był świadomy lub zrozumienie, w jaki sposób czynniki ryzyka nieodłącznego, takie jak zmiana, wpływają na podatność stwierdzeń na zniekształcenia.

Rodzaje procedur analitycznych

A29. Procedury analityczne wykonywane jako procedury oszacowania ryzyka mogą:

- obejmować zarówno informacje finansowe, jak i niefinansowe, na przykład, powiązania między sprzedażą a metrażem powierzchni handlowych lub ilością sprzedanych towarów (niefinansowe),
- wykorzystywać dane zagregowane na wysokim poziomie. W związku z tym, wyniki tych procedur analitycznych mogą dostarczyć szerokich wstępnych wskazówek co do prawdopodobieństwa wystąpienia istotnego zniekształcenia.

Przykład:

Podczas badania wielu jednostek, w tym tych o mniej złożonych modelach biznesowych i procesach oraz mniej skomplikowanym systemie informacyjnym, audytor może wykonać proste porównanie informacji, takich jak zmiana śródrocznych lub miesięcznych sald kont w stosunku do sald w poprzednich okresach, aby uzyskać wskazówki dotyczące obszarów potencjalnie podwyższonego ryzyka.

A30. Niniejszy MSB dotyczy wykorzystania przez audytora procedur analitycznych jako procedur oszacowania ryzyka. MSB 520²⁴ dotyczy wykorzystania przez audytora procedur analitycznych jako procedur wiarygodności („analityczne procedury wiarygodności”) oraz odpowiedzialności audytora za wykonanie procedur analitycznych pod koniec badania. W związku z tym, wykonanie procedur analitycznych wykonywanych jako procedury oszacowania ryzyka nie jest wymagane zgodnie z wymogami MSB 520. Jednakże, wymogi i materiał dotyczący zastosowania zawarte w MSB 520 mogą zapewnić użyteczne wskazówki dla audytora podczas wykonywania procedur analitycznych jako części procedur oszacowania ryzyka.

Zautomatyzowane narzędzia i techniki

A31. Procedury analityczne mogą być wykonywane przy użyciu szeregu narzędzi lub technik, które mogą być zautomatyzowane. Zastosowanie zautomatyzowanych procedur analitycznych w odniesieniu do danych można określić mianem analizy danych.

²⁴ MSB 520 *Procedury analityczne*.

Przykład:

Audytora może korzystać z arkusza kalkulacyjnego w celu porównania rzeczywistych zaksięgowanych kwot z kwotami przewidzianymi w budżecie lub może wykonać bardziej zaawansowaną procedurę poprzez pobranie danych z systemu informacyjnego jednostki i dalszą analizę tych danych z wykorzystaniem technik wizualizacji, aby zidentyfikować grupy transakcji, salda kont lub ujawnień, dla których mogą być zagwarantowane dalsze szczegółowe procedury oszacowania ryzyka.

Obserwacja i inspekcja (Zob. par. 14(c))

Dlaczego obserwacja i inspekcja są wykonywane jako procedury oszacowania ryzyka

A32. Obserwacja i inspekcja mogą wspomagać, potwierdzać lub zaprzeczać zapytaniom kierowanym do kierownictwa i innych osób, a także mogą dostarczać informacji o jednostce i jej otoczeniu.

Skalowalność

A33. Gdy polityki lub procedury nie są udokumentowane lub jednostka ma mniej sformalizowane kontrole, audytor może nadal być w stanie uzyskać niektóre dowody badania wspierające identyfikację i oszacowanie ryzyk istotnego zniekształcenia poprzez obserwację lub inspekcję wykonania kontroli.

Przykłady:

- Audytor może uzyskać zrozumienie kontroli dotyczących spisu z natury zapasów, nawet jeżeli nie zostały one udokumentowane przez jednostkę, poprzez bezpośrednią obserwację.
- Audytor może być w stanie zaobserwować podział obowiązków.
- Audytor może być w stanie zaobserwować wprowadzanie haseł.

Obserwacja i inspekcja jako procedury oszacowania ryzyka

A34. Procedury oszacowania ryzyka mogą obejmować obserwację lub inspekcję następujących elementów:

- działalności jednostki,
- dokumentów wewnętrznych (takich jak biznes plany i strategie), rejestrów i instrukcji kontroli wewnętrznej,
- raportów sporządzanych przez kierownictwo (takich jak kwartalne raporty kierownictwa i śródroczne sprawozdania finansowe) i przez osoby sprawujące nadzór (takich jak protokoły z posiedzeń rady nadzorczej),
- siedziby i wyposażenia zakładów jednostki,
- informacji uzyskanych ze źródeł zewnętrznych, takich jak czasopisma handlowe i gospodarcze; raporty analityków, banków lub agencji ratingowych; publikacje o charakterze regulacyjnym lub finansowym; lub inne zewnętrzne dokumenty dotyczące wyników finansowych jednostki (takie jak te przywołane w paragrafie A79),
- zachowań i działań kierownictwa lub osób sprawujących nadzór (takie jak obserwacja spotkania komitetu audytu).

Zautomatyzowane narzędzia i techniki

A35. Zautomatyzowane narzędzia lub techniki mogą być również wykorzystywane do obserwacji lub inspekcji, w szczególności aktywów, na przykład poprzez wykorzystanie narzędzi do zdalnej obserwacji (np. dron).

Szczególne rozważania dla jednostek sektora publicznego

A36. Procedury oszacowania ryzyka wykonywane przez audytorów jednostek sektora publicznego mogą również obejmować obserwację i inspekcję dokumentów sporządzonych przez kierownictwo dla ustawodawcy, na przykład dokumentów związanych z obowiązkową sprawozdawczością dotyczącą wyników.

Informacje z innych źródeł (Zob. par. 15)

Dlaczego audytor rozważa informacje z innych źródeł

A37. Informacje uzyskane z innych źródeł mogą być stosowne dla identyfikacji i oszacowania ryzyk istotnego zniekształcenia poprzez dostarczenie informacji i spostrzeżeń na temat:

- charakteru jednostki i jej ryzyk gospodarczych oraz tego, co mogło się zmienić w porównaniu z poprzednimi okresami,
- uczciwości i wartości etycznych kierownictwa i osób sprawujących nadzór, które mogą być również stosowne dla zrozumienia przez audytora środowiska kontroli,
- mających zastosowanie ramowych założeń sprawozdawczości finansowej i ich zastosowania do charakteru i okoliczności jednostki.

Inne stosowne źródła

A38. Inne stosowne źródła informacji obejmują:

- procedury audytora dotyczące akceptacji lub kontynuacji relacji z klientem lub zlecenia badania zgodnie z MSB 220 (zmienionym), w tym wyciągnięte na ich podstawie wnioski²⁵,
- inne zlecenia wykonane dla jednostki przez partnera odpowiedzialnego za zlecenie. Partner odpowiedzialny za zlecenie mógł uzyskać wiedzę stosowną dla badania, w tym na temat jednostki i jej otoczenia, podczas wykonywania innych zleceń dla jednostki. Takie zlecenia mogą obejmować zlecenia uzgodnionych procedur lub inne zlecenia badania lub usług atestacyjnych, w tym zlecenia odnoszące się do dodatkowych wymogów sprawozdawczych w danym systemie prawnym.

Informacje uzyskane z wcześniejszych doświadczeń audytora z jednostką oraz wcześniejszych badań (Zob. par. 16)

Dlaczego informacje z wcześniejszych badań są ważne dla bieżącego badania

A39. Wcześniejsze doświadczenie audytora z jednostką oraz wynikające z procedur badania wykonanych podczas wcześniejszych badań mogą dostarczyć audytorowi informacji, które są stosowne dla określenia przez audytora rodzaju i zakresu procedur oszacowania ryzyka oraz identyfikacji i oszacowania ryzyk istotnego zniekształcenia.

Charakter informacji z wcześniejszych badań

²⁵ MSB 220 (zmieniony) *Zarządzanie jakością dla badania sprawozdania finansowego*, paragrafy 22-24.

A40. Wcześniejsze doświadczenie audytora z daną jednostką oraz procedury badania wykonane podczas wcześniejszych badań mogą dostarczyć audytorowi informacji na temat takich spraw, jak:

- historyczne zniekształcenia oraz czy były one terminowo korygowane,
- charakterystyka jednostki i jej otoczenia oraz systemu kontroli wewnętrznej jednostki (w tym słabości kontroli),
- znaczące zmiany, jakie nastąpiły w jednostce lub jej działalności, od poprzedniego okresu finansowego,
- te szczególne rodzaje transakcji i inne zdarzenia lub salda kont (oraz związane z nimi ujawnienia), gdy audytor napotkał trudności podczas wykonywania niezbędnych procedur badania, na przykład ze względu na ich złożoność.

A41. Od audytora wymagane jest ustalenie czy informacje uzyskane z wcześniejszego doświadczenia audytora z jednostką oraz z procedur badania wykonanych podczas poprzednich badań pozostają stosowne i wiarygodne, jeżeli audytor zamierza wykorzystać te informacje dla celów bieżącego badania. Jeżeli charakter lub okoliczności jednostki zmieniły się lub uzyskano nowe informacje, informacje z poprzednich okresów mogą nie być już stosowne lub wiarygodne dla bieżącego badania. Aby ustalić, czy nastąpiły zmiany, które mogą wpłynąć na stosowność lub wiarygodność takich informacji, audytor może kierować zapytania i wykonywać inne odpowiednie procedury badania, takie jak testy „krok po kroku” (ang. *walk-throughs*) stosownych systemów. Jeżeli informacje te nie są wiarygodne, audytor może rozważyć wykonanie dodatkowych procedur, które są odpowiednie w danych okolicznościach.

Dyskusja zespołu wykonującego zlecenie (Zob. par. 17–18)

Dlaczego od zespołu wykonującego zlecenie wymagane jest przedyskutowanie zastosowania mających zastosowanie ramowych założeń sprawozdawczości finansowej oraz podatności sprawozdania finansowego jednostki na istotne zniekształcenie

A42. Dyskusja w gronie zespołu wykonującego zlecenie na temat zastosowania mających zastosowanie ramowych założeń sprawozdawczości finansowej i podatności sprawozdania finansowego jednostki na istotne zniekształcenie:

- stwarza okazję, aby bardziej doświadczeni członkowie zespołu wykonującego zlecenie, w tym partner odpowiedzialny za zlecenie, podzielili się swymi poglądami opartymi o ich wiedzę na temat jednostki. Dzielenie się informacjami przyczynia się do lepszego zrozumienia przez wszystkich członków zespołu wykonującego zlecenie,
- umożliwia członkom zespołu wykonującego zlecenie wymianę informacji na temat ryzyk gospodarczych, którym podlega jednostka, w jaki sposób czynniki ryzyka nieodłącznego mogą wpływać na podatność na zniekształcenie grup transakcji, sald kont i ujawnień oraz tego, jak i gdzie sprawozdanie finansowe może być podatne na istotne zniekształcenie spowodowane oszustwem lub błędem,
- pomaga członkom zespołu wykonującego zlecenie zdobyć lepsze zrozumienie potencjału dla istotnego zniekształcenia sprawozdania finansowego w poszczególnych, przydzielonych im obszarach oraz zrozumieć, jak wyniki procedur badania, które wykonali, mogą wpływać na inne aspekty badania, w tym na decyzje o rodzaju, rozłożeniu w czasie i zakresie dalszych procedur badania. W szczególności dyskusja pomaga członkom zespołu wykonującego zlecenie w dalszym rozważaniu sprzecznych informacji w oparciu o własne zrozumienie przez każdego z członków zespołu charakteru i okoliczności danej jednostki,

- stwarza podstawę, aby członkowie zespołu wykonującego zlecenie komunikowali się i dzielili się nowymi informacjami uzyskanymi w trakcie całego badania, które mogą wpływać na oszacowanie ryzyk istotnego zniekształcenia lub na procedury badania wykonane w celu odniesienia się do tych ryzyk.

MSB 240 wymaga, aby podczas dyskusji zespołu wykonującego zlecenie położyć szczególny nacisk na to, w jaki sposób i gdzie sprawozdanie finansowe jednostki może być podatne na istotne zniekształcenie spowodowane oszustwem, w tym na to, w jaki sposób może wystąpić oszustwo²⁶.

- A43. Zawodowy sceptycyzm jest niezbędny do krytycznej oceny dowodów badania, a solidna i otwarta dyskusja zespołu wykonującego zlecenie, w tym dla badań cyklicznych, może prowadzić do lepszej identyfikacji i oszacowania ryzyk istotnego zniekształcenia. Innym wynikiem dyskusji może być zidentyfikowanie przez audytora konkretnych obszarów badania, dla których stosowanie zawodowego sceptycyzmu może być szczególnie ważne i może prowadzić do zaangażowania bardziej doświadczonych członków zespołu wykonującego zlecenie, którzy posiadają odpowiednie umiejętności, aby uczestniczyć w wykonywaniu procedur badania związanych z tymi obszarami.

Skalowalność

- A44. Gdy zlecenie jest przeprowadzane przez jedną osobę, taką jak samodzielnie pracujący praktyk (tj. tam, gdzie nie byłaby możliwa dyskusja zespołu wykonującego zlecenie), rozważenie zagadnień, o których mowa w paragrafach A42 i A46, może jednak pomóc audytorowi w zidentyfikowaniu, gdzie mogą być ryzyka istotnego zniekształcenia.
- A45. Gdy zlecenie jest przeprowadzane przez duży zespół wykonujący zlecenie, tak jak badanie sprawozdania finansowego grupy, nie zawsze jest konieczne lub wykonalne włączenie do jednej dyskusji wszystkich członków (na przykład, podczas badania w wielu lokalizacjach), ani nie jest konieczne, aby wszyscy członkowie zespołu wykonującego zlecenie byli informowani o wszystkich decyzjach podjętych w trakcie dyskusji. Partner odpowiedzialny za zlecenie może omawiać sprawy z kluczowymi członkami zespołu wykonującego zlecenie, w tym, jeżeli uzna to za odpowiednie, z osobami o szczególnych umiejętnościach lub wiedzy i osobami odpowiedzialnymi za prace do wykonania w częściach składowych grupy wtedy, gdy deleguje przeprowadzanie dyskusji z pozostałymi osobami, bierze pod uwagę zakres komunikacji uważanej za niezbędną w całym zespole wykonującym zlecenie. Przydatny może być plan komunikacji, uzgodniony przez partnera odpowiedzialnego za zlecenie.

Omówienie ujawnień zawartych w mających zastosowanie ramowych założeniach sprawozdawczości finansowej

- A46. W ramach dyskusji w gronie zespołu wykonującego zlecenie, rozważenie wymogów dotyczących ujawnień zawartych w mających zastosowanie ramowych założeniach sprawozdawczości finansowej pomaga we wczesnym identyfikowaniu podczas badania, gdzie mogą wystąpić ryzyka istotnego zniekształcenia w odniesieniu do ujawnień, nawet w okolicznościach, gdy mające zastosowanie ramowe założenia sprawozdawczości finansowej wymagają jedynie uproszczonych ujawnień. Zagadnienia, które zespół wykonujący zlecenie może omówić, obejmują:
- zmiany w wymogach sprawozdawczości finansowej, które mogą skutkować znaczącymi nowymi lub zmienionymi ujawnieniami,

²⁶ MSB 240, paragraf 16.

- zmiany w otoczeniu, sytuacji finansowej lub działalności jednostki, które mogą skutkować znaczącymi nowymi lub zmienionymi ujawnieniami, na przykład znaczące połączenie jednostek gospodarczych w okresie objętym badaniem,
- ujawnienia, dla których uzyskanie wystarczających odpowiednich dowodów badania mogło być trudne w przeszłości, oraz
- ujawnienia na temat złożonych zagadnień, w tym tych wiążących się ze znaczącym osądem kierownictwa co do tego, które informacje ujawnić.

Szczególne rozważania dla jednostek sektora publicznego

A47. W ramach dyskusji w gronie zespołu wykonującego zlecenie przez audytorów jednostek sektora publicznego można również rozważyć wszelkie dodatkowe szersze cele i związane z nimi ryzyka powstające z upoważnienia do badania lub obowiązków jednostek sektora publicznego.

Uzyskanie zrozumienia jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej oraz systemu kontroli wewnętrznej jednostki (Zob. par. 19-27)

Załączniki 1 do 6 przedstawiają dalsze rozważania dotyczące uzyskania zrozumienia jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej oraz systemu kontroli wewnętrznej jednostki.

Uzyskanie wymaganego zrozumienia (Zob. par. 19-27)

A48. Uzyskanie zrozumienia jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej oraz systemu kontroli wewnętrznej jednostki jest dynamicznym i iteratywnym procesem gromadzenia, aktualizowania i analizowania informacji i trwa przez całe badanie. W związku z tym, oczekiwania audytora mogą zmienić się po uzyskaniu nowych informacji.

A49. Zrozumienie przez audytora jednostki i jej otoczenia oraz mających zastosowanie ramowych założeń sprawozdawczości finansowej może również pomóc audytorowi w opracowaniu wstępnych oczekiwań dotyczących grup transakcji, sald kont i ujawnień, które mogą być istotnymi grupami transakcji, saldami kont i ujawnieniami. Te oczekiwane znaczące grupy transakcji, salda kont i ujawnienia stanowią podstawę zakresu zrozumienia przez audytora systemu informacyjnego jednostki.

Dlaczego wymagane jest zrozumienie jednostki i jej otoczenia oraz mających zastosowanie ramowych założeń sprawozdawczości finansowej (Zob. par. 19-20)

A50. Zrozumienie przez audytora jednostki i jej otoczenia oraz mających zastosowanie ramowych założeń sprawozdawczości finansowej pomaga audytorowi w zrozumieniu zdarzeń i warunków, które są stosowne dla jednostki oraz w zidentyfikowaniu, w jaki sposób i w jakim stopniu czynniki ryzyka nieodłącznego wpływają na podatność stwierdzeń na zniekształcenie podczas sporządzania sprawozdania finansowego, zgodnie z mającymi zastosowanie ramowymi założeniami sprawozdawczości finansowej. Informacje takie ustalają ramy odniesienia, w których audytor identyfikuje i szacuje ryzyka istotnego zniekształcenia. Te ramy odniesienia pomagają również audytorowi w planowaniu badania oraz w stosowaniu zawodowego osądu i zawodowego sceptycyzmu w trakcie całego badania, na przykład, gdy:

- identyfikuje i dokonuje oszacowania ryzyk istotnego zniekształcenia sprawozdania finansowego zgodnie z MSB 315 (zmienionym w 2019 r.) lub innymi stosownymi

standardami (np. w odniesieniu do ryzyk oszustwa zgodnie z MSB 240 lub podczas identyfikowania lub szacowania ryzyk związanych z szacunkami księgowymi zgodnie z MSB 540 (zmienionym)),

- wykonuje procedury pomagające zidentyfikować przypadki niezgodności z przepisami prawa i regulacją, które mogą mieć istotny wpływ na sprawozdanie finansowe zgodnie z MSB 250²⁷,
- ocenia, czy sprawozdanie finansowe zapewnia adekwatne ujawnienia zgodnie z MSB 700 (zmienionym)²⁸,
- ustala istotność lub istotność wykonawczą zgodnie z MSB 320²⁹ lub
- rozważa odpowiedniość wyboru i zastosowania zasad (polityki) rachunkowości oraz adekwatność ujawnień w sprawozdaniu finansowym.

A51. Zrozumienie przez audytora jednostki i jej otoczenia oraz mających zastosowanie ramowych założeń sprawozdawczości finansowej informuje również, w jaki sposób audytor planuje i wykonuje dalsze procedury badania, na przykład, gdy:

- opracowuje oczekiwania do wykorzystania podczas wykonywania procedur analitycznych zgodnie z MSB 520³⁰,
- projektuje i wykonuje dalsze procedury badania w celu uzyskania wystarczających odpowiednich dowodów badania zgodnie z MSB 330, oraz
- ocenia wystarczalność i odpowiedniość uzyskanych dowodów badania (np. odnoszących się do założeń lub ustnych i pisemnych oświadczeń kierownictwa).

Skalowalność

A52. Charakter i zakres wymaganego zrozumienia są sprawą zawodowego osądu audytora i różni się pomiędzy jednostkami w oparciu o charakterystykę i okoliczności jednostki, w tym:

- wielkość i złożoność jednostki, w tym jej środowiska IT,
- wcześniejsze doświadczenie audytora z jednostką,
- charakter systemów i procesów jednostki, w tym, czy są one sformalizowane czy nie, oraz
- charakter i forma dokumentacji jednostki.

A53. Procedury oszacowania ryzyka przez audytora, w celu uzyskania wymaganego zrozumienia, mogą być mniej rozbudowane podczas badań mniej złożonych jednostek, a bardziej rozbudowane dla jednostek, które są bardziej złożone. Oczekuje się, że głębokość zrozumienia, która jest wymagana przez audytora, będzie mniejsza niż ta posiadana przez kierownictwo podczas zarządzania jednostką.

A54. Niektóre ramowe założenia sprawozdawczości finansowej pozwalają mniejszym jednostkom przedstawiać prostsze i mniej szczegółowe ujawnienia w sprawozdaniu finansowym. Nie zwalnia to jednak audytora z obowiązku uzyskania zrozumienia jednostki i jej otoczenia oraz mających zastosowanie ramowych założeń sprawozdawczości finansowej, które mają zastosowanie do jednostki.

²⁷ MSB 250 (zmieniony) *Rozważenie przepisów prawa i regulacji podczas badania sprawozdania finansowego*, paragraf 14.

²⁸ MSB 700 (zmieniony) *Formułowanie opinii oraz sprawozdawczość na temat sprawozdania finansowego*, paragraf 13(e).

²⁹ MSB 320 *Istotność w planowaniu i wykonywaniu badania*, paragrafy 10-11.

³⁰ MSB 520, paragraf 5.

A55. Korzystanie przez jednostkę z IT oraz charakter i zakres zmian w środowisku IT może również wpływać na specjalistyczne umiejętności, które są niezbędne, aby pomóc w uzyskaniu wymaganego zrozumienia.

Jednostka i jej otoczenie (Zob. par. 19(a))

Struktura organizacyjna jednostki, struktura właścicielska i ład korporacyjny oraz model biznesowy (Zob. par. 19(a)(i))

Struktura organizacyjna i właścicielska jednostki

A56. Zrozumienie struktury organizacyjnej jednostki i jej struktury właścicielskiej może umożliwić audytorowi zrozumienie takich zagadnień, jak:

- Złożoność struktury jednostki.

Przykład:

Jednostka może być pojedynczą jednostką lub struktura jednostki może obejmować spółki zależne, oddziały lub inne części składowe, znajdujące się w wielu lokalizacjach. Ponadto, struktura prawna może różnić się od struktury operacyjnej. Złożone struktury często wprowadzają czynniki, które mogą powodować powstanie zwiększonej podatności na ryzyka istotnego zniekształcenia. Takie kwestie mogą obejmować ustalenie czy wartość firmy, wspólne przedsięwzięcia, inwestycje lub jednostki specjalnego przeznaczenia są odpowiednio księgowane oraz czy kwestie takie zostały adekwatnie ujawnione w sprawozdaniu finansowym.

- Struktura właścicielska oraz powiązania pomiędzy właścicielami i innymi osobami lub jednostkami, w tym ze stronami powiązanymi. Zrozumienie to może pomóc w ustaleniu, czy transakcje ze stronami powiązanymi zostały odpowiednio zidentyfikowane, zaksięgowane i adekwatnie ujawnione w sprawozdaniu finansowym.³¹
- Rozróżnienie pomiędzy właścicielami, osobami sprawującymi nadzór i kierownictwem.

Przykład:

W mniej złożonych jednostkach właściciele jednostki mogą być zaangażowani w zarządzanie jednostką, dlatego też rozróżnienie to jest niewielkie lub nie istnieje. W przeciwieństwie do tego tak, jak w niektórych jednostkach notowanych, może istnieć wyraźne rozróżnienie pomiędzy kierownictwem, właścicielami jednostki i osobami sprawującymi nadzór³².

³¹ MSB 550 ustanawia wymogi i zapewnia wytyczne na temat rozważań audytora stosownych do stron powiązanych.

³² Paragrafy A1 i A2 w MSB 260 (zmienionym) dostarczają wytycznych dotyczących identyfikacji osób sprawujących nadzór oraz wyjaśniają, że w niektórych przypadkach niektóre lub wszystkie osoby sprawujące nadzór mogą być zaangażowane w zarządzanie jednostką.

- Struktura i złożoność środowiska IT jednostki.

Przykłady:

Jednostka może:

- posiadać wiele starszych systemów IT w różnych działaniach, które nie są dobrze zintegrowane, co skutkuje skomplikowanym środowiskiem IT,
- korzystać z usług zewnętrznych lub wewnętrznych dostawców usług dla określonych aspektów swojego środowiska IT (np. outsourcing hostingu swojego środowiska IT do strony trzeciej lub korzystanie z centrum usług wspólnych dla centralnego zarządzania procesami IT w grupie).

Zautomatyzowane narzędzia i techniki

A57. Audytor, w celu zrozumienia przepływów transakcji i przetwarzania, może wykorzystywać zautomatyzowane narzędzia i techniki jako część procedur audytora mających na celu zrozumienie systemu informacyjnego. Wynikiem tych procedur może być uzyskanie przez audytora informacji na temat struktury organizacyjnej jednostki lub podmiotów, z którymi jednostka prowadzi działalność (np. dostawcy, klienci, strony powiązane).

Szczególne rozważania dla jednostek sektora publicznego

A58. Struktura właścicielska jednostki sektora publicznego może nie mieć takiego samego znaczenia jak w sektorze prywatnym, ponieważ decyzje związane z tą jednostką mogą być podejmowane poza jednostką w wyniku procesów politycznych. W związku z tym, kierownictwo może nie mieć kontroli nad pewnymi decyzjami, które są podejmowane. Zagadnienia, które mogą być stosowne, obejmują zrozumienie zdolności jednostki do podejmowania jednostronnych decyzji oraz zdolności innych jednostek sektora publicznego do kontrolowania lub wpływania na uprawnienia i strategiczny kierunek jednostki.

Przykład:

Jednostka sektora publicznego może podlegać przepisom prawa lub innym dyrektywom władz, które wymagają od niej uzyskania akceptacji stron zewnętrznych w stosunku do jednostki na jej strategię i cele przed ich wdrożeniem. Dlatego też zagadnienia związane ze zrozumieniem struktury prawnej jednostki mogą obejmować mające zastosowanie przepisy prawa i regulację oraz klasyfikację jednostki (tj. czy jednostka jest ministerstwem, departamentem, agencją lub innym rodzajem jednostki).

Ład korporacyjny

Dlaczego audytor uzyskuje zrozumienie w zakresie ładu korporacyjnego

A59. Zrozumienie ładu korporacyjnego jednostki może pomóc audytorowi w zrozumieniu zdolności jednostki do zapewnienia odpowiedniego nadzoru nad jej systemem kontroli wewnętrznej. Jednakże, zrozumienie to może również dostarczyć dowodów słabości, które mogą wskazywać na wzrost podatności sprawozdania finansowego jednostki na ryzyka istotnego zniekształcenia.

Zrozumienie ładu korporacyjnego jednostki

A60. Zagadnienia, które mogą być stosowne do rozważenia przez audytora podczas uzyskiwania zrozumienia ładu korporacyjnego jednostki, obejmują:

- czy jakiekolwiek lub wszystkie osoby sprawujące nadzór są zaangażowane w zarządzanie jednostką,
- istnienie organu nadzorującego, jeżeli jakikolwiek istnieje, i jego rozdzielenie od kierownictwa wykonawczego,
- czy osoby sprawujące nadzór zajmują stanowiska, które stanowią integralną część struktury prawnej jednostki, na przykład jako dyrektorzy,
- istnienie podgrup osób sprawujących nadzór, takich jak komitet audytu oraz obowiązki takiej podgrupy,
- obowiązki osób sprawujących nadzór w zakresie nadzoru nad sprawozdawczością finansową, w tym zatwierdzanie sprawozdania finansowego.

Model biznesowy jednostki

Załącznik 1 określa dodatkowe rozważania dla uzyskania zrozumienia jednostki i jej modelu biznesowego, jak również dodatkowe rozważania dla badania jednostek specjalnego przeznaczenia.

Dlaczego audytor uzyskuje zrozumienie modelu biznesowego jednostki

A61. Zrozumienie celów, strategii i modelu biznesowego jednostki pomaga audytorowi zrozumieć jednostkę na poziomie strategicznym oraz zrozumieć ryzyka gospodarcze, które jednostka podejmuje i z którymi się mierzy. Zrozumienie ryzyk gospodarczych, które mają wpływ na sprawozdanie finansowe, pomaga audytorowi w identyfikowaniu ryzyk istotnego zniekształcenia, ponieważ większość ryzyk gospodarczych będzie miała ostatecznie konsekwencje finansowe, a tym samym wpływ na sprawozdanie finansowe.

Przykłady:

Model biznesowy jednostki może opierać się na wykorzystaniu IT na różne sposoby:

- jednostka sprzedaje obuwie w sklepie stacjonarnym i wykorzystuje zaawansowany system magazynowy i obsługujący punkty sprzedaży do rejestrowania sprzedaży obuwia, lub
- jednostka sprzedaje obuwie przez Internet, dzięki czemu wszystkie transakcje sprzedaży są przetwarzane w środowisku IT, w tym inicjowanie transakcji poprzez stronę internetową.

Dla obu tych jednostek ryzyka gospodarcze powstające na skutek znacząco różniącego się modelu biznesowego byłyby zasadniczo różne, pomimo że obie jednostki sprzedają obuwie.

Zrozumienie modelu biznesowego jednostki

A62. Nie wszystkie aspekty modelu biznesowego są stosowne dla zrozumienia przez audytora. Ryzyka gospodarcze są szersze niż ryzyka istotnego zniekształcenia sprawozdania finansowego, chociaż ryzyka gospodarcze obejmują te drugie. Audytor nie ma obowiązku zrozumienia lub identyfikacji wszystkich ryzyk gospodarczych, ponieważ nie wszystkie ryzyka gospodarcze powodują powstanie ryzyk istotnego zniekształcenia.

A63. Ryzyka gospodarcze zwiększające podatność na ryzyka istotnego zniekształcenia mogą powstawać na skutek:

- niewłaściwych celów lub strategii, nieskutecznej realizacji strategii, zmian lub złożoności,

- braku uznania potrzeby zmian, który może również powodować powstanie ryzyka gospodarczego, na przykład z powodu:
 - opracowania nowych produktów lub usług, które mogą być nieudane,
 - rynku, który, nawet jeżeli pomyślnie się rozwinął, jest nieadekwatny, aby wspierać produkt lub usługę, lub
 - wad produktu lub usługi, które mogą skutkować odpowiedzialnością prawną i ryzykiem utraty reputacji.
 - zachęt i nacisków na kierownictwo, które mogą skutkować celową lub niezamierzoną stronniczością kierownictwa, a tym samym wpływać na zasadność znaczących założeń i oczekiwań kierownictwa lub osób sprawujących nadzór.
- A64. Przykłady zagadnień, które audytor może rozważyć, uzyskując zrozumienie modelu biznesowego jednostki, jej celów, strategii i związanych z nimi ryzyk gospodarczych, które mogą skutkować ryzykiem istotnego zniekształcenia sprawozdania finansowego, obejmują:
- rozwój branży, taki jak brak personelu lub wiedzy fachowej, aby radzić sobie ze zmianami w branży,
 - nowe produkty i usługi, które mogą prowadzić do zwiększonej odpowiedzialności za produkt,
 - rozszerzenie działalności jednostki, a popyt nie został dokładnie oszacowany,
 - nowe wymogi dotyczące rachunkowości, gdy nastąpiło ich niepełne lub nieprawidłowe wdrożenie,
 - wymogi regulacyjne skutkujące zwiększonym narażeniem na ryzyko prawne,
 - bieżące i przyszłe wymogi finansowe, takie jak utrata finansowania w związku z niezdolnością jednostki do spełnienia wymogów,
 - wykorzystanie IT, takie jak wdrożenie nowego systemu IT, który będzie mieć wpływ zarówno na działalność, jak i na sprawozdawczość finansową, lub
 - skutki wdrożenia strategii, w szczególności wszelkie skutki, które doprowadzą do nowych wymogów w zakresie rachunkowości.
- A65. Zazwyczaj kierownictwo identyfikuje ryzyka gospodarcze i opracowuje podejście, aby odnieść się do nich. Taki proces oszacowania ryzyka stanowi część systemu kontroli wewnętrznej jednostki i jest omówiony w paragrafie 22 oraz w paragrafach A109-A113.

Szczególne rozważania dla jednostek sektora publicznego

- A66. Jednostki działające w sektorze publicznym mogą tworzyć i dostarczać wartość na różne sposoby, aby tworzyć majątek dla właścicieli, ale nadal będą miały „model biznesowy” o określonym celu. Zagadnienia, których zrozumienie mogą uzyskać audytorzy jednostek z sektora publicznego, a które są stosowne dla modelu biznesowego jednostki, obejmują:
- wiedzę o stosownych działaniach rządowych, w tym powiązanych z nimi programach,
 - cele i strategię programu, w tym elementy polityki publicznej.
- A67. Przy badaniach jednostek sektora publicznego, na „cele kierownictwa” mogą wpływać wymogi wykazania publicznej odpowiedzialności i mogą one obejmować cele, które mają swoje źródło w przepisach prawa, regulacji lub innych kompetencjach organów.

Czynniki branżowe, regulacyjne i inne czynniki zewnętrzne (Zob. par. 19(a)(ii))

Czynniki branżowe

A68. Stosowne czynniki branżowe obejmują warunki w branży, takie jak otoczenie konkurencyjne, powiązania z dostawcami i odbiorcami oraz postęp technologiczny. Zagadnienia, które audytor może rozważyć, obejmują:

- rynek i konkurencję, w tym popyt, potencjał i konkurencję cenową,
- cykliczność lub sezonowość działalności,
- technologię wytwarzania produktów związaną z produktami jednostki,
- dostawy i koszty energii.

A69. Branża, w której działa jednostka, może powodować powstanie określonych ryzyk istotnego zniekształcenia wynikających z charakteru działalności lub stopnia regulacji.

Przykład:

W branży budowlanej kontrakty długoterminowe mogą obejmować znaczące szacunki przychodów i kosztów, które powodują powstanie ryzyk istotnego zniekształcenia. W takich przypadkach ważne jest, aby zespół wykonujący zlecenie obejmował członków posiadających odpowiednie kompetencje i możliwości³³.

Czynniki regulacyjne

A70. Stosowne czynniki regulacyjne obejmują otoczenie regulacyjne. Otoczenie regulacyjne obejmuje, między innymi, mające zastosowanie ramowe założenia sprawozdawczości finansowej oraz otoczenie prawne i polityczne i wszelkie zmiany w tym zakresie. Zagadnienia, które audytor może rozważyć, obejmują:

- ramowe założenia regulacyjne dla branży podlegającej regulacjom, na przykład, wymogi ostrożnościowe, w tym powiązane ujawnienia,
- ustawodawstwo i regulacje, które znacząco wpływają na działalność jednostki, na przykład, przepisy prawa i regulacje z zakresu prawa pracy,
- przepisy prawa i regulacje dotyczące opodatkowania,
- polityki rządu bieżąco wpływające na prowadzenie działalności przez jednostkę, takie jak polityka pieniężna, w tym kontrola dewizowa, polityka fiskalna, zachęty finansowe (na przykład rządowe programy pomocowe) oraz cła lub polityki ograniczeń handlowych,
- wymogi środowiskowe wpływające na branżę i działalność jednostki.

A71. MSB 250 (zmieniony) zawiera niektóre szczególne wymogi związane z ramowymi założeniami prawnymi i regulacyjnymi, mającymi zastosowanie do jednostki i branży lub sektora, w którym jednostka działa³⁴.

Szczególne rozważania dla jednostek sektora publicznego

A72. Dla badań jednostek sektora publicznego, mogą istnieć szczególne przepisy prawa lub regulacje, które mają wpływ na działalność jednostki. Rozważenie takich elementów może być kluczowe podczas uzyskiwania zrozumienia jednostki i jej otoczenia.

³³ MSB 220 (zmieniony), paragrafy 25-28.

³⁴ MSB 250 (zmieniony), paragraf 13.

Inne czynniki zewnętrzne

A73. Inne czynniki zewnętrzne wpływające na jednostkę, które audytor może rozważyć, obejmują ogólne warunki gospodarcze, stopy procentowe i dostępność finansowania oraz inflację lub dewaluację waluty.

Mierniki wykorzystywane przez kierownictwo do oceny wyników finansowych jednostki (Zob. par. 19(a)(iii))

Dlaczego audytor rozumie mierniki wykorzystywane przez kierownictwo

A74. Zrozumienie mierników jednostki pomaga audytorowi w rozważeniu, czy takie mierniki, niezależnie od tego, czy są wykorzystywane zewnętrznie, czy wewnętrznie, powodują powstanie presji na jednostce na osiągnięcie celów w zakresie wyników. Naciski te mogą motywować kierownictwo do podejmowania działań, które zwiększają podatność na zniekształcenie z powodu stronniczości kierownictwa lub oszustwa (np., aby poprawić wyniki działalności lub celowo zniekształcić sprawozdanie finansowe) (zobacz MSB 240 dotyczący wymogów i wytycznych związanych z ryzykami oszustwa).

A75. Mierniki mogą również wskazywać audytorowi prawdopodobieństwo ryzyk istotnego zniekształcenia powiązanych informacji w sprawozdaniu finansowym. Na przykład, mierniki wyniku mogą wskazywać, że jednostka wykazuje niezwykle szybki wzrost lub rentowność w porównaniu z innymi jednostkami w tej samej branży.

Mierniki wykorzystywane przez kierownictwo

A76. Kierownictwo oraz inne osoby zazwyczaj dokonują pomiaru i przeglądu zagadnień, które uznają za ważne. Zapytania kierowane do kierownictwa mogą wykazać, że dla celów dokonywania oceny wyników finansowych i podejmowania działań polega ono na pewnych kluczowych wskaźnikach, niezależnie od tego, czy są one publicznie dostępne, czy nie. W takich przypadkach audytor może zidentyfikować stosowne mierniki działalności, niezależnie od tego, czy są one wewnętrzne, czy zewnętrzne, poprzez rozważenie informacji, które jednostka wykorzystuje do zarządzania swoją działalnością. Jeżeli takie zapytanie wskazuje na brak pomiaru lub przeglądu wyników działalności, może wystąpić podwyższone ryzyko niewykrytych i nieskorygowanych zniekształceń.

A77. Kluczowe wskaźniki wykorzystywane do dokonywania oceny wyników finansowych mogą obejmować:

- kluczowe wskaźniki działalności (finansowe i niefinansowe) oraz kluczowe współczynniki, trendy i statystyki operacyjne,
- analizy wyników finansowych za kolejne okresy,
- budżety, prognozy, analizy odchyleń, informacje o segmentach oraz raporty z działalności wydziałów, departamentów lub innych szczebli,
- mierniki dokonań pracowników oraz polityki wynagradzania premiowego,
- porównania wyników działalności jednostki z wynikami konkurencji.

Skalowalność (Zob. par. 19(a)(iii))

A78. Procedury podejmowane, aby zrozumieć mierniki jednostki, mogą różnić się w zależności od wielkości lub złożoności jednostki, jak również od zaangażowania właścicieli lub osób sprawujących nadzór w zarządzanie jednostką.

Przykłady:

- Dla niektórych mniej złożonych jednostek, warunki kredytów bankowych jednostki (tj. kowenanty bankowe) mogą być powiązane z konkretnymi miernikami działalności związanymi z wynikami lub sytuacją finansową jednostki (np. maksymalna kwota kapitału obrotowego). Zrozumienie przez audytora mierników działalności używanych przez bank może pomóc zidentyfikować obszary, gdzie występuje zwiększona podatność na ryzyko istotnego zniekształcenia.
- Dla niektórych jednostek, których charakter i okoliczności są bardziej złożone, takich jak te działające w branży ubezpieczeniowej lub bankowej, wyniki lub sytuacja finansowa mogą być mierzone wobec wymogów regulacyjnych (np. wymogi dotyczące wskaźnika regulacyjnego, takiego jak adekwatność kapitałowa i przeszkody w osiąganiu wskaźników płynności). Zrozumienie przez audytora tych mierników wyników może pomóc zidentyfikować obszary, gdzie występuje zwiększona podatność na ryzyko istotnego zniekształcenia.

Inne rozważania

A79. Strony zewnętrzne mogą również dokonywać przeglądu i analizować wyniki finansowe jednostki, w szczególności dla jednostek, gdzie informacje finansowe są publicznie dostępne. Audytor może również rozważyć informacje dostępne publicznie, które mogą pomóc audytorowi w dalszym zrozumieniu działalności lub zidentyfikowaniu sprzecznych informacji, takich jak informacje pochodzące od:

- analityków lub agencji kredytowych,
- agencji informacyjnych i innych mediów, w tym mediów społecznościowych,
- organów podatkowych,
- regulatorów,
- związków zawodowych,
- dostawców finansowania.

Takie informacje finansowe można często uzyskać od badanej jednostki.

A80. Pomiar i przegląd wyników finansowych nie są tożsame z monitorowaniem systemu kontroli wewnętrznej (omówionym jako element systemu kontroli wewnętrznej w paragrafach A114–A122), pomimo, że ich cele mogą się pokrywać:

- pomiar i przegląd wyników działalności są nakierowane na to, czy działalność gospodarcza spełnia cele wyznaczone przez kierownictwo (lub strony trzecie),
- w przeciwieństwie do tego, monitorowanie systemu kontroli wewnętrznej polega na monitorowaniu skuteczności kontroli, w tym tych związanych z pomiarem i przeglądem wyników finansowych przez kierownictwo.

Jednakże, w niektórych przypadkach, wskaźniki działalności dostarczają także informacji, które umożliwiają kierownictwu identyfikację słabości kontroli.

Szczególne rozważania dla jednostek sektora publicznego

A81. Oprócz rozważenia stosownych mierników wykorzystywanych przez jednostkę sektora publicznego do oceny wyników finansowych jednostki, audytorzy jednostek sektora publicznego

mogą również rozważyć informacje niefinansowe, takie jak osiągnięcie wyników w zakresie pożytku publicznego (na przykład liczba osób, które otrzymują pomoc poprzez konkretny program).

Mające zastosowanie ramowe założenia sprawozdawczości finansowej (Zob. par. 19(b))

Zrozumienie mających zastosowanie ramowych założeń sprawozdawczości finansowej i zasad (polityk) rachunkowości jednostki

A82. Zagadnienia, które audytor może rozważyć uzyskując zrozumienie mających zastosowanie ramowych założeń sprawozdawczości finansowej jednostki oraz sposobu ich zastosowania w kontekście charakteru i okoliczności jednostki oraz jej otoczenia obejmują:

- praktyki jednostki w zakresie sprawozdawczości finansowej zgodnie z mającymi zastosowanie ramowymi założeniami sprawozdawczości finansowej, takie jak:
 - zasady rachunkowości i praktyki specyficzne dla danej branży, w tym znaczące dla konkretnej branży grupy transakcji, salda kont i powiązane ujawnienia w sprawozdaniu finansowym (na przykład, pożyczki i inwestycje w bankach lub prace badawcze i rozwojowe w branży farmaceutycznej),
 - ujmowanie przychodów,
 - rachunkowość dotycząca instrumentów finansowych, w tym związanych z nimi strat kredytowych,
 - aktywa, zobowiązania i transakcje w walucie obcej,
 - rachunkowość nietypowych lub złożonych transakcji, w tym tych w obszarach kontrowersyjnych lub nowatorskich (na przykład, rachunkowość dotycząca kryptowalut),
- zrozumienie doboru i zastosowania zasad (polityk) rachunkowości przez jednostkę, w tym wszelkich zmian do nich i ich przyczyn, może dotyczyć takich zagadnień, jak:
 - metody wykorzystywane przez jednostkę do ujmowania, wyceny, prezentacji i ujawniania znaczących i nietypowych transakcji,
 - skutek znaczących zasad (polityk) rachunkowości w kontrowersyjnych lub nowatorskich obszarach, dla których brak jest wiążących wytycznych lub uzgodnionego podejścia,
 - zmiany w otoczeniu, takie jak zmiany mających zastosowanie ramowych założeń sprawozdawczości finansowej lub reformy podatkowe, które mogą wymagać zmiany zasad (polityk) rachunkowości jednostki,
 - standardy sprawozdawczości finansowej oraz przepisy prawa i regulacja, które są nowe dla jednostki, oraz kiedy i w jaki sposób jednostka wdroży lub spełni takie wymogi.

- A83. Uzyskanie zrozumienia jednostki i jej otoczenia może pomóc audytorowi w rozważeniu, gdy można oczekiwać zmian w sprawozdawczości finansowej jednostki (np. od poprzednich okresów).

Przykład:

Jeżeli w trakcie okresu sprawozdawczego jednostka dokonała znaczącego połączenia przedsięwzięć, to audytor prawdopodobnie oczekiwałby zmian w grupach transakcji, saldach kont i ujawnieniach związanych z tym połączeniem przedsięwzięć. Odwrotnie, jeżeli w danym okresie nie nastąpiły żadne znaczące zmiany w ramowych założeniach sprawozdawczości finansowej, zrozumienie audytora może pomóc w potwierdzeniu, że zrozumienie uzyskane w poprzednim okresie ma nadal zastosowanie.

Szczegółne rozważania dla jednostek sektora publicznego

- A84. Mające zastosowanie ramowe założenia sprawozdawczości finansowej w jednostce sektora publicznego są określone przez ramowe założenia legislacyjne i regulacyjne stosowne dla każdego systemu prawnego lub dla każdego obszaru geograficznego. Zagadnienia, które mogą być rozważane przy stosowaniu przez jednostkę mających zastosowanie wymogów sprawozdawczości finansowej oraz sposób ich zastosowania w kontekście charakteru i okoliczności jednostki i jej otoczenia, obejmują zagadnienie, czy jednostka stosuje pełną zasadę memoriału czy zasadę kasową zgodnie z Międzynarodowymi Standardami Rachunkowości Sektora Publicznego, czy też ich hybrydę.

W jaki sposób czynniki ryzyka nieodłącznego wpływają na podatność stwierdzeń na zniekształcenie (Zob. par. 19(c))

Załącznik 2 zapewnia przykłady zdarzeń i uwarunkowań, które mogą powodować powstawanie ryzyk istotnego zniekształcenia, sklasyfikowanych według czynników ryzyka nieodłącznego.

Dlaczego audytor rozumie czynniki ryzyka nieodłącznego rozumiejąc jednostkę i jej otoczenie oraz mające zastosowanie ramowe założenia sprawozdawczości finansowej

- A85. Zrozumienie jednostki i jej otoczenia oraz mających zastosowanie ramowych założeń sprawozdawczości finansowej pomaga audytorowi w identyfikowaniu zdarzeń lub warunków, których charakterystyka może mieć wpływ na podatność stwierdzeń dotyczących grup transakcji, sald kont lub ujawnień na zniekształcenia. Te cechy charakterystyczne są czynnikami ryzyka nieodłącznego. Czynniki ryzyka nieodłącznego mogą mieć wpływ na podatność stwierdzeń na zniekształcenia, wpływając na prawdopodobieństwo wystąpienia zniekształcenia lub wielkość zniekształcenia, jeżeli takie zniekształcenie wystąpi. Zrozumienie, w jaki sposób czynniki ryzyka nieodłącznego wpływają na podatność stwierdzeń na zniekształcenie, może pomóc audytorowi we wstępnym zrozumieniu prawdopodobieństwa lub wielkości zniekształceń, co pomaga audytorowi w identyfikowaniu ryzyk istotnego zniekształcenia na poziomie stwierdzeń zgodnie z paragrafem 28(b). Zrozumienie stopnia, w jakim czynniki ryzyka nieodłącznego wpływają na podatność stwierdzeń na zniekształcenie pomaga również audytorowi w dokonaniu oceny prawdopodobieństwa i wielkości ewentualnego zniekształcenia podczas szacowania ryzyka nieodłącznego zgodnie z paragrafem 31(a). W związku z tym, zrozumienie czynników ryzyka nieodłącznego może również pomóc audytorowi w zaprojektowaniu i wykonaniu dalszych procedur badania zgodnie z MSB 330.

- A86. Na identyfikację przez audytora ryzyk istotnego zniekształcenia na poziomie stwierdzeń oraz na oszacowanie ryzyka nieodłącznego mogą mieć również wpływ dowody badania uzyskane przez audytora podczas wykonywania innych procedur oszacowania ryzyka, dalszych procedur badania lub wypełniania innych wymogów opisanych w MSB (zobacz paragrafy A95, A103, A111, A121, A124 i A151).

Wpływ czynników ryzyka nieodłącznego na daną grupę transakcji, saldo konta lub ujawnienie

- A87. Zakres podatności na zniekształcenie danej grupy transakcji, salda konta lub ujawnienia powstającego na skutek złożoności lub subiektywizmu jest często ściśle związany z zakresem, w jakim podlegają one zmianom lub niepewności.

Przykład:

Jeżeli jednostka ma szacunek księgowy oparty na założeniach, których wybór podlega znaczącemu osądowi, na wycenę tego szacunku księgowego prawdopodobnie wpłynie zarówno subiektywizm, jak i niepewność.

- A88. Im większy stopień, w jakim dana grupa transakcji, saldo konta lub ujawnienie są podatne na zniekształcenie ze względu na złożoność lub subiektywizm, tym większa jest potrzeba stosowania przez audytora zawodowego sceptycyzmu. Ponadto, gdy grupa transakcji, saldo konta lub ujawnienie są podatne na zniekształcenie ze względu na złożoność, subiektywizm, zmianę lub niepewność, te czynniki ryzyka nieodłącznego mogą stwarzać możliwość stronniczości kierownictwa, niezależnie od tego, czy jest ona niezamierzona, czy zamierzona, oraz wpływać na podatność na zniekształcenie ze względu na stronniczość kierownictwa. Na identyfikację przez audytora ryzyk istotnego zniekształcenia oraz na oszacowanie ryzyka nieodłącznego na poziomie stwierdzeń, mają również wpływ wzajemne powiązania pomiędzy czynnikami ryzyka nieodłącznego.
- A89. Zdarzenia lub warunki, które mogą wpływać na podatność na zniekształcenie ze względu na stronniczość kierownictwa, mogą również wpłynąć na podatność na zniekształcenie ze względu na inne czynniki ryzyka oszustwa. W związku z tym, mogą to być stosowne informacje do wykorzystania zgodnie z paragrafem 24 w MSB 240, który wymaga, aby audytor ocenił, czy informacje uzyskane z innych procedur oszacowania ryzyka i związanych z nimi czynności wskazują, że występuje jeden lub więcej czynników ryzyka oszustwa.

Zrozumienie elementów systemu kontroli wewnętrznej jednostki (Zob. par. 21-27)

Załącznik 3 dalej opisuje, odpowiednio, charakter systemu kontroli wewnętrznej jednostki oraz nieodłączne ograniczenia kontroli wewnętrznej. Załącznik 3 zawiera również dalsze wyjaśnienia dotyczące elementów systemu kontroli wewnętrznej do celów MSB.

- A90. Zrozumienie przez audytora systemu kontroli wewnętrznej jednostki uzyskuje się poprzez procedury oszacowania ryzyka wykonywane w celu zrozumienia i oceny każdego z elementów systemu kontroli wewnętrznej określonego w paragrafach od 21 do 27.
- A91. Elementy systemu kontroli wewnętrznej jednostki dla celów niniejszego MSB niekoniecznie mogą odzwierciedlać, w jaki sposób jednostka projektuje, wdraża i utrzymuje swój system kontroli wewnętrznej albo w jaki sposób może ona klasyfikować poszczególne elementy. Jednostki mogą używać różnej terminologii lub ramowych założeń, aby opisać różne aspekty systemu kontroli wewnętrznej. Dla celów badania audytorzy mogą również używać innej

terminologii lub ramowych założeń pod warunkiem odniesienia się do wszystkich elementów opisanych w niniejszym MSB.

Skalowalność

A92. Sposób, w jaki system kontroli wewnętrznej jednostki jest projektowany, wdrażany i utrzymywany, różni się w zależności od wielkości i złożoności jednostki. Na przykład mniej złożone jednostki mogą używać mniej ustrukturyzowanych lub prostszych kontroli (tj. polityk i procedur), aby osiągnąć swoje cele.

Szczególne rozważania dla jednostek sektora publicznego

A93. Na audytorach jednostek sektora publicznego spoczywają często dodatkowe obowiązki w odniesieniu do kontroli wewnętrznej, na przykład, aby zaraportować o zgodności z ustalonym kodeksem postępowania lub sprawozdawczości dotyczącej wydatków względem budżetu. Audytorzy jednostek sektora publicznego mogą mieć także obowiązki, aby zaraportować o zgodności z przepisami prawa, regulacją lub innymi wytycznymi. W rezultacie ich rozważania dotyczące systemu kontroli wewnętrznej mogą być szersze i bardziej szczegółowe.

Technologia informacyjna w elementach systemu kontroli wewnętrznej jednostki

Załącznik 5 zawiera dalsze wytyczne dotyczące zrozumienia wykorzystania przez jednostkę IT w elementach systemu kontroli wewnętrznej.

A94. Ogólny cel i zakres badania nie różnią się niezależnie od tego, czy jednostka działa w środowisku głównie ręcznym, w pełni zautomatyzowanym, czy też w środowisku obejmującym jakąś kombinację elementów ręcznych i zautomatyzowanych (tj. kontrole ręczne i zautomatyzowane oraz inne zasoby wykorzystywane w systemie kontroli wewnętrznej jednostki).

Zrozumienie charakteru elementów systemu kontroli wewnętrznej jednostki

A95. Podczas dokonywania oceny skuteczności projektu kontroli oraz tego, czy zostały one wdrożone (zobacz paragrafy od A175 do A181), zrozumienie przez audytora każdego z elementów systemu kontroli wewnętrznej jednostki zapewnia wstępne zrozumienie, w jaki sposób jednostka identyfikuje ryzyka gospodarcze i jak na nie reaguje. Może to również wpłynąć w różny sposób na identyfikację i oszacowanie przez audytora ryzyk istotnego zniekształcenia (zobacz paragraf A86). Pomaga to audytorowi w zaprojektowaniu i wykonaniu dalszych procedur badania, w tym wszelkich planów przetestowania skuteczności działania kontroli. Na przykład:

- zrozumienie przez audytora środowiska kontroli w jednostce, procesu oszacowania ryzyka w jednostce oraz procesu monitorowania elementów kontroli przez jednostkę z większym prawdopodobieństwem wpływa na identyfikację i oszacowanie ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego,
- zrozumienie przez audytora systemu informacyjnego i komunikacji w jednostce, a także elementu czynności kontrolnych jednostki, z większym prawdopodobieństwem wpływa na identyfikację i oszacowanie ryzyk istotnego zniekształcenia na poziomie stwierdzeń.

Środowisko kontroli, proces oszacowania ryzyka w jednostce oraz proces monitorowania systemu kontroli wewnętrznej przez jednostkę (Zob. par. 21-24)

A96. Kontrole w środowisku kontroli, proces oszacowania ryzyka w jednostce oraz proces monitorowania systemu kontroli wewnętrznej przez jednostkę obejmują przede wszystkim kontrole pośrednie (tj. kontrole, które nie są wystarczająco precyzyjne, aby zapobiegać,

wykrywać lub korygować zniekształcenia na poziomie stwierdzeń, ale które wspierają inne kontrole, a zatem mogą mieć pośredni wpływ na prawdopodobieństwo, że zniekształcenie zostanie wykryte lub uda się mu zapobiec w odpowiednim czasie). Jednakże, niektóre kontrole w ramach tych elementów mogą być również kontrolami bezpośrednimi.

Dlatego od audytora wymagane jest, aby zrozumiał środowisko kontroli, proces oszacowania ryzyka w jednostce oraz proces monitorowania systemu kontroli wewnętrznej przez jednostkę

A97. Środowisko kontroli zapewnia ogólną podstawę działania innych elementów systemu kontroli wewnętrznej. Środowisko kontroli bezpośrednio nie zapobiega, nie wykrywa ani nie koryguje zniekształceń. Może ono jednak wpływać na skuteczność kontroli w innych elementach systemu kontroli wewnętrznej. Podobnie, proces oszacowania ryzyka w jednostce oraz jej proces monitorowania systemu kontroli wewnętrznej są zaprojektowane tak, aby działały w sposób, który także wspiera cały system kontroli wewnętrznej.

A98. Ze względu na to, że te elementy stanowią podstawę systemu kontroli wewnętrznej jednostki, wszelkie słabości w ich działaniu mogłyby mieć rozległy wpływ na sporządzenie sprawozdania finansowego. W związku z tym, zrozumienie i ocena tych elementów przez audytora wpływają na identyfikację i oszacowanie ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego przez audytora, a także mogą mieć wpływ na identyfikację i oszacowanie ryzyk istotnego zniekształcenia na poziomie stwierdzeń. Ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego mają wpływ na zaprojektowanie przez audytora ogólnych reakcji, w tym, jak wyjaśniono w MSB 330, wpływ na rodzaj, rozłożenie w czasie i zakres dalszych procedur audytora³⁵.

Uzyskanie zrozumienia środowiska kontroli (Zob. par. 21)

Skalowalność

A99. Charakter środowiska kontroli w mniej złożonej jednostce jest prawdopodobnie inny niż środowiska kontroli w jednostce bardziej złożonej. Na przykład, osoby sprawujące nadzór w mniej złożonych jednostkach mogą nie obejmować niezależnych lub zewnętrznych członków, a tam, gdzie nie ma innych właścicieli, rolę nadzorczą może bezpośrednio sprawować zarządzający właściciel. W związku z tym, niektóre rozważania dotyczące środowiska kontroli jednostki mogą być mniej stosowne lub mogą nie mieć zastosowania.

A100. Ponadto, dowody badania dotyczące elementów środowiska kontroli mogą być w mniej złożonych jednostkach niedostępne w formie dokumentów, w szczególności, gdy komunikacja pomiędzy kierownictwem i innymi pracownikami jest nieformalna, ale dowody mogą być nadal odpowiednio stosowne i wiarygodne w danych okolicznościach.

Przykłady:

- Struktura organizacyjna w mniej złożonej jednostce będzie prawdopodobnie prostsza i może obejmować niewielką liczbę pracowników zaangażowanych w funkcje związane ze sprawozdawczością finansową.
- Jeżeli rolę nadzoru podejmuje bezpośrednio zarządzający właściciel, audytor może stwierdzić, że niezależność osób sprawujących nadzór nie jest stosowna.
- Mniej złożone jednostki mogą nie mieć pisemnego kodeksu postępowania, ale zamiast tego rozwijać kulturę, która kładzie nacisk na ważność uczciwości i etycznego

³⁵ MSB 330, paragrafy A1–A3.

postępowania, poprzez komunikację ustną i przykład kierownictwa. Dlatego postawa, świadomość oraz działania kierownictwa lub zarządzającego właściciela są szczególnie ważne dla zrozumienia przez audytora środowiska kontroli mniej złożonej jednostki.

Zrozumienie środowiska kontroli (Zob. par. 21(a))

A101. Dowody badania dotyczące zrozumienia środowiska kontroli przez audytora mogą zostać uzyskane poprzez połączenie zapytań i innych procedur oszacowania ryzyka (tj. potwierdzenie zapytań poprzez obserwację lub inspekcję dokumentów).

A102. Rozważając zakres, w jakim kierownictwo wykazuje się zaangażowaniem na rzecz uczciwości i wartości etycznych, audytor może uzyskać zrozumienie poprzez zapytania kierowane do kierownictwa i pracowników, a także poprzez rozważenie informacji ze źródeł zewnętrznych na następujące tematy:

- w jaki sposób kierownictwo komunikuje pracownikom swoje poglądy na temat praktyk biznesowych i etycznego zachowania oraz
- inspekcji pisemnego kodeksu postępowania kierownictwa i obserwowania, czy kierownictwo działa w sposób, który wspiera ten kodeks.

Dokonywanie oceny środowiska kontroli (Zob. par. 21(b))

Dlaczego audytor ocenia środowisko kontroli

A103. Ocena audytora dotycząca tego, w jaki sposób jednostka wykazuje zachowanie spójne ze zobowiązaniem jednostki do uczciwości i wartości etycznych; czy środowisko kontroli zapewnia odpowiednią podstawę dla innych elementów systemu kontroli wewnętrznej jednostki; oraz czy jakiegokolwiek zidentyfikowane słabości kontroli podważają inne elementy systemu kontroli wewnętrznej, pomaga audytorowi w identyfikowaniu potencjalnych kwestii w innych elementach systemu kontroli wewnętrznej. Dzieje się tak, ponieważ środowisko kontroli jest podstawą dla innych elementów systemu kontroli wewnętrznej jednostki. Ocena ta może również pomóc audytorowi w zrozumieniu ryzyk, na jakie narażona jest jednostka, a tym samym w identyfikacji i oszacowaniu ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego i stwierdzeń (zobacz paragraf A86).

Ocena środowiska kontroli przez audytora

A104. Ocena środowiska kontroli przez audytora opiera się na zrozumieniu uzyskanym zgodnie z paragrafem 21(a).

A105. Niektóre jednostki mogą być zdominowane przez jedną osobę, która może korzystać z dużej swobody. Działania i postawy tej osoby mogą mieć rozległy wpływ na kulturę jednostki, co z kolei może mieć rozległy wpływ na środowisko kontroli. Taki wpływ może być pozytywny lub negatywny.

Przykład:

Bezpośrednie zaangażowanie jednej osoby może być kluczowe dla umożliwienia jednostce osiągnięcia wzrostu i innych celów, a także może znacząco przyczynić się do skutecznego systemu kontroli wewnętrznej. Z drugiej strony, taka koncentracja wiedzy i uprawnień może również prowadzić do zwiększonej podatności na zniekształcenie poprzez omijanie kontroli przez kierownictwo.

A106. Audytor może rozważyć, w jaki sposób filozofia i styl działania kierownictwa wyższego szczebla może wpływać na różne elementy środowiska kontroli, biorąc pod uwagę zaangażowanie niezależnych członków wśród osób sprawujących nadzór.

A107. Chociaż środowisko kontroli może zapewniać odpowiednią podstawę dla systemu kontroli wewnętrznej i może pomóc w ograniczeniu ryzyka oszustwa, odpowiednie środowisko kontroli niekoniecznie jest skutecznym środkiem odstraszającym oszustwa.

Przykład:

Polityki i procedury dotyczące zasobów ludzkich nakierowane na zatrudnianie kompetentnego personelu finansowego, księgowego i IT mogą ograniczyć ryzyko błędów w przetwarzaniu i rejestrowaniu informacji finansowych. Jednakże, takie polityki i procedury mogą nie złagodzić obejścia kontroli przez kierownictwo wyższego szczebla (np., aby zawyżyć zyski).

A108. Ocena środowiska kontroli przez audytora w odniesieniu do wykorzystania IT przez jednostkę może obejmować takie zagadnienia jak:

- czy nadzór nad IT jest współmierny do charakteru i złożoności jednostki oraz jej działalności gospodarczej, umożliwionych przez IT, w tym złożoności lub dojrzałości platformy technologicznej lub architektury jednostki oraz zakresu, w jakim jednostka polega na aplikacjach IT, aby wspierać swoją sprawozdawczość finansową,
- struktura organizacyjna zarządzania w zakresie IT i przydzielonych zasobów (na przykład czy jednostka zainwestowała w odpowiednie środowisko IT i niezbędne ulepszenia, lub czy zatrudniła wystarczającą liczbę odpowiednio wykwalifikowanych osób, w tym, gdy jednostka korzysta z komercyjnego oprogramowania (bez modyfikacji lub z ograniczonymi modyfikacjami)).

Uzyskanie zrozumienia procesu oszacowania ryzyka w jednostce (Zob. par. 22-23)

Zrozumienie procesu oszacowania ryzyka w jednostce (Zob. par. 22(a))

A109. Jak wyjaśniono w paragrafie A62, nie wszystkie ryzyka gospodarcze powodują powstanie ryzyk istotnego zniekształcenia. Uzyskując zrozumienie, w jaki sposób kierownictwo i osoby sprawujące nadzór zidentyfikowały ryzyka gospodarcze stosowne dla sporządzenia sprawozdania finansowego oraz zdecydowały o działaniach mających na celu reakcję na te ryzyka, zagadnienia, które audytor może rozważyć, obejmują sposób w jaki kierownictwo lub odpowiednio, osoby sprawujące nadzór:

- określiły cele jednostki z dokładnością i jasnością wystarczającą, aby umożliwić identyfikację i oszacowanie ryzyk związanych z tymi celami,
- zidentyfikowały ryzyka dla osiągnięcia celów jednostki i przeanalizowały ryzyka jako podstawę do określenia sposobu, w jaki ryzyka te powinny być zarządzane, oraz
- rozważyły potencjał dla oszustwa w trakcie rozważania ryzyk dla osiągnięcia celów jednostki³⁶.

A110. Audytor może rozważyć następstwa takich ryzyk gospodarczych dla sporządzenia sprawozdania finansowego jednostki i innych aspektów jej systemu kontroli wewnętrznej.

³⁶ MSB 240, paragraf 19.

Dokonywanie oceny procesu oszacowania ryzyka jednostki (Zob. par. 22(b))

Dlaczego audytor ocenia, czy proces oszacowania ryzyka w jednostce jest odpowiedni

A111. Ocena procesu oszacowania ryzyka w jednostce przez audytora może pomóc audytorowi w zrozumieniu, gdzie jednostka zidentyfikowała ryzyka, jakie mogą wystąpić oraz w jaki sposób jednostka zareagowała na te ryzyka. Ocena przez audytora sposobu, w jaki jednostka identyfikuje swoje ryzyka gospodarcze oraz sposobu, w jaki ocenia ona i reaguje na te ryzyka, pomaga audytorowi w zrozumieniu, czy ryzyka, na które narażona jest jednostka, zostały zidentyfikowane, oszacowane i odniesiono się do nich odpowiednio do charakteru i złożoności jednostki. Ta ocena może również pomóc audytorowi w zidentyfikowaniu i oszacowaniu ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego i na poziomie stwierdzeń. (Zobacz paragraf A86)

Dokonywanie oceny czy proces oszacowania ryzyka w jednostce jest odpowiedni (Zob. par. 22(b))

A112. Ocena odpowiedniości procesu oszacowania ryzyka w jednostce przez audytora jest oparta na zrozumieniu uzyskanym zgodnie z paragrafem 22(a).

Skalowalność

A113. To, czy proces oszacowania ryzyka w jednostce jest odpowiedni w stosunku do okoliczności jednostki, biorąc pod uwagę charakter i złożoność jednostki, jest sprawą zawodowego osądu audytora.

Przykład:

W niektórych mniej złożonych jednostkach, a w szczególności w jednostkach zarządzanych przez właściciela, odpowiednie oszacowanie ryzyka może zostać wykonane poprzez bezpośrednie zaangażowanie kierownictwa lub zarządzającego właściciela (np. kierownik lub zarządzający właściciel może rutynowo poświęcać czas na monitorowanie działań konkurentów i innego postępu na rynku, aby zidentyfikować pojawiające się ryzyka gospodarcze). Dowody tego oszacowania ryzyka występującego w tego typu jednostkach często nie są formalnie udokumentowane, ale z rozmów, jakie audytor prowadzi z kierownictwem może ewidentnie wynikać, że kierownictwo faktycznie wykonuje procedury oszacowania ryzyka.

Uzyskanie zrozumienia procesu monitorowania przez jednostkę systemu kontroli wewnętrznej jednostki (Zob. par. 24)

Skalowalność

A114. W mniej złożonych jednostkach, a w szczególności w jednostkach zarządzanych przez właściciela, zrozumienie przez audytora procesu monitorowania systemu kontroli wewnętrznej przez jednostkę często koncentruje się na tym, w jaki sposób kierownictwo lub zarządzający właściciel jest bezpośrednio zaangażowany w działalność, ponieważ mogą nie występować żadne inne działania monitorujące.

Przykład:

Kierownictwo może otrzymać od klientów skargi dotyczące nieścisłości w ich miesięcznych sprawozdaniach, które stanowią ostrzeżenie dla zarządzającego właściciela o problemach z określeniem terminu, w którym płatności klientów są ujmowane w księgach rachunkowych.

A115. Dla jednostek, w których nie istnieje formalny proces monitorowania systemu kontroli wewnętrznej, zrozumienie procesu monitorowania systemu kontroli wewnętrznej może obejmować zrozumienie okresowych przeglądów informacji z zakresu rachunkowości zarządczej, które są zaprojektowane, aby przyczyniać się do tego, w jaki sposób jednostka zapobiega lub wykrywa zniekształcenia.

Zrozumienie procesu monitorowania systemu kontroli wewnętrznej przez jednostkę (Zob. par. 24(a))

A116. Zagadnienia, które mogą być stosowne dla audytora do rozważenia podczas uzyskiwania zrozumienia sposobu, w jaki jednostka monitoruje swój system kontroli wewnętrznej, obejmują:

- projekt działań monitorujących, na przykład, czy jest to monitoring okresowy, czy ciągły,
- wykonanie i częstotliwość działań monitorujących,
- ocenę wyników działań monitorujących, w odpowiednim czasie, aby ustalić, czy kontrole były skuteczne oraz
- w jaki sposób zareagowano na zidentyfikowane słabości poprzez odpowiednie działania naprawcze, w tym terminowe informowanie o takich słabościach osób odpowiedzialnych za podjęcie działań naprawczych.

A117. Audytor może również rozważyć, w jaki sposób proces monitorowania przez jednostkę systemu kontroli wewnętrznej odnosi się do monitorowania kontroli przetwarzania informacji, które wiążą się z wykorzystaniem IT. Może to obejmować, na przykład:

- kontrole monitorujące złożone środowiska IT, które:
 - oceniają ciągłą skuteczność projektu kontroli przetwarzania informacji i modyfikują je, jeżeli to odpowiednie, w odniesieniu do zmian warunków, lub
 - oceniają skuteczność działania kontroli przetwarzania informacji,
- kontrole monitorujące uprawnienia stosowane w zautomatyzowanych kontrolach przetwarzania informacji, które wymuszają podział obowiązków,
- kontrole monitorujące w jaki sposób błędy lub słabości kontroli w zakresie automatyzacji sprawozdawczości finansowej są identyfikowane i reaguje się na nie.

Zrozumienie funkcji audytu wewnętrznego w jednostce (Zob. par. 24(a)(ii))

Załącznik 4 określa dalsze rozważania dotyczące zrozumienia funkcji audytu wewnętrznego w jednostce.

A118. Zapytania kierowane przez audytora do odpowiednich osób wewnątrz funkcji audytu wewnętrznego pomagają audytorowi uzyskać zrozumienie charakteru obowiązków funkcji audytu wewnętrznego. Jeżeli audytor ustali, że obowiązki funkcji są związane ze sprawozdawczością finansową jednostki, audytor może uzyskać dalsze zrozumienie działań, które zostały lub mają zostać wykonane przez funkcję audytu wewnętrznego, dokonując przeglądu planu audytu funkcji audytu wewnętrznego za dany okres, jeżeli jakkolwiek istnieje, oraz omawiając ten plan z odpowiednimi osobami w ramach tej funkcji. Zrozumienie to, wraz z informacjami uzyskanymi poprzez zapytania audytora, może również dostarczyć informacji, które są bezpośrednio stosowne dla identyfikacji i oszacowania ryzyk istotnego zniekształcenia przez audytora. Jeżeli, w oparciu o wstępne zrozumienie przez audytora funkcji audytu wewnętrznego, audytor spodziewa się wykorzystać pracę funkcji audytu wewnętrznego, aby

zmodyfikować rodzaj lub rozłożenie w czasie, lub zmniejszyć zakres procedur badania, które mają zostać wykonane, zastosowanie ma MSB 610 (zmieniony w 2013 r.)³⁷.

Inne źródła informacji wykorzystywane w procesie monitorowania systemu kontroli wewnętrznej w jednostce

Zrozumienie źródeł informacji (Zob. par. 24(b))

A119. Czynności monitorowania przez kierownictwo mogą wykorzystywać informacje z komunikacji od stron zewnętrznych, takich jak zażalenia klientów lub uwagi regulatora, które mogą wskazywać problemy lub podkreślać obszary wymagające poprawienia.

Dlaczego wymagane jest, aby audytor rozumiał źródła informacji wykorzystywanych do monitorowania systemu kontroli wewnętrznej w jednostce

A120. Zrozumienie przez audytora źródeł informacji wykorzystywanych przez jednostkę do monitorowania systemu kontroli wewnętrznej jednostki, w tym stwierdzenie, czy wykorzystywane informacje są stosowne i wiarygodne, pomaga audytorowi w dokonaniu oceny, czy proces monitorowania systemu kontroli wewnętrznej w jednostce jest właściwy. Jeżeli kierownictwo zakłada, że informacje wykorzystywane do monitorowania są stosowne i wiarygodne, nie mając podstaw do takiego założenia, błędy, które mogą występować w informacjach, mogłyby potencjalnie prowadzić do wyciągania przez kierownictwo błędnych wniosków z jego działań monitorujących.

Dokonywanie oceny procesu monitorowania systemu kontroli wewnętrznej w jednostce (Zob. par. 24(c))

Dlaczego audytor ocenia, czy proces monitorowania systemu kontroli wewnętrznej w jednostce jest odpowiedni

A121. Ocena audytora dotycząca sposobu dokonywania przez jednostkę bieżących i odrębnych ocen w celu monitorowania skuteczności kontroli, pomaga audytorowi zrozumieć, czy inne elementy systemu kontroli wewnętrznej jednostki istnieją i funkcjonują, a zatem pomaga zrozumieć inne elementy systemu kontroli wewnętrznej jednostki. Ta ocena może również pomóc audytorowi w zidentyfikowaniu i oszacowaniu ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego i na poziomie stwierdzeń (zobacz paragraf A86).

Dokonywanie oceny czy proces monitorowania systemu kontroli wewnętrznej w jednostce jest odpowiedni (Zob. par. 24(c))

A122. Ocena przez audytora odpowiedności procesu monitorowania systemu kontroli wewnętrznej w jednostce jest oparta na zrozumieniu przez audytora procesu monitorowania systemu kontroli wewnętrznej w jednostce.

System informacyjny i komunikacja oraz czynności kontrolne (Zob. par. 25-26)

A123. Kontrole w systemie informacyjnym i komunikacji oraz elementy czynności kontrolnych stanowią przede wszystkim kontrole bezpośrednie (tj. kontrole, które są wystarczająco dokładne, aby zapobiegać, wykrywać lub korygować zniekształcenia na poziomie stwierdzeń).

³⁷ MSB 610 (zmieniony w 2013 r.) *Wykorzystanie pracy audytorów wewnętrznych*.

Dlaczego wymagane jest zrozumienie przez audytora systemu informacyjnego i komunikacji oraz kontroli w ramach elementu czynności kontrolnych

A124. Wymagane jest, aby audytor rozumiał system informacyjny i komunikację w jednostce, ponieważ zrozumienie polityk jednostki określających przepływy transakcji oraz inne aspekty czynności przetwarzania informacji w jednostce stosowne dla sporządzenia sprawozdania finansowego, i dokonanie oceny, czy dany element odpowiednio wspiera sporządzenie sprawozdania finansowego jednostki, pomaga audytorowi w identyfikacji i oszacowaniu ryzyk istotnego zniekształcenia na poziomie stwierdzeń. To zrozumienie i ocena mogą również skutkować zidentyfikowaniem ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego, gdy wyniki procedur audytora są niespójne z oczekiwaniami dotyczącymi systemu kontroli wewnętrznej jednostki, które mogły zostać ustalone na podstawie informacji uzyskanych w trakcie procesu akceptacji lub kontynuacji zlecenia (zobacz paragraf A86).

A125. Od audytora wymagane jest, aby zidentyfikował konkretne kontrole w elemencie czynności kontrolnych oraz ocenił projekt i ustalił, czy kontrole zostały wdrożone, ponieważ pomaga to audytorowi w zrozumieniu podejścia kierownictwa do reakcji na pewne ryzyka i w związku z tym zapewnia podstawę do zaprojektowania i wykonania dalszych procedur badania odpowiadających na te ryzyka zgodnie z wymogami MSB 330. Im wyżej na skali ryzyka nieodłącznego oszacowane jest ryzyko, tym bardziej przekonujące muszą być dowody badania. Nawet, gdy audytor nie planuje testowania skuteczności działania zidentyfikowanych kontroli, zrozumienie audytora może nadal wpływać na zaprojektowanie rodzaju, rozłożenia w czasie i zakresu procedur badania wiarygodności, które odpowiadają na związane z nimi ryzyka istotnego zniekształcenia.

Iteracyjny charakter zrozumienia i oceny przez audytora systemu informacyjnego i komunikacji oraz czynności kontrolnych

A126. Jak wyjaśniono w paragrafie A49, zrozumienie przez audytora jednostki i jej otoczenia oraz mających zastosowanie ramowych założeń sprawozdawczości finansowej może pomóc audytorowi w opracowaniu wstępnych oczekiwań dotyczących grup transakcji, sald kont i ujawnień, które mogą być znaczącymi grupami transakcji, saldami kont i ujawnieniami. Uzyskując zrozumienie elementu systemu informacyjnego i komunikacji zgodnie z paragrafem 25(a), audytor może wykorzystać te wstępne oczekiwania w celu określenia zakresu zrozumienia czynności przetwarzania informacji w jednostce, które należy uzyskać.

A127. Zrozumienie systemu informacyjnego przez audytora obejmuje zrozumienie polityk, które określają przepływy informacji dotyczących znaczących grup transakcji jednostki, sald kont oraz ujawnień, a także innych powiązanych aspektów czynności przetwarzania informacji w jednostce. Informacje te, jak również informacje uzyskane w wyniku oceny przez audytora systemu informacyjnego, mogą potwierdzać lub dalej wpływać na oczekiwania audytora dotyczące początkowo zidentyfikowanych znaczących grup transakcji, sald kont i ujawnień (zobacz paragraf A126).

A128. Uzyskując zrozumienie, w jaki sposób informacje dotyczące znaczących grup transakcji, sald kont i ujawnień przepływają do, poprzez i z systemu informacyjnego jednostki, audytor może również zidentyfikować kontrole w ramach elementu czynności kontrolnych, których identyfikacja jest wymagana zgodnie z paragrafem 26(a). Identyfikacja i ocena kontroli w ramach elementu czynności kontrolnych przez audytora może w pierwszej kolejności skoncentrować się na kontrolach zapisów w dzienniku oraz kontrolach, które audytor planuje przetestować pod kątem skuteczności działania projektując rodzaj, rozłożenie w czasie i zakres procedur wiarygodności.

A129. Oszacowanie ryzyka nieodłącznego przez audytora może również wpłynąć na identyfikację kontroli w elemencie czynności kontrolnych. Na przykład, identyfikacja przez audytora kontroli odnoszących się do znaczących ryzyk może być wykonalna tylko wtedy, gdy audytor oszacował ryzyko nieodłączne na poziomie stwierdzeń zgodnie z paragrafem 31. Ponadto, kontrole odnoszące się do ryzyk, dla których audytor stwierdził, że same procedury wiarygodności nie zapewniają wystarczających odpowiednich dowodów badania (zgodnie z paragrafem 33), mogą być możliwe do zidentyfikowania tylko, gdy audytor oszacował ryzyko nieodłączne.

A130. Na identyfikację i oszacowanie ryzyk istotnego zniekształcenia na poziomie stwierdzeń przez audytora wpływają:

- zrozumienie przez audytora polityk jednostki w zakresie czynności przetwarzania informacji w systemie informacyjnym i elementu komunikacji, oraz
- identyfikacja i ocena kontroli w elemencie czynności kontrolnych przez audytora.

Uzyskanie zrozumienia systemu informacyjnego i komunikacji (Zob. par. 25)

Załącznik 3, Paragrafy 15-19, przedstawia dalsze rozważania dotyczące systemu informacyjnego i komunikacji.

Skalowalność

A131. System informacyjny i związane z nim procesy gospodarcze w mniej złożonych jednostkach są prawdopodobnie mniej skomplikowane niż w większych jednostkach i prawdopodobnie obejmują mniej złożone środowisko IT; jednakże rola systemu informacyjnego jest równie ważna. Mniej złożone jednostki z bezpośrednim zaangażowaniem kierownictwa mogą nie wymagać obszernych opisów procedur księgowych, skomplikowanej dokumentacji księgowej lub pisemnych polityk. Zrozumienie stosownych aspektów systemu informacyjnego jednostki może zatem wymagać mniejszego wysiłku podczas badania mniej złożonej jednostki i może obejmować większą ilość pytań niż obserwacji lub inspekcji dokumentacji. Potrzeba uzyskania zrozumienia pozostaje jednak ważna, aby zapewnić podstawę do zaprojektowania dalszych procedur badania zgodnie z MSB 330 i może dodatkowo pomóc audytorowi w zidentyfikowaniu lub oszacowaniu ryzyk istotnego zniekształcenia (zobacz paragraf A86).

Uzyskanie zrozumienia systemu informacyjnego (Zob. par. 25(a))

A132. W skład systemu kontroli wewnętrznej jednostki wchodzi aspekty, które odnoszą się do celów sprawozdawczych jednostki, w tym jej celów sprawozdawczości finansowej, ale mogą one również obejmować aspekty odnoszące się do jej działalności lub celów w zakresie zgodności, gdy takie aspekty są stosowne dla sprawozdawczości finansowej. Zrozumienie sposobu, w jaki jednostka inicjuje transakcje oraz ujmuje informacje w ramach zrozumienia systemu informacyjnego przez audytora może obejmować informacje o systemach jednostki (jej politykach) zaprojektowanych w celu odniesienia się do zgodności i celów operacyjnych, ponieważ takie informacje są stosowne dla sporządzenia sprawozdania finansowego. Ponadto, niektóre jednostki mogą posiadać systemy informacyjne, które są wysoce zintegrowane tak, że kontrole mogą zostać zaprojektowane w taki sposób, aby jednocześnie osiągać cele sprawozdawczości finansowej, zgodności i operacyjne oraz ich kombinacje.

A133. Zrozumienie systemu informacyjnego jednostki obejmuje również zrozumienie zasobów, które mają być wykorzystywane w działaniach jednostki w zakresie przetwarzania informacji. Informacje o zaangażowanych zasobach ludzkich, które mogą być stosowne dla zrozumienia ryzyk dla integralności systemu informacyjnego, obejmują:

- kompetencje osób podejmujących pracę,
- czy istnieją adekwatne zasoby oraz
- czy istnieje odpowiedni podział obowiązków.

A134. Zagadnienia, które audytor może rozważyć podczas uzyskiwania zrozumienia polityk określających przepływy informacji dotyczących znaczących grup transakcji, sald kont oraz ujawnień jednostki w systemie informacyjnym i elementu komunikacji, obejmują charakter:

- (a) danych lub informacji odnoszących się do transakcji, innych zdarzeń i warunków, które mają być przetwarzane,
- (b) przetwarzania informacji w celu zachowania integralności tych danych lub informacji, oraz
- (c) procesów informacyjnych, personelu i innych zasobów wykorzystywanych w procesie przetwarzania informacji.

A135. Uzyskanie zrozumienia procesów gospodarczych jednostki, które obejmuje w jaki sposób transakcje są inicjowane, pomaga audytorowi w uzyskaniu zrozumienia systemu informacyjnego jednostki w sposób, który jest odpowiedni do okoliczności jednostki.

A136. Zrozumienie systemu informacyjnego przez audytora może zostać uzyskane na różne sposoby i może obejmować:

- zapytania skierowane do stosownych pracowników na temat procedur wykorzystywanych do inicjowania, rejestrowania, przetwarzania i raportowania transakcji lub na temat procesu sprawozdawczości finansowej jednostki,
- inspekcję instrukcji dotyczących polityki lub procesu lub innej dokumentacji systemu informacyjnego jednostki,
- obserwację wykonania polityk lub procedur przez personel jednostki lub
- wybór transakcji i śledzenie ich poprzez mający zastosowanie proces w systemie informacyjnym (tj. wykonanie procedury walk-through).

Zautomatyzowane narzędzia i techniki

A137. Audytor może również korzystać ze zautomatyzowanych technik, aby uzyskać bezpośredni dostęp lub cyfrowo pobrać z baz danych w systemie informacyjnym jednostki, w którym przechowywane są zapisy księgowe dotyczące transakcji. Poprzez zastosowanie zautomatyzowanych narzędzi lub technik w odniesieniu do tych informacji, audytor może potwierdzić uzyskane zrozumienie na temat sposobu, w jaki transakcje przepływają przez system informacyjny, śledząc zapisy w dzienniku lub inne zapisy cyfrowe dotyczące konkretnej transakcji lub całej populacji transakcji, od ich zainicjowania w zapisach księgowych, aż po zapis w księdze głównej. Analiza kompletnych lub dużych zbiorów transakcji może również skutkować zidentyfikowaniem odchyleń od normalnych lub oczekiwanych procedur przetwarzania tych transakcji, co może skutkować zidentyfikowaniem ryzyk istotnego zniekształcenia.

Informacje uzyskane spoza ksiąg głównej i pomocniczych

A138. Sprawozdanie finansowe może zawierać informacje, które zostały uzyskane spoza księgi głównej i ksiąg pomocniczych. Przykłady takich informacji, które audytor może rozważyć, obejmują:

- informacje uzyskane z umów leasingu stosowne dla ujawnień w sprawozdaniu finansowym,

- informacje ujawniane w sprawozdaniu finansowym, które są sporządzane przez system zarządzania ryzykiem jednostki,
- informacje o wartości godziwej sporządzone przez ekspertów kierownictwa i ujawnione w sprawozdaniu finansowym,
- informacje ujawnione w sprawozdaniu finansowym, które zostały uzyskane z modeli lub z innych obliczeń wykorzystywanych, aby opracować szacunki księgowe ujęte lub ujawnione w sprawozdaniu finansowym, w tym informacje dotyczące danych bazowych i założeń wykorzystanych w tych modelach, takie jak:
 - założenia opracowane wewnętrznie, które mogą mieć wpływ na okres użyteczności składnika aktywów, lub
 - dane takie jak stopy procentowe, na które wpływ mają czynniki znajdujące się poza kontrolą jednostki,
- informacje ujawnione w sprawozdaniu finansowym dotyczące analiz wrażliwości wynikających z modeli finansowych, które pokazują, że kierownictwo rozważyło alternatywne założenia,
- informacje ujęte lub ujawnione w sprawozdaniu finansowym, które zostały uzyskane z deklaracji i ewidencji podatkowych jednostki,
- informacje ujawniane w sprawozdaniu finansowym, które zostały uzyskane z analiz sporządzonych w celu wsparcia oceny kierownictwa odnośnie do zdolności jednostki do kontynuowania działalności, takie jak ujawnienia, jeżeli jakiegokolwiek występują, dotyczące zdarzeń lub warunków, które zostały zidentyfikowane, a które mogą budzić znaczące wątpliwości co do zdolności jednostki do kontynuowania działalności³⁸.

A139. Pewne kwoty lub ujawnienia w sprawozdaniu finansowym jednostki (takie jak ujawnienia na temat ryzyka kredytowego, ryzyka płynności i ryzyka rynkowego) mogą być oparte na informacjach uzyskanych z systemu zarządzania ryzykiem w jednostce. Jednakże od audytora nie jest wymagane zrozumienie wszystkich aspektów systemu zarządzania ryzykiem, ale używał zawodowego osądu podczas ustalania niezbędnego zrozumienia.

Wykorzystanie przez jednostkę technologii informacyjnych w systemie informacyjnym

Dlaczego audytor uzyskuje zrozumienie środowiska IT stosownego dla systemu informacyjnego

A140. Zrozumienie systemu informacyjnego przez audytora obejmuje środowisko IT stosowne dla przepływów transakcji oraz przetwarzania informacji w systemie informacyjnym jednostki, ponieważ korzystanie przez jednostkę z aplikacji IT lub innych aspektów środowiska IT może spowodować powstanie ryzyk wynikających z korzystania z IT.

A141. Zrozumienie modelu biznesowego jednostki i sposobu, w jaki integruje on wykorzystanie IT, może również zapewnić użyteczny kontekst dla charakteru i zakresu IT oczekiwanego w systemie informacyjnym.

Zrozumienie wykorzystania IT przez jednostkę

A142. Zrozumienie środowiska IT przez audytora może skupiać się na identyfikacji i zrozumieniu charakteru i liczby konkretnych aplikacji IT oraz innych aspektów środowiska IT, które są stosowne dla przepływu transakcji i przetwarzania informacji w systemie informacyjnym. Zmiany w przepływie transakcji lub informacji w systemie informacyjnym mogą wynikać ze zmian

³⁸ MSB 570 (zmieniony), paragrafy 19-20.

programowych w aplikacjach IT lub bezpośrednich zmian danych w bazach danych zaangażowanych w przetwarzanie lub przechowywanie tych transakcji lub informacji.

A143. Audytor może zidentyfikować aplikacje IT oraz wspierającą je infrastrukturę IT jednocześnie ze zrozumieniem przez audytora sposobu, w jaki informacje dotyczące znaczących grup transakcji, sald kont oraz ujawnień wpływają do systemu informacyjnego jednostki, przepływają przez ten system i z niego wypływają.

Uzyskanie zrozumienia komunikacji jednostki (Zob. par. 25(b))

Skalowalność

A144. W większych, bardziej złożonych jednostkach, informacje, które audytor może rozważyć, uzyskując zrozumienie komunikacji w jednostce, mogą pochodzić z podręczników polityk i podręczników sprawozdawczości finansowej.

A145. W mniej złożonych jednostkach komunikacja może być mniej ustrukturyzowana (np. można nie korzystać z formalnych podręczników) ze względu na mniej poziomów odpowiedzialności i większą widoczność i dostępność kierownictwa. Niezależnie od wielkości jednostki, otwarte kanały komunikacji ułatwiają raportowanie wyjątków i pracę nad nimi.

Dokonywanie oceny, czy stosowne aspekty systemu informacyjnego wspomagają sporządzanie sprawozdania finansowego jednostki (Zob. par. 25(c))

A146. Ocena audytora czy system informacyjny i komunikacja w jednostce odpowiednio wspierają sporządzenie sprawozdania finansowego, opiera się na zrozumieniu uzyskanym w paragrafach 25(a)-(b).

Czynności kontrolne (Zob. par. 26)

Kontrole w elemencie czynności kontrolnych

Załącznik 3, paragrafy 20 i 21 przedstawiają dalsze rozważania dotyczące czynności kontrolnych.

A147. Element czynności kontrolnych obejmuje kontrole, które są zaprojektowane, aby zapewnić właściwe stosowanie polityk (które są również kontrolami) we wszystkich innych elementach systemu kontroli wewnętrznej jednostki i obejmuje zarówno kontrole bezpośrednie, jak i pośrednie.

Przykład:

Kontrole, które jednostka ustanowiła, aby zapewnić, że jej personel prawidłowo przelicza i rejestruje roczny spis z natury zapasów, wiążą się bezpośrednio z ryzykami istotnego zniekształcenia stosownymi dla stwierdzeń istnienia i kompletności dla salda konta zapasów.

A148. Identyfikacja i ocena kontroli przez audytora w ramach elementu czynności kontrolnych jest skupiona na kontrolach przetwarzania informacji, które są kontrolami stosowanymi podczas przetwarzania informacji w systemie informacyjnym jednostki, które bezpośrednio odnoszą się do ryzyk integralności informacji (tj. kompletności, dokładności i poprawności transakcji oraz innych informacji). Jednakże, od audytora nie jest wymagane, aby identyfikował i oceniał wszystkie kontrole przetwarzania informacji związane z politykami jednostki, które określają przepływy transakcji oraz inne aspekty czynności przetwarzania informacji jednostki dla znaczących grup transakcji, sald kont i ujawnień.

A149. Mogą również istnieć kontrole bezpośrednie, które występują w środowisku kontroli, w procesie oszacowania ryzyka w jednostce lub w procesie monitorowania systemu kontroli wewnętrznej w jednostce, które mogą być zidentyfikowane zgodnie z paragrafem 26. Jednakże, im bardziej pośredni jest związek pomiędzy kontrolami, które wspierają inne kontrole, a kontrolą, która jest rozważana, tym mniejsza może być skuteczność tej kontroli w zapobieganiu lub wykrywaniu i korygowaniu powiązanych zniekształceń.

Przykład:

Przegląd przez kierownika sprzedaży podsumowań działalności handlowej poszczególnych sklepów w regionie, zwykle jest tylko pośrednio powiązany z ryzykami istotnego zniekształcenia stosownymi dla stwierdzenia kompletności dla przychodów ze sprzedaży. W związku z tym może być mniej skuteczny w reagowaniu na te ryzyka niż kontrole bardziej bezpośrednio powiązane z tym stwierdzeniem, takie jak porównywanie dokumentów przewozowych z fakturami.

A150. Paragraf 26 wymaga również, aby audytor zidentyfikował i ocenił ogólne kontrole IT dla aplikacji IT i innych aspektów środowiska IT, które audytor określił jako podlegające ryzykom powstającym z powodu wykorzystania IT, ponieważ ogólne kontrole IT wspierają dalsze skuteczne funkcjonowanie kontroli przetwarzania informacji. Sama ogólna kontrola IT zazwyczaj nie jest wystarczająca, aby odnieść się do ryzyka istotnego zniekształcenia na poziomie stwierdzeń.

A151. Kontrole, których identyfikacja i ocena projektu oraz ustalenie wdrożenia są wymagane od audytora, zgodnie z paragrafem 26, obejmują:

- kontrole, których testy skuteczności działania audytor planuje przeprowadzić podczas określania rodzaju, rozłożenia w czasie i zakresu procedur wiarygodności. Ocena takich kontroli zapewnia podstawę do zaprojektowania przez audytora testów procedur kontroli zgodnie z MSB 330. Te kontrole obejmują również kontrole, które odnoszą się do ryzyk, dla których same procedury wiarygodności nie dostarczają wystarczających odpowiednich dowodów badania,
- kontrole obejmują kontrole, które odnoszą się do znaczących ryzyk oraz kontrole zapisów dziennika. Identyfikacja i ocena takich kontroli przez audytora może również wpłynąć na zrozumienie przez audytora ryzyk istotnego zniekształcenia, w tym na identyfikację dodatkowych ryzyk istotnego zniekształcenia (zobacz paragraf A95). To zrozumienie zapewnia również podstawę do zaprojektowania przez audytora rodzaju, rozłożenia w czasie i zakresu procedur badania wiarygodności, które odpowiadają na związane z nimi oszacowane ryzyka istotnego zniekształcenia,
- inne kontrole, które audytor uzna za odpowiednie, aby umożliwić audytorowi spełnienie celów określonych w paragrafie 13 w odniesieniu do ryzyk na poziomie stwierdzeń, w oparciu o zawodowy osąd audytora.

A152. Wymagane jest zidentyfikowanie kontroli w elemencie czynności kontrolnych, gdy takie kontrole spełniają jedno lub więcej kryteriów zawartych w paragrafie 26(a). Jednakże, gdy spośród wielu kontroli każda osiąga ten sam cel, niepotrzebna jest identyfikacja każdej kontroli związanej z tym celem.

Rodzaje kontroli w elemencie czynności kontrolnych (Zob. par. 26)

A153. Przykłady kontroli w elemencie czynności kontrolnych obejmują autoryzacje i akceptacje, uzgodnienia, weryfikacje (takie, jak edycja i walidacja lub automatyczne obliczenia), podział

obowiązków oraz kontrole fizyczne lub logiczne, w tym te odnoszące się do zabezpieczenia aktywów.

A154. Kontrole w elemencie czynności kontrolnych mogą również obejmować kontrole ustanowione przez kierownictwo, które odnoszą się do ryzyk istotnego zniekształcenia związanych z ujawnieniami, które nie zostały sporządzone zgodnie z mającymi zastosowanie ramowymi założeniami sprawozdawczości finansowej. Takie kontrole mogą dotyczyć informacji zawartych w sprawozdaniu finansowym, uzyskanych spoza ksiąg głównej i pomocniczych.

A155. Niezależnie od tego, czy kontrole znajdują się w środowisku IT, czy w systemach ręcznych, kontrole mogą mieć różne cele i mogą być stosowane na różnych poziomach organizacyjnych i funkcjonalnych.

Skalowalność (Zob. par. 26)

A156. Kontrole w elemencie czynności kontrolnych dla mniej złożonych jednostek będą prawdopodobnie podobne do tych w dużych jednostkach, ale formalizm, z którym działają, może się różnić. Ponadto, w mniej złożonych jednostkach, więcej kontroli może być stosowanych bezpośrednio przez kierownictwo.

Przykład:

Wyłączne uprawnienie kierownictwa do przyznawania kredytów klientom oraz aprobowania znaczących zakupów może zapewniać silną kontrolę ważnych sald kont i transakcji.

A157. Ustalenie podziału obowiązków w mniej złożonych jednostkach, które zatrudniają mniej pracowników, może być mniej praktyczne. Jednakże, w jednostce zarządzanej przez właściciela, zarządzający właściciel może być w stanie sprawować bardziej skuteczny nadzór poprzez swoje bezpośrednie zaangażowanie niż w większej jednostce, co może zrekompensować ogólnie bardziej ograniczone możliwości podziału obowiązków. Chociaż, jak wyjaśniono również w MSB 240, zdominowanie kierownictwa przez jedną osobę może być potencjalną słabością kontroli, ponieważ istnieje możliwość obejścia kontroli przez kierownictwo³⁹.

Kontrole, które odnoszą się do ryzyk istotnego zniekształcenia na poziomie stwierdzeń (Zob. par. 26(a))

Kontrole, które odnoszą się do ryzyk, które są określane jako ryzyka znaczące (Zob. par. 26(a)(i))

A158. Niezależnie od tego, czy audytor planuje testować skuteczność działania kontroli, które odnoszą się do znaczących ryzyk, zrozumienie uzyskane na temat podejścia kierownictwa do reakcji na te ryzyka może zapewnić podstawę do zaprojektowania i wykonania procedur wiarygodności odpowiadających na znaczące ryzyka, zgodnie z wymogami MSB 330⁴⁰. Pomimo tego, że często jest mniej prawdopodobne, aby ryzyka związane ze znaczącymi nietypowymi lub wymagającymi osądu sprawami podlegały rutynowym kontrolom, to kierownictwo może mieć inne odpowiedzi, które w zamierzeniu mają poradzić sobie z takimi ryzykami. Dlatego zrozumienie przez audytora, czy jednostka zaprojektowała i wdrożyła kontrole dla znaczących ryzyk powstających na skutek nietypowych lub wymagających osądu spraw, może obejmować to, czy i w jaki sposób kierownictwo reaguje na te ryzyka. Reakcje takie mogą obejmować:

- kontrole, takie jak przegląd założeń przez kierownictwo wyższego szczebla lub ekspertów,
- udokumentowane procesy dla szacunków księgowych,

³⁹ MSB 240, paragraf A28.

⁴⁰ MSB 330, paragraf 21.

- zatwierdzanie przez osoby sprawujące nadzór.

Przykład:

Gdy występują zdarzenia jednorazowe, takie jak otrzymanie zawiadomienia o znaczącym sporze sądowym, rozważenie reakcji jednostki może obejmować takie zagadnienia, jak to, czy zwrócono się do odpowiednich ekspertów (takich, jak wewnętrzni lub zewnętrzni doradcy prawni), czy dokonano oceny potencjalnych skutków oraz w jaki sposób proponuje się ujawnić okoliczności w sprawozdaniu finansowym.

A159. MSB 240⁴¹ wymaga, aby audytor rozumiał kontrole związane z oszacowanymi ryzykami istotnego zniekształcenia spowodowanego oszustwem (które są traktowane jako ryzyka znaczące), a ponadto wyjaśnia, że ważne jest, aby audytor uzyskał zrozumienie kontroli, które kierownictwo zaprojektowało, wdrożyło i utrzymało w celu zapobiegania i wykrywania oszustwa.

Kontrole dotyczące zapisów dziennika (Zob. par. 26(a)(ii))

A160. Kontrolami, które odnoszą się do ryzyk istotnego zniekształcenia na poziomie stwierdzeń, a których zidentyfikowania oczekuje się dla wszystkich badań, są kontrole dotyczące zapisów dziennika, ponieważ sposób, w jaki jednostka wprowadza informacje pochodzące z przetwarzania transakcji do księgi głównej, zazwyczaj wiąże się z wykorzystaniem zapisów dziennika, zarówno typowych, nietypowych, jak i zautomatyzowanych lub ręcznych. Zakres, w jakim identyfikowane są inne kontrole, może się różnić w zależności od charakteru jednostki i planowanego podejścia audytora do dalszych procedur badania.

Przykład:

Podczas badania mniej złożonej jednostki, system informacyjny jednostki może nie być złożony i audytor może nie planować polegania na skuteczności działania kontroli. Ponadto, audytor mógł nie zidentyfikować żadnych znaczących ryzyk lub żadnych innych ryzyk istotnego zniekształcenia, w odniesieniu do których audytor musi ocenić projekt kontroli i określić, że zostały one wdrożone. Podczas takiego badania audytor może stwierdzić, że poza kontrolą dotyczącą zapisów dziennika w jednostce nie istnieją inne zidentyfikowane kontrole.

Zautomatyzowane narzędzia i techniki

A161. W ręcznych systemach księgi głównej, niestandardowe zapisy dziennika mogą być zidentyfikowane poprzez inspekcję ksiąg, dzienników i dokumentacji stanowiącej podstawę zapisów. Gdy do prowadzenia księgi głównej i sporządzania sprawozdania finansowego wykorzystywane są procedury automatyczne, takie zapisy mogą istnieć tylko w formie elektronicznej i dlatego mogą być łatwiejsze do zidentyfikowania poprzez wykorzystanie technik automatycznych.

Przykład:

Podczas badania mniej złożonej jednostki, audytor może być w stanie przenieść do prostego arkusza kalkulacyjnego łączne zestawienie wszystkich zapisów dziennika. Następnie audytor może mieć możliwość sortowania zapisów dziennika z zastosowaniem różnych filtrów, takich jak kwota w walucie, nazwisko sporządzającego lub weryfikatora, zapisy dziennika, które podnoszą tylko wartości bilansu oraz rachunku zysków i strat, lub zobaczenia zestawienia

⁴¹ MSB 240, paragrafy 28 i A33.

posortowanego według daty, pod jaką zapis dziennika został zaksięgowany w księdze głównej, co pomoże audytorowi w zaprojektowaniu reakcji na zidentyfikowane ryzyka związane z zapisami dziennika.

Kontrole, dla których audytor planuje testować ich skuteczność działania (Zob. par. 26(a)(iii))

A162. Audytor określa, czy występują jakiekolwiek ryzyka istotnego zniekształcenia na poziomie stwierdzeń, dla których nie jest możliwe uzyskanie wystarczających odpowiednich dowodów badania wyłącznie poprzez procedury wiarygodności. Zgodnie z MSB 330⁴², od audytora wymagane jest zaprojektowanie i wykonanie testów kontroli, które odnoszą się do takich ryzyk istotnego zniekształcenia, gdy same procedury wiarygodności nie dostarczają wystarczających odpowiednich dowodów badania na poziomie stwierdzeń. W wyniku tego, gdy istnieją takie kontrole, które odnoszą się do tych ryzyk, wymagane jest ich zidentyfikowanie i ocena.

A163. W innych przypadkach, gdy audytor planuje wziąć pod uwagę skuteczność działania kontroli podczas określania rodzaju, rozłożenia w czasie i zakresu procedur wiarygodności zgodnie z MSB 330, wymagane jest także zidentyfikowanie takich kontroli, ponieważ MSB 330⁴³ wymaga, aby audytor zaprojektował i wykonał testy tych kontroli.

Przykłady:

Audytor może zaplanować przetestowanie skuteczności działania kontroli:

- rutynowych grup transakcji, ponieważ takie testowanie może być bardziej skuteczne lub efektywne dla dużych wolumenów jednorodnych transakcji,
- kompletności i dokładności informacji sporządzanych przez jednostkę (np. kontrole sporządzania sprawozdań generowanych przez system) w celu określenia wiarygodności tych informacji, gdy audytor zamierza wziąć pod uwagę skuteczność działania tych kontroli podczas projektowania i wykonywania dalszych procedur badania,
- odnoszących się do celów działalności i zgodności, gdy odnoszą się one do danych, które audytor ocenia lub wykorzystuje podczas stosowania procedur badania.

A164. Na plany audytora w zakresie testowania skuteczności działania kontroli mogą mieć również wpływ zidentyfikowane ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego. Na przykład, jeżeli zostaną zidentyfikowane słabości związane ze środowiskiem kontroli, może to wpłynąć na ogólne oczekiwania audytora dotyczące skuteczności działania kontroli bezpośrednich.

Inne kontrole, które audytor uznaje za odpowiednie (Zob. par. 26(a)(iv))

A165. Inne kontrole, które audytor może uznać za odpowiednie w celu identyfikacji i oceny projektu oraz ustalenia wdrożenia, mogą obejmować:

- kontrole, które odnoszą się do ryzyk oszacowanych jako wyższe w ramach zakresu ryzyka nieodłącznego, ale nie zostały określone jako będące ryzykami znaczącymi,
- kontrole związane z uzgadnianiem szczegółowych zapisów do księgi głównej lub
- uzupełniające kontrole jednostki korzystającej, jeżeli korzysta z organizacji usługowej⁴⁴.

⁴² MSB 330, paragraf 8(b).

⁴³ MSB 330, paragraf 8(a).

⁴⁴ MSB 402 *Rozważania podczas badania związane z jednostką korzystającą z organizacji usługowej*.

Identyfikowanie aplikacji IT i innych aspektów środowiska IT, ryzyk wynikających z wykorzystania IT oraz ogólnych kontroli IT (Zob. par. 26(b)–(c))

Załącznik 5 zawiera przykładowe cechy aplikacji IT i inne aspekty środowiska IT oraz wytyczne dotyczące tych cech, które mogą być stosowne podczas identyfikowania aplikacji IT i innych aspektów środowiska IT podlegających ryzykom wynikającym z wykorzystania IT.

Identyfikowanie aplikacji IT i innych aspektów środowiska IT (Zob. par. 26(b))

Dlaczego audytor identyfikuje ryzyka powstające na skutek wykorzystania IT i ogólnych kontroli IT związanych ze zidentyfikowanymi aplikacjami IT i innymi aspektami środowiska IT

A166. Zrozumienie ryzyk powstających na skutek wykorzystania IT oraz ogólnych kontroli IT wdrożonych przez jednostkę w celu odniesienia się do tych ryzyk, może wpływać na:

- decyzję audytora dotyczącą tego, czy przetestować skuteczność działania kontroli, aby odnieść się do ryzyk istotnego zniekształcenia na poziomie stwierdzeń,

Przykład:

Gdy ogólne kontrole IT nie są zaprojektowane skutecznie lub odpowiednio wdrożone, aby odnieść się do ryzyk powstających na skutek wykorzystania IT (np. kontrole nie zapobiegają właściwie lub nie wykrywają nieautoryzowanych zmian w programach lub nieautoryzowanego dostępu do aplikacji IT), może to mieć wpływ na decyzję audytora o poleganiu na automatycznych kontrolach wewnątrz odpowiednich aplikacji IT.

- oszacowanie ryzyka kontroli przez audytora na poziomie stwierdzeń,

Przykład:

Bieżąca skuteczność działania kontroli przetwarzania informacji może zależeć od pewnych ogólnych kontroli IT, które zapobiegają lub wykrywają nieautoryzowane zmiany w programach w zakresie kontroli przetwarzania informacji IT (tj. kontroli zmian w programach powiązanej aplikacji IT). W takich okolicznościach oczekiwana skuteczność działania (lub jej brak) ogólnej kontroli IT może mieć wpływ na oszacowanie ryzyka kontroli przez audytora (np. ryzyko kontroli może być wyższe, gdy oczekuje się, że takie ogólne kontrole IT będą nieskuteczne lub jeżeli audytor nie planuje testować ogólnych kontroli IT).

- strategię audytora dotyczącą testowania informacji sporządzanych przez jednostkę, które są generowane przez aplikacje IT jednostki lub obejmują informacje pochodzące z tych aplikacji,

Przykład:

Gdy informacje sporządzane przez jednostkę, które mają być wykorzystane jako dowody badania, są generowane przez aplikacje IT, audytor może zdecydować o przetestowaniu kontroli raportów generowanych przez system, w tym o identyfikacji i przetestowaniu ogólnych kontroli IT, które odnoszą się do ryzyk niewłaściwych lub nieautoryzowanych zmian w programie lub bezpośrednich zmian danych w raportach.

- oszacowanie ryzyka nieodłącznego przez audytora na poziomie stwierdzeń lub

Przykład:

Gdy występują znaczące lub rozległe zmiany oprogramowania w aplikacji IT, aby uwzględnić nowe lub zmienione wymogi sprawozdawcze wynikające z mających zastosowanie ramowych założeń sprawozdawczości finansowej, może to stanowić wskaźnik złożoności nowych wymogów oraz ich wpływu na sprawozdanie finansowe jednostki. Gdy wystąpią takie znaczne zmiany oprogramowania lub danych, aplikacja IT prawdopodobnie również podlega ryzykom powstającym na skutek wykorzystania IT.

- zaprojektowanie dalszych procedur badania.

Przykład:

Jeżeli kontrole przetwarzania informacji zależą od ogólnych kontroli IT, audytor może podjąć decyzję o przetestowaniu skuteczności działania ogólnych kontroli IT, co będzie dalej wymagało zaprojektowania testów kontroli dla takich ogólnych kontroli IT. Jeżeli w takich samych okolicznościach audytor podejmie decyzję, aby nie testować skuteczności działania ogólnych kontroli IT lub oczekuje się, że ogólne kontrole IT będą nieskuteczne, może zaistnieć potrzeba odniesienia się do powiązanych z nimi ryzyk powstających na skutek wykorzystania IT poprzez zaprojektowanie procedur wiarygodności. Jednakże odniesienie się do ryzyk powstających na skutek wykorzystania IT może nie być możliwe, gdy takie ryzyka związane są z ryzykami, dla których same procedury wiarygodności nie dostarczają wystarczających odpowiednich dowodów badania. W takich okolicznościach audytor może być zmuszony rozważyć konsekwencje dla opinii z badania.

Identyfikowanie aplikacji IT, które podlegają ryzykom powstającym na skutek wykorzystania IT

A167. Dla aplikacji IT stosownych dla systemu informacyjnego, zrozumienie charakteru i złożoności poszczególnych procesów IT oraz ogólnych kontroli IT, które jednostka wdrożyła może pomóc audytorowi w ustaleniu, na których aplikacjach IT jednostka polega, aby dokładnie przetwarzać i utrzymywać integralność informacji w systemie informacyjnym jednostki. Takie aplikacje IT mogą podlegać ryzykom powstającym na skutek wykorzystania IT.

A168. Identyfikowanie aplikacji IT, które podlegają ryzykom powstającym na skutek wykorzystania IT, obejmuje wzięcie pod uwagę kontroli zidentyfikowanych przez audytora, ponieważ kontrole takie mogą obejmować wykorzystanie IT lub polegać na IT. Audytor może skupić się na tym, czy dana aplikacja IT zawiera zautomatyzowane kontrole, na których polega kierownictwo i które audytor zidentyfikował, w tym kontrole, które odnoszą się do ryzyk, dla których same procedury wiarygodności nie dostarczają wystarczających odpowiednich dowodów badania. Audytor może również rozważyć, w jaki sposób przechowywane i przetwarzane w systemie informacyjnym są informacje dotyczące znaczących grup transakcji, sald kont i ujawnień oraz czy kierownictwo polega na ogólnych kontrolach IT, aby utrzymać integralność tych informacji.

A169. Kontrole zidentyfikowane przez audytora mogą być uzależnione od raportów generowanych przez system i w takim przypadku aplikacje IT, które generują te raporty, mogą podlegać ryzykom powstającym na skutek wykorzystania IT. W innych przypadkach audytor może nie planować polegania na kontrolach raportów generowanych przez system i zaplanować, aby bezpośrednio przetestować dane wejściowe i wyjściowe takich raportów i w takim przypadku audytor może nie zidentyfikować powiązanych aplikacji IT jako podlegających ryzykom wynikającym z IT.

Skalowalność

A170. Zakres zrozumienia przez audytora procesów IT, w tym zakresu, w jakim jednostka posiada ogólne kontrole IT, będzie się różnić w zależności od charakteru i okoliczności jednostki oraz jej środowiska IT, jak również w zależności od rodzaju i zakresu kontroli zidentyfikowanych przez audytora. Na podstawie tych czynników różni się także liczba aplikacji IT, które podlegają ryzykom powstającym na skutek wykorzystania IT.

Przykłady:

- Jednostka, która korzysta z komercyjnego oprogramowania i nie ma dostępu do kodu źródłowego, aby dokonywać jakichkolwiek zmian w programie, prawdopodobnie nie posiada procesu dokonywania zmian w programie, ale może posiadać proces lub procedury, aby konfigurować oprogramowanie (np. plan kont, parametry sprawozdawczości lub progi). Ponadto, jednostka może posiadać proces lub procedury, aby zarządzać dostępem do aplikacji (np. wyznaczona osoba z administracyjnym dostępem do oprogramowania komercyjnego). W takich okolicznościach jest mało prawdopodobne, aby jednostka posiadała lub potrzebowała sformalizowanych ogólnych kontroli IT.
- W przeciwieństwie do tego, większa jednostka może w dużym stopniu polegać na IT, a środowisko IT może obejmować wiele aplikacji IT i procesy IT, aby zarządzać środowiskiem IT, mogą być złożone (np. istnieje dział IT poświęcony opracowywaniu i wdrażaniu zmian w programach oraz zarządzaniu prawami dostępu), łącznie z tym, że jednostka wdrożyła sformalizowane ogólne kontrole IT swoich procesów IT.
- Gdy kierownictwo nie polega na kontrolach automatycznych lub ogólnych kontrolach IT, aby przetwarzać transakcje lub utrzymywać dane, a audytor nie zidentyfikował żadnych kontroli automatycznych lub innych kontroli przetwarzania informacji (lub jakichkolwiek, które są zależne od ogólnych kontroli IT), audytor może zaplanować, aby bezpośrednio przetestować wszelkie informacje wygenerowane przez jednostkę z wykorzystaniem IT i może nie identyfikować żadnych aplikacji IT, które podlegają ryzykom powstającym na skutek wykorzystania IT.
- Gdy kierownictwo polega na aplikacji IT, aby przetwarzać lub utrzymywać dane, a ilość danych jest znacząca i kierownictwo polega na aplikacji IT, aby wykonać kontrole automatyczne, które audytor również zidentyfikował, prawdopodobnie aplikacja IT będzie podlegała ryzykom powstającym na skutek wykorzystania IT.

A171. Gdy jednostka ma bardziej złożone środowisko IT, identyfikowanie aplikacji IT i innych aspektów środowiska IT, określenie powiązanych ryzyk powstających na skutek wykorzystania IT oraz identyfikowanie ogólnych kontroli IT prawdopodobnie wymagać będzie zaangażowania członków zespołu posiadających specjalistyczne umiejętności w zakresie IT. Zaangażowanie takie będzie prawdopodobnie kwestią zasadniczą i może wymagać rozszerzenia dla złożonych środowisk IT.

Identyfikowanie innych aspektów środowiska IT, które podlegają ryzykom powstającym na skutek wykorzystania IT

A172. Inne aspekty środowiska IT, które mogą podlegać ryzykom powstającym na skutek wykorzystania IT, obejmują sieć, system operacyjny i bazy danych oraz w pewnych okolicznościach, interfejsy pomiędzy aplikacjami IT. Inne aspekty środowiska IT zazwyczaj nie są identyfikowane, gdy audytor nie identyfikuje aplikacji IT, które podlegają ryzykom

powstającym na skutek wykorzystania IT. Gdy audytor zidentyfikował aplikacje IT, które podlegają ryzykom powstającym z powodu IT, inne aspekty środowiska IT (np. baza danych, system operacyjny, sieć) prawdopodobnie zostaną zidentyfikowane, ponieważ takie aspekty wspierają zidentyfikowane aplikacje IT i współdziałają z nimi.

Identyfikowanie ryzyk powstających na skutek wykorzystania IT i ogólnych kontroli IT (Zob. par. 26(c))

Załącznik 6 przedstawia rozważania dotyczące zrozumienia ogólnych kontroli IT.

A173. Identyfikując ryzyka powstające na skutek wykorzystania IT, audytor może rozważyć charakter zidentyfikowanej aplikacji IT lub inny aspekt środowiska IT oraz przyczyny, dla których podlega ona ryzykom powstającym na skutek wykorzystania IT. Dla niektórych zidentyfikowanych aplikacji IT lub innych aspektów środowiska IT, audytor może zidentyfikować mające zastosowanie ryzyka powstające na skutek wykorzystania IT, które są związane przede wszystkim z nieautoryzowanym dostępem lub nieuprawnionymi zmianami w programie, jak również takie, które odnoszą się do ryzyk związanych z niewłaściwymi zmianami danych (np. ryzyko niewłaściwych zmian danych poprzez bezpośredni dostęp do bazy danych lub zdolność do bezpośredniej manipulacji informacjami).

A174. Zakres i charakter mających zastosowanie ryzyk powstających na skutek wykorzystania IT różni się w zależności od rodzaju i cech zidentyfikowanych aplikacji IT oraz innych aspektów środowiska IT. Mające zastosowanie ryzyka IT mogą być skutkiem, gdy jednostka korzysta z usług zewnętrznych lub wewnętrznych dostawców usług dla zidentyfikowanych aspektów swojego środowiska IT (np. outsourcing hostingu swojego środowiska IT od osoby trzeciej lub korzystanie z centrum usług wspólnych w celu centralnego zarządzania procesami IT w grupie). Można również zidentyfikować mające zastosowanie ryzyka powstające na skutek wykorzystania IT związane z bezpieczeństwem cybernetycznym. Bardziej prawdopodobne jest, że będzie więcej ryzyk powstających na skutek wykorzystania IT, gdy wolumen lub złożoność automatycznych kontroli aplikacji będą wyższe, a kierownictwo będzie w większym stopniu polegać na tych kontrolach w celu skutecznego przetwarzania transakcji lub skutecznego utrzymania integralności informacji podstawowych.

Dokonywanie oceny zaprojektowania i ustalenie wdrożenia zidentyfikowanych kontroli w elemencie czynności kontrolnych (Zob. par. 26(d))

A175. Dokonywanie oceny projektu zidentyfikowanej kontroli obejmuje rozważenie przez audytora, czy kontrola, pojedynczo lub w połączeniu z innymi kontrolami, jest w stanie skutecznie zapobiegać istotnym zniekształceniom lub je wykrywać i korygować (tj. cel kontroli).

A176. Audytor ustala wdrożenie zidentyfikowanej kontroli poprzez ustalenie, że kontrola istnieje i że jednostka ją wykorzystuje. Ocenianie przez audytora wdrożenia kontroli, która nie została skutecznie zaprojektowana nie ma większego sensu. Dlatego też audytor najpierw ocenia zaprojektowanie kontroli. Niewłaściwie zaprojektowana kontrola może stanowić słabość kontroli.

A177. Procedury oszacowania ryzyka, aby uzyskać dowody badania dotyczące zaprojektowania i wdrożenia zidentyfikowanych kontroli w elemencie czynności kontrolnych, mogą obejmować:

- zapytania skierowane do personelu jednostki,
- obserwację zastosowania poszczególnych kontroli,
- inspekcję dokumentów i raportów.

Jednakże, samo zapytanie nie jest wystarczające dla takich celów.

- A178. Audytor może oczekiwać, na podstawie doświadczenia z poprzedniego badania lub w oparciu o procedury oszacowania ryzyka w bieżącym okresie, że kierownictwo nie zaprojektowało lub nie wdrożyło skutecznie kontroli, aby odnieść się do znaczącego ryzyka. W takich przypadkach procedury wykonane, aby odnieść się do wymogu określonego w paragrafie 26(d), mogą składać się z ustalenia, że takie kontrole nie zostały skutecznie zaprojektowane lub wdrożone. Jeżeli wyniki procedur wskazują, że kontrole zostały od nowa zaprojektowane lub wdrożone, od audytora wymagane jest wykonanie procedur określonych w paragrafie 26(b)-(d) dotyczących nowo zaprojektowanych lub wdrożonych kontroli.
- A179. Audytor może stwierdzić, że kontrola, która jest skutecznie zaprojektowana i wdrożona, może być odpowiednia do przetestowania w celu uwzględnienia jej skuteczności działania podczas projektowania procedur wiarygodności. Jednakże, gdy kontrola nie jest zaprojektowana lub wdrożona skutecznie, jej testowanie nie przyniesie żadnych korzyści. Gdy audytor planuje przetestować kontrolę, uzyskane informacje na temat zakresu, w jakim kontrola odnosi się do ryzyka(ryzyk) istotnego zniekształcenia, stanowią dane wejściowe do oszacowania przez audytora ryzyka kontroli na poziomie stwierdzeń.
- A180. Dokonywanie oceny zaprojektowania i ustalenie wdrożenia zidentyfikowanych kontroli w elemencie czynności kontrolnych nie jest wystarczające, aby przetestować ich skuteczność działania. Dla kontroli automatycznych audytor może jednak zaplanować, aby przetestować skuteczność działania kontroli automatycznych poprzez identyfikowanie i testowanie ogólnych kontroli IT, które zapewniają spójne działanie kontroli automatycznej, zamiast wykonywania testów skuteczności działania bezpośrednio na kontrolach automatycznych. Uzyskanie dowodów badania dotyczących wdrożenia ręcznej kontroli na określony moment nie dostarcza dowodów badania dotyczących skuteczności działania kontroli w innych momentach w trakcie okresu objętego badaniem. Testy skuteczności działania kontroli, w tym testy kontroli pośrednich, są pełniej opisane w MSB 330⁴⁵.
- A181. Gdy audytor nie planuje testować skuteczności działania zidentyfikowanych kontroli, zrozumienie audytora może nadal pomóc w zaprojektowaniu rodzaju, rozłożenia w czasie i zakresu procedur badania wiarygodności, które są reakcją na powiązane ryzyka istotnego zniekształcenia.

Przykład:

Wyniki tych procedur oszacowania ryzyka mogą zapewnić podstawę do rozważenia przez audytora możliwych odchyłeń w populacji podczas projektowania próbek do badania.

Słabości kontroli w systemie kontroli wewnętrznej jednostki (Zob. par. 27)

- A182. Wykonując oceny każdego z elementów systemu kontroli wewnętrznej w jednostce⁴⁶ audytor może ustalić, że pewne polityki jednostki w danym elemencie nie są odpowiednie do charakteru i okoliczności jednostki. Takie ustalenie może być wskaźnikiem, który pomaga audytorowi w identyfikowaniu słabości kontroli. Jeżeli audytor zidentyfikował jedną lub więcej słabości kontroli, audytor może rozważyć wpływ tych słabości kontroli na zaprojektowanie dalszych procedur badania zgodnie z MSB 330.

⁴⁵ MSB 330, paragrafy 8-11.

⁴⁶ Paragrafy 21(b), 22(b), 24(c), 25(c) i 26(d).

A183. Jeżeli audytor zidentyfikował jedną lub więcej słabości kontroli, MSB 265⁴⁷ wymaga, aby audytor ustalił, czy te słabości, pojedynczo lub łącznie, stanowią znaczącą słabość. Audytor stosuje zawodowy osąd podczas ustalania, czy dana słabość stanowi znaczącą słabość kontroli⁴⁸.

Przykłady:

Okoliczności, które mogą wskazywać, że występuje znacząca słabość kontroli, obejmują takie zagadnienia, jak:

- identyfikacja oszustwa o dowolnej wielkości, które obejmuje kierownictwo wyższego szczebla,
- zidentyfikowane procesy wewnętrzne, które są nieadekwatne w odniesieniu do sprawozdawczości i informowania o słabościach zauważonych przez audyt wewnętrzny,
- wcześniej zakomunikowane słabości, które nie zostały skorygowane przez kierownictwo w odpowiednim czasie,
- brak reakcji kierownictwa na znaczące ryzyka, na przykład, poprzez brak wdrożenia kontroli znaczących ryzyk oraz
- przekształcenie wcześniej wydanego sprawozdania finansowego.

Identyfikacja i oszacowanie ryzyk istotnego zniekształcenia (Zob. par. 28–37)

Dlaczego audytor identyfikuje i szacuje ryzyka istotnego zniekształcenia

A184. Ryzyka istotnego zniekształcenia są identyfikowane i szacowane przez audytora w celu ustalenia rodzaju, rozłożenia w czasie i zakresu dalszych procedur badania niezbędnych, aby uzyskać wystarczające odpowiednie dowody badania. Dowody te umożliwiają audytorowi wyrażenie opinii o sprawozdaniu finansowym przy akceptowalnie niskim poziomie ryzyka badania.

A185. Informacje zgromadzone poprzez wykonanie procedur oszacowania ryzyka są wykorzystywane jako dowody badania, aby zapewnić podstawę do identyfikacji i oszacowania ryzyk istotnego zniekształcenia. Na przykład, dowody badania uzyskane podczas dokonywania oceny projektu zidentyfikowanych kontroli i ustalania czy kontrole te zostały wdrożone w elemencie czynności kontrolnych, są wykorzystywane jako dowody badania na poparcie oszacowania ryzyka. Dowody takie zapewniają również podstawę do zaprojektowania przez audytora ogólnych reakcji, aby odnieść się do oszacowanych ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego, jak również do zaprojektowania i wykonania dalszych procedur badania, których rodzaj, rozłożenie w czasie i zakres są reakcją na oszacowane ryzyka istotnego zniekształcenia na poziomie stwierdzeń, zgodnie z MSB 330.

Identyfikowanie ryzyk istotnego zniekształcenia (Zob. par. 28)

A186. Identyfikacja ryzyk istotnego zniekształcenia wykonywana jest przed rozważeniem wszelkich powiązanych kontroli (tj. ryzyka nieodłącznego) i oparta jest na wstępnym rozważeniu przez audytora zniekształceń, które mają uzasadnioną możliwość zarówno wystąpienia, jak i bycia istotnymi, gdyby miały one wystąpić⁴⁹.

⁴⁷ MSB 265 *Informowanie o słabościach kontroli wewnętrznej osób sprawujących nadzór i kierownictwa*, paragraf 8.

⁴⁸ MSB 265, paragrafy A6–A7 określają wskaźniki znaczących słabości oraz zagadnienia, które należy rozważyć podczas ustalania czy słabość lub połączenie słabości w kontroli wewnętrznej stanowi znaczącą słabość.

⁴⁹ MSB (PL) 200, paragraf A16.

A187. Identyfikowanie ryzyk istotnego zniekształcenia zapewnia również podstawę do ustalenia przez audytora stosownych stwierdzeń, co pomaga audytorowi w ustaleniu znaczących grup transakcji, sald kont i ujawnień.

Stwierdzenia

Dlaczego audytor korzysta ze stwierdzeń

A188. Podczas identyfikowania i dokonywania oszacowania ryzyk istotnego zniekształcenia, audytor korzysta ze stwierdzeń, aby rozważyć różne rodzaje potencjalnych zniekształceń, które mogą wystąpić. Stwierdzenia, dla których audytor zidentyfikował powiązane ryzyka istotnego zniekształcenia, stanowią stosowne stwierdzenia.

Wykorzystanie stwierdzeń

A189. Podczas identyfikowania i oszacowania ryzyk istotnego zniekształcenia audytor może korzystać z kategorii stwierdzeń opisanych w paragrafie A190(a)-(b) poniżej lub może wyrazić je w inny sposób, pod warunkiem, że wszystkie aspekty opisane poniżej zostały uwzględnione. Audytor może wybrać połączenie stwierdzeń dotyczących grup transakcji i zdarzeń oraz powiązanych z nimi ujawnień ze stwierdzeniami dotyczącymi sald kont oraz związanych z nimi ujawnień.

A190. Stwierdzenia wykorzystywane przez audytora podczas rozważania różnych rodzajów potencjalnych zniekształceń, które mogą wystąpić, mogą należeć do następujących kategorii:

- (a) stwierdzenia dotyczące grup transakcji i zdarzeń oraz związanych z nimi ujawnień za okres objęty badaniem:
 - (i) występowanie – transakcje i zdarzenia, które zostały zarejestrowane lub ujawnione, wystąpiły i takie transakcje i zdarzenia dotyczą jednostki,
 - (ii) kompletność – wszystkie transakcje i zdarzenia, które powinny być zarejestrowane, zostały zarejestrowane, a wszystkie związane z nimi ujawnienia, które powinny zostać zawarte w sprawozdaniu finansowym, zostały zawarte,
 - (iii) dokładność – kwoty i inne dane dotyczące zarejestrowanych transakcji i zdarzeń zostały odpowiednio zarejestrowane, a związane z nimi ujawnienia zostały odpowiednio wycenione i opisane,
 - (iv) rozgraniczenie między okresami – transakcje i zdarzenia zostały zarejestrowane we właściwym okresie księgowym,
 - (v) klasyfikacja – transakcje i zdarzenia zostały zarejestrowane na właściwych kontach,
 - (vi) prezentacja – transakcje i zdarzenia są odpowiednio zagregowane lub zdezagregowane i jasno opisane, a związane z nimi ujawnienia są stosowne i zrozumiałe w kontekście wymogów mających zastosowanie ramowych założeń sprawozdawczości finansowej,
- (b) stwierdzenia dotyczące sald kont i związanych z nimi ujawnień na koniec okresu:
 - (i) istnienie – aktywa, zobowiązania i kapitał własny istnieją,
 - (ii) prawa i obowiązki – jednostka posiada lub kontroluje prawa do aktywów, a zobowiązania są obowiązkami jednostki,
 - (iii) kompletność – wszystkie aktywa, zobowiązania i kapitał własny, które powinny być zarejestrowane, zostały zarejestrowane, a wszystkie związane z nimi ujawnienia, które powinny zostać zawarte w sprawozdaniu finansowym, zostały zawarte,

- (iv) dokładność, wycena i przyporządkowanie – aktywa, zobowiązania i kapitał własny zostały wykazane w sprawozdaniu finansowym we właściwych kwotach, a wszelkie wyniki korekty wyceny lub przyporządkowania zostały odpowiednio zarejestrowane oraz związane z nimi ujawnienia zostały odpowiednio wycenione i opisane,
- (v) klasyfikacja – aktywa, zobowiązania i kapitał własny zostały zarejestrowane na właściwych kontach,
- (vi) prezentacja – aktywa, zobowiązania i kapitał własny są odpowiednio zagregowane lub zdezagregowane i jasno opisane, a związane z nimi ujawnienia są stosowne i zrozumiałe w kontekście wymogów mających zastosowanie ramowych założeń sprawozdawczości finansowej.

A191. Stwierdzenia opisane powyżej w paragrafie A190(a)-(b), odpowiednio dostosowane, mogą być także wykorzystane przez audytora podczas rozważania różnych rodzajów zniekształceń, które mogą wystąpić w ujawnieniach nie związanych bezpośrednio z zarejestrowanymi grupami transakcji, zdarzeniami lub saldami kont.

Przykład:

Przykład takiego ujawnienia obejmuje sytuację, gdy mające zastosowanie ramowe założenia sprawozdawczości finansowej mogą wymagać od jednostki, aby opisała swoje narażenie na ryzyka powstające z instrumentów finansowych, w tym jak ryzyka powstają, cele, polityki i procesy zarządzania ryzykami, oraz metody wykorzystywane do pomiaru ryzyk.

Szczególne rozważania dla jednostek sektora publicznego

A192. Formułując stwierdzenia dotyczące sprawozdania finansowego jednostek sektora publicznego, oprócz tych stwierdzeń, określonych w paragrafie A190(a)-(b), kierownictwo może często stwierdzać, że transakcje i zdarzenia nastąpiły zgodnie z przepisami prawa, regulacją lub innymi nadanymi uprawnieniami. Takie stwierdzenia mogą wchodzić w zakres badania sprawozdania finansowego.

Ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego (Zob. par. 28(a) i 30)

Dlatego audytor identyfikuje i szacuje ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego

A193. Audytor identyfikuje ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego, aby ustalić, czy ryzyka mają rozległy wpływ na sprawozdanie finansowe, a zatem wymagałyby ogólnej reakcji zgodnie z MSB 330.⁵⁰

A194. Ponadto ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego mogą również wpływać na poszczególne stwierdzenia, a identyfikowanie tych ryzyk może pomóc audytorowi w oszacowaniu ryzyk istotnego zniekształcenia na poziomie stwierdzeń oraz w zaprojektowaniu dalszych procedur badania, aby odnieść się do zidentyfikowanych ryzyk.

⁵⁰ MSB 330, paragraf 5.

Identyfikowanie i oszacowanie ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego

A195. Ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego odnoszą się do ryzyk, które w sposób rozległy wiążą się ze sprawozdaniem finansowym jako całością i potencjalnie wpływają na wiele stwierdzeń. Ryzyka tego rodzaju niekoniecznie są ryzykami identyfikowalnymi z poszczególnymi stwierdzeniami na poziomie grupy transakcji, salda konta lub ujawnienia (np. ryzyko obejścia kontroli przez kierownictwo). Raczej przedstawiają one okoliczności, które mogą w sposób rozległy zwiększyć ryzyka istotnego zniekształcenia na poziomie stwierdzeń. Ocena przez audytora, czy zidentyfikowane ryzyka wiążą się w rozległe ze sprawozdaniem finansowym, wspiera oszacowanie przez audytora ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego. W innych przypadkach można również zidentyfikować szereg stwierdzeń jako podatnych na ryzyko, a zatem może mieć wpływ na identyfikację ryzyka przez audytora i oszacowanie ryzyk istotnego zniekształcenia na poziomie stwierdzeń.

Przykład:

Jednostka jest narażona na straty operacyjne i problemy z płynnością i jest uzależniona od finansowania, które nie zostało jeszcze zabezpieczone. W takich okolicznościach audytor może ustalić, że założenie kontynuacji działalności powoduje powstanie ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego. W tej sytuacji konieczne może być zastosowanie ramowych założeń rachunkowości wykorzystujących zasady likwidacyjne, co prawdopodobnie wpłynęłoby rozległe na wszystkie stwierdzenia.

A196. Na identyfikację i oszacowanie ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego przez audytora wpływa zrozumienie systemu kontroli wewnętrznej jednostki, w szczególności zrozumienie przez audytora środowiska kontroli, procesu oszacowania ryzyka przez jednostkę i procesu monitorowania systemu kontroli wewnętrznej przez jednostkę oraz:

- wyniki powiązanych ocen wymaganych przez paragrafy 21(b), 22(b), 24(c) i 25(c) oraz
- wszelkie słabości kontroli zidentyfikowane zgodnie z paragrafem 27.

W szczególności, ryzyka na poziomie sprawozdania finansowego mogą powstawać na skutek słabości środowiska kontroli lub z zewnętrznych zdarzeń lub warunków, takich jak pogarszające się warunki gospodarcze.

A197. Ryzyka istotnego zniekształcenia spowodowane oszustwem mogą być szczególnie stosowne dla rozważań audytora w zakresie ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego.

Przykład:

Na podstawie zapytań kierowanych do kierownictwa audytor rozumie, że sprawozdanie finansowe jednostki ma być wykorzystywane podczas rozmów z kredytodawcami w celu zapewnienia dalszego finansowania dla utrzymania kapitału obrotowego. Audytor może zatem ustalić, że występuje większa podatność na zniekształcenie wynikające z czynników ryzyka oszustwa, które wpływa na ryzyko nieodłączne (tj. podatność sprawozdania finansowego na istotne zniekształcenie ze względu na ryzyko oszukańczej sprawozdawczości finansowej, takie jak zawyżanie aktywów i przychodów oraz zaniżanie zobowiązań i kosztów, aby zapewnić, że finansowanie zostanie uzyskane).

A198. Zrozumienie środowiska kontroli i innych elementów systemu kontroli wewnętrznej przez audytora, w tym związane z tym oceny, może budzić wątpliwości co do zdolności audytora do uzyskania dowodów badania, na których można oprzeć opinię z badania, lub które mogą być przyczyną wycofania się ze zlecenia, gdy wycofanie się jest możliwe zgodnie z mającymi zastosowanie przepisami prawa lub regulacją.

Przykłady:

- W wyniku dokonania oceny środowiska kontroli jednostki, audytor ma wątpliwości dotyczące uczciwości kierownictwa jednostki, które mogą być na tyle poważne, że skłonią audytora do stwierdzenia, iż ryzyko celowego wprowadzenia w błąd przez kierownictwo w sprawozdaniu finansowym jest takie, że badanie nie może zostać przeprowadzone.
- W wyniku dokonania oceny systemu informacyjnego i komunikacji w jednostce, audytor stwierdza, że znaczące zmiany w środowisku IT były słabo zarządzane, przy niewielkim nadzorze ze strony kierownictwa i osób sprawujących nadzór. Audytor stwierdza, że istnieją znaczące wątpliwości dotyczące stanu i wiarygodności dokumentacji księgowej jednostki. W takich okolicznościach audytor może stwierdzić, że jest mało prawdopodobne, aby dostępne były wystarczające odpowiednie dowody badania, aby wesprzeć niezmodyfikowaną opinię o sprawozdaniu finansowym.

A199.MSB 705 (zmieniony)⁵¹ ustanawia wymogi i dostarcza wytycznych dotyczących ustalenia, czy występuje potrzeba wyrażenia przez audytora opinii z zastrzeżeniem lub odmowy wyrażenia opinii lub, co może być wymagane w niektórych przypadkach, wycofania się ze zlecenia, gdy wycofanie się jest możliwe zgodnie z mającymi zastosowanie przepisami prawa lub regulacją.

Szczególne rozważania dla jednostek sektora publicznego

A200. Dla jednostek sektora publicznego identyfikacja ryzyk na poziomie sprawozdania finansowego może obejmować rozważenie zagadnień związanych z klimatem politycznym, interesem publicznym i wrażliwością programu.

Ryzyka istotnego zniekształcenia na poziomie stwierdzeń (Zob. par. 28(b))

Załącznik 2 zawiera przykłady zdarzeń lub warunków, które mogą wskazywać na podatność na zniekształcenie, które może być istotne, w kontekście czynników ryzyka nieodłącznego.

A201. Ryzyka istotnego zniekształcenia, które nie odnoszą się w sposób rozległy do sprawozdania finansowego, są ryzykami istotnego zniekształcenia na poziomie stwierdzeń.

Stosowne stwierdzenia i znaczące grupy transakcji, salda kont i ujawnienia (Zob. par. 29)

Dlatego ustala się stosowne stwierdzenia i znaczące grupy transakcji, salda kont i ujawnienia

A202. Ustalenie stosownych stwierdzeń oraz znaczących grup transakcji, sald kont i ujawnień zapewnia podstawę zakresu zrozumienia przez audytora systemu informacyjnego jednostki, którego

⁵¹ MSB 705 (zmieniony) *Modyfikacje opinii w sprawozdaniu niezależnego audytora.*

uzyskanie jest wymagane zgodnie z paragrafem 25(a). Zrozumienie to może dalej pomóc audytorowi w identyfikowaniu i oszacowaniu ryzyk istotnego zniekształcenia (zobacz A86).

Zautomatyzowane narzędzia i techniki

A203. Audytor może korzystać z technik zautomatyzowanych, aby pomóc sobie w identyfikacji znaczących grup transakcji, sald kont i ujawnień.

Przykłady:

- Cała populacja transakcji może być przeanalizowana przy użyciu zautomatyzowanych narzędzi i technik, aby zrozumieć ich charakter, źródło, wielkość i wolumen. Poprzez zastosowanie zautomatyzowanych technik, audytor może, na przykład, zidentyfikować, że konto o zerowym saldzie na koniec okresu obejmowało liczne transakcje kompensujące się wzajemnie i zapisy w dzienniku występujące w trakcie okresu, wskazujące, że saldo konta lub grupa transakcji mogą być znaczące (np. konto rozliczeniowe płac). To samo konto rozliczeniowe płac może również identyfikować zwroty kosztów dla kierownictwa (i innych pracowników), które mogą stanowić znaczące ujawnienie ze względu na fakt, że płatności te są dokonywane na rzecz podmiotów powiązanych.
- Analizując przepływy w całej populacji transakcji przychodowych, audytor może łatwiej zidentyfikować znaczącą grupę transakcji, która nie została wcześniej zidentyfikowana.

Ujawnienia, które mogą być znaczące

A204. Znaczące ujawnienia obejmują zarówno ujawnienia ilościowe, jak i jakościowe, w odniesieniu do których występuje jedno lub więcej stosownych stwierdzeń. Przykłady ujawnień, które mają aspekty jakościowe i które mogą odnosić się do stosownych stwierdzeń i w związku z tym mogą być uznane za znaczące przez audytora, obejmują ujawnienia dotyczące:

- płynności i kowenantów kredytowych jednostki znajdującej się w trudnej sytuacji finansowej,
- zdarzeń lub okoliczności, które doprowadziły do ujęcia odpisu aktualizującego z tytułu utraty wartości,
- kluczowych źródeł niepewności szacunków, w tym założeń dotyczących przyszłości,
- charakteru zmian zasad (polityki) rachunkowości oraz innych stosownych ujawnień wymaganych przez mające zastosowanie ramowe założenia sprawozdawczości finansowej, gdy na przykład, oczekuje się, że nowe wymogi sprawozdawczości finansowej będą miały znaczący wpływ na sytuację finansową i wyniki finansowe jednostki,
- umów dotyczących płatności w formie akcji, w tym informacji na temat sposobu ustalenia wszelkich ujętych kwot oraz innych stosownych ujawnień,
- stron powiązanych i transakcji ze stronami powiązanymi,
- analizy wrażliwości, w tym wpływu zmian w założeniach wykorzystywanych w technikach wyceny stosowanych przez jednostkę, mających na celu umożliwienie użytkownikom zrozumienie podstawy niepewności związanej z wyceną zaksięgowanej lub ujawnionej kwoty.

Oszacowanie ryzyk istotnego zniekształcenia na poziomie stwierdzeń

Oszacowanie ryzyka nieodłącznego (Zob. par. 31–33)

Oszacowanie prawdopodobieństwa i wielkości zniekształcenia (Zob. par. 31)

Dlaczego audytor szacuje prawdopodobieństwo oraz wielkość zniekształcenia

A205. Audytor szacuje prawdopodobieństwo oraz wielkość zniekształcenia dla zidentyfikowanych ryzyk istotnego zniekształcenia, ponieważ znaczenie połączenia prawdopodobieństwa wystąpienia zniekształcenia i wielkości potencjalnego zniekształcenia w przypadku wystąpienia takiego zniekształcenia decyduje o tym, gdzie na skali ryzyka nieodłącznego oszacowane jest zidentyfikowane ryzyko, co wpływa na zaprojektowanie przez audytora dalszych procedur badania, aby odnieść się do tego ryzyka.

A206. Oszacowanie ryzyka nieodłącznego zidentyfikowanych ryzyk istotnego zniekształcenia pomaga również audytorowi w ustaleniu znaczących ryzyk. Audytor ustala znaczące ryzyka, ponieważ zgodnie z MSB 330 i innymi MSB wymagane są konkretne reakcje na znaczące ryzyka.

A207. Czynniki ryzyka nieodłącznego wpływają na oszacowanie przez audytora prawdopodobieństwa i wielkości zniekształcenia dla zidentyfikowanych ryzyk istotnego zniekształcenia na poziomie stwierdzeń. Im większy jest stopień podatności grupy transakcji, salda konta lub ujawnienia na istotne zniekształcenie, tym wyższe prawdopodobieństwo będzie oszacowanie ryzyka nieodłącznego. Rozważenie stopnia, w jakim czynniki ryzyka nieodłącznego wpływają na podatność stwierdzenia na zniekształcenie pomaga audytorowi we właściwym oszacowaniu ryzyka nieodłącznego dla ryzyk istotnego zniekształcenia na poziomie stwierdzeń oraz w zaprojektowaniu bardziej precyzyjnej reakcji na takie ryzyko.

Skala ryzyka nieodłącznego

A208. Szacując ryzyko nieodłączne, audytor stosuje zawodowy osąd podczas ustalania znaczenia połączenia prawdopodobieństwa i wielkości zniekształcenia.

A209. Oszacowane ryzyko nieodłączne związane z konkretnym ryzykiem istotnego zniekształcenia na poziomie stwierdzeń stanowi osąd w ramach skali ryzyka nieodłącznego, od niższego do wyższego. Osąd co do tego, gdzie w ramach skali zostało oszacowane ryzyko nieodłączne, może różnić się w zależności od charakteru, wielkości i złożoności jednostki, a także uwzględnia oszacowane prawdopodobieństwo i wielkość zniekształcenia oraz czynniki ryzyka nieodłącznego.

A210. Rozważając prawdopodobieństwo zniekształcenia, audytor rozważa możliwość, że zniekształcenie może wystąpić na podstawie rozważenia czynników ryzyka nieodłącznego.

A211. Rozważając wielkość zniekształcenia, audytor rozważa jakościowe i ilościowe aspekty możliwego zniekształcenia (tj. zniekształcenia w stwierdzeniach dotyczących grup transakcji, sald kont lub ujawnień mogą zostać uznane za istotne ze względu na wielkość, charakter lub okoliczności).

A212. Audytor wykorzystuje znaczenie połączenia prawdopodobieństwa i wielkości możliwego zniekształcenia podczas ustalania, gdzie na skali ryzyka nieodłącznego (tj. w zakresie) oszacowane zostało ryzyko nieodłączne. Im wyższe połączenie prawdopodobieństwa i wielkości, tym wyższe oszacowanie ryzyka nieodłącznego; im niższe połączenie prawdopodobieństwa i wielkości, tym niższe oszacowanie ryzyka nieodłącznego.

A213. Oszacowanie ryzyka jako wyższe na skali ryzyka nieodłącznego nie oznacza, że zarówno jego wielkość, jak i prawdopodobieństwo muszą być oszacowane jako wysokie. O tym, czy oszacowane ryzyko nieodłączne jest wyższe, czy niższe na skali ryzyka nieodłącznego,

zadecyduje raczej punkt przecięcia wielkości i prawdopodobieństwa istotnego zniekształcenia na skali ryzyka nieodłącznego. Wyższe oszacowanie ryzyka nieodłącznego może również wynikać z różnych połączeń prawdopodobieństwa i wielkości, na przykład wyższe oszacowanie ryzyka nieodłącznego mogłoby wynikać z niższego prawdopodobieństwa, ale z bardzo wysokiej wielkości.

A214. W celu opracowania odpowiednich strategii reagowania na ryzyka istotnego zniekształcenia, audytor może wyznaczyć ryzyka istotnego zniekształcenia w ramach kategorii ze skali ryzyka nieodłącznego, w oparciu o oszacowania ich ryzyka nieodłącznego. Kategorie te mogą być opisane na różne sposoby. Niezależnie od zastosowanej metody kategoryzacji, oszacowanie przez audytora ryzyka nieodłącznego jest odpowiednie, gdy zaprojektowanie i wdrożenie dalszych procedur badania, aby odnieść się do zidentyfikowanych ryzyk istotnego zniekształcenia na poziomie stwierdzeń jest odpowiednio dostosowane do oszacowania ryzyka nieodłącznego i przyczyn tego oszacowania.

Rozległe ryzyka istotnego zniekształcenia na poziomie stwierdzeń (Zob. par. 31(b))

A215. Szacując zidentyfikowane ryzyka istotnego zniekształcenia na poziomie stwierdzeń, audytor może uznać, że niektóre ryzyka istotnego zniekształcenia odnoszą się w sposób bardziej rozległy do sprawozdania finansowego jako całości i potencjalnie wpływają na wiele stwierdzeń, i w takim przypadku audytor może zaktualizować identyfikację ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego.

A216. W okolicznościach, w których ryzyka istotnego zniekształcenia zostały zidentyfikowane jako ryzyka na poziomie sprawozdania finansowego ze względu na ich rozległy wpływ na szereg stwierdzeń i są identyfikowalne z określonymi stwierdzeniami, od audytora wymagane jest uwzględnienie tych ryzyk podczas oszacowania ryzyka nieodłącznego dla ryzyk istotnego zniekształcenia na poziomie stwierdzeń.

Szczególne rozważania dla jednostek sektora publicznego

A217. Dokonując zawodowego osądu co do oszacowania ryzyka istotnego zniekształcenia, audytorzy jednostek sektora publicznego mogą rozważyć złożoność regulacji i dyrektyw oraz ryzyk niezgodności z innymi nadanymi uprawnieniami.

Znaczące ryzyka (Zob. par. 32)

Dlaczego ustalane są znaczące ryzyka oraz konsekwencje dla badania

A218. Ustalenie znaczących ryzyk umożliwia audytorowi skoncentrowanie większej uwagi na tych ryzykach, które znajdują się w górnej granicy skali ryzyka nieodłącznego, poprzez wykonanie pewnych wymaganych reakcji, w tym:

- wymaga się, aby kontrole, które odnoszą się do znaczących ryzyk, zostały zidentyfikowane zgodnie z paragrafem 26(a)(i), wraz z wymogiem oceny czy kontrola została zaprojektowana skutecznie i wdrożona zgodnie z paragrafem 26(d),
- MSB 330 wymaga, aby kontrole odnoszące się do znaczących ryzyk zostały przetestowane w bieżącym okresie (gdy audytor zamierza polegać na skuteczności działania takich kontroli) oraz aby zaplanowano i wykonano procedury wiarygodności, które specyficznie odpowiadają na zidentyfikowane znaczące ryzyko⁵²,

⁵² MSB 330, paragrafy 15 i 21.

- MSB 330 wymaga, aby audytor uzyskał tym bardziej przekonujące dowody badania, im wyższe jest oszacowanie ryzyka przez audytora⁵³,
- MSB 260 (zmieniony) wymaga komunikowania się z osobami sprawującymi nadzór w sprawie znaczących ryzyk zidentyfikowanych przez audytora⁵⁴,
- MSB 701 wymaga, aby audytor wziął pod uwagę znaczące ryzyka podczas ustalania tych zagadnień, które wymagały znaczącej uwagi audytora, a które mogą być kluczowymi sprawami badania⁵⁵,
- terminowy przegląd dokumentacji badania przez partnera odpowiedzialnego za zlecenie na odpowiednich etapach podczas badania pozwala na terminowe rozwiązanie znaczących spraw, w tym znaczących ryzyk, w sposób zadowalający dla partnera odpowiedzialnego za zlecenie w dniu sporządzenia sprawozdania z badania lub przed tym dniem⁵⁶,
- MSB 600 (zmieniony) wymaga, aby audytor grupy ocenił odpowiedniość projektu i wykonania dalszych procedur badania dla obszarów wyższych oszacowanych ryzyk istotnego zniekształcenia sprawozdania finansowego grupy lub znaczących ryzyk, dla których audytor części składowej grupy ustala dalsze procedury badania do wykonania.⁵⁷

Ustalanie znaczących ryzyk

A219. Ustalając znaczące ryzyka, audytor może najpierw zidentyfikować te oszacowane ryzyka istotnego zniekształcenia, które zostały oszacowane jako wyższe na skali ryzyka nieodłącznego, aby stworzyć podstawę do rozważenia, które ryzyka mogą być bliskie górnej granicy zakresu. Bliskość w stosunku do górnej granicy zakresu ryzyka nieodłącznego będzie się różnić pomiędzy jednostkami i niekoniecznie będzie taka sama dla jednostki z okresu na okres. Może to zależeć od charakteru i okoliczności jednostki, dla której dokonywane jest oszacowanie ryzyka.

A220. Ustalenie, które z oszacowanych ryzyk istotnego zniekształcenia są bliskie górnej granicy skali ryzyka nieodłącznego, a tym samym stanowią znaczące ryzyka, jest sprawą zawodowego osądu, chyba że jest to ryzyko szczególnego rodzaju, które należy traktować jako znaczące ryzyko zgodnie z wymogami innego MSB. MSB 240 zawiera dalsze wymogi i wytyczne w odniesieniu do identyfikacji i oszacowania ryzyk istotnego zniekształcenia spowodowanego oszustwem⁵⁸.

⁵³ MSB 330, paragraf 7(b).

⁵⁴ MSB 260 (zmieniony), paragraf 15.

⁵⁵ MSB 701 *Komunikowanie kluczowych spraw badania w sprawozdaniu niezależnego audytora*, paragraf 9.

⁵⁶ MSB 220 (zmieniony), paragrafy 32 i A87-A89.

⁵⁷ MSB 600 (zmieniony), paragraf 42.

⁵⁸ MSB 240, paragrafy 26-28.

Przykład:

- Gotówka w sieci sprzedaży detalicznej zwykle zostałaby określona jako mająca wysokie prawdopodobieństwo możliwego zniekształcenia (ze względu na ryzyko przywłaszczenia środków pieniężnych), jednak wielkość byłaby zazwyczaj bardzo niska (ze względu na niski poziom fizycznej gotówki utrzymywanej w sklepach). Jest mało prawdopodobne, aby połączenie tych dwóch czynników na skali ryzyka nieodłącznego spowodowało, że istnienie gotówki zostałoby uznane za znaczące ryzyko.
- Jednostka prowadzi negocjacje, aby sprzedać segment działalności. Audytor rozważa wpływ na utratę wartości firmy i może ustalić, że istnieje wyższe prawdopodobieństwo możliwego zniekształcenia oraz jego wyższa wielkość ze względu na wpływ czynników ryzyka nieodłącznego związanych z subiektywizmem, niepewnością i podatnością na stronniczość kierownictwa lub inne czynniki ryzyka oszustwa. Może to spowodować, że utrata wartości firmy zostanie uznana za znaczące ryzyko.

A221. Podczas szacowania ryzyka nieodłącznego audytor bierze również pod uwagę względne skutki czynników ryzyka nieodłącznego. Im niższy jest wpływ czynników ryzyka nieodłącznego, tym niższe prawdopodobieństwo będzie oszacowane ryzyko. Ryzyka istotnego zniekształcenia, które mogą zostać oszacowane jako charakteryzujące się wyższym ryzykiem nieodłącznym i przez to mogą zostać uznane za znaczące ryzyko, mogą powstawać na skutek spraw takich jak następujące:

- transakcji, dla których istnieje wiele akceptowalnych sposobów księgowania, takich jak związane z subiektywizmem,
- szacunków księgowych, które mają wysoką niepewność oszacowań lub złożone modele,
- złożoność gromadzenia i przetwarzania danych, aby wspierać salda kont,
- sald kont lub ujawnień ilościowych, które obejmują skomplikowane obliczenia,
- zasad rachunkowości, które mogą podlegać różniącym się interpretacjom,
- zmian w działalności jednostki, które obejmują zmiany w rachunkowości, na przykład fuzje i przejęcia.

Ryzyka, dla których same procedury wiarygodności nie dostarczają wystarczających odpowiednich dowodów badania (Zob. par. 33)

Dlatego wymagane jest zidentyfikowanie ryzyk, dla których same procedury wiarygodności nie dostarczają wystarczających odpowiednich dowodów badania

A222. Ze względu na charakter ryzyka istotnego zniekształcenia oraz czynności kontrolnych, które odnoszą się do tego ryzyka, w niektórych okolicznościach jedynym sposobem uzyskania wystarczających odpowiednich dowodów badania jest przetestowanie skuteczności działania kontroli. W związku z tym istnieje wymóg, aby audytor zidentyfikował wszelkie takie ryzyka ze względu na konsekwencje dla zaprojektowania i wykonania dalszych procedur badania zgodnie z MSB 330, aby odnieść się do ryzyk istotnego zniekształcenia na poziomie stwierdzeń.

A223. Paragraf 26(a)(iii) wymaga również identyfikacji kontroli, które odnoszą się do ryzyk, dla których same procedury wiarygodności nie mogą dostarczyć wystarczających odpowiednich dowodów badania, ponieważ zgodnie z MSB 330⁵⁹, od audytora wymagane jest zaprojektowanie i wykonanie testów takich kontroli.

⁵⁹ MSB 330, paragraf 8.

Ustalenie ryzyk, dla których same procedury wiarygodności nie dostarczają wystarczających odpowiednich dowodów badania

A224. Gdy rutynowe transakcje gospodarcze podlegają wysoce zautomatyzowanemu przetwarzaniu, w którym nie następuje lub następuje tylko niewielka ingerencja ręczna, wykonanie tylko procedur wiarygodności w związku z tym ryzykiem może nie być możliwe. Może tak być w przypadku okolicznościach, gdzie znacząca ilość informacji jednostki jest inicjowana, rejestrowana, przetwarzana lub raportowana tylko w formie elektronicznej, takiej jak w systemie informacyjnym, który charakteryzuje się wysokim stopniem integracji pomiędzy jego aplikacjami IT. W takich przypadkach:

- dowody badania mogą być dostępne tylko w formie elektronicznej, a ich wystarczalność i odpowiedniość zależy zazwyczaj od skuteczności kontroli ich dokładności i kompletności,
- potencjał dla wystąpienia niewłaściwego zainicjowania lub modyfikacji informacji i niewykrycia tego może być większy, jeżeli odpowiednie kontrole nie działają skutecznie.

Przykład:

Zazwyczaj nie jest możliwe, aby uzyskać wystarczające odpowiednie dowody badania dotyczące przychodów jednostki telekomunikacyjnej wyłącznie w oparciu o procedury wiarygodności. Dzieje się tak, ponieważ dowody działań w zakresie połączeń lub danych nie istnieją w formie, którą można zaobserwować. Zamiast tego wykonuje się zazwyczaj znaczące testy kontroli, aby ustalić, że inicjowanie i zakończenie działań w zakresie połączeń i danych są prawidłowo ujęte (np. minuty połączenia lub wielkość pobranych danych) i prawidłowo zarejestrowane w systemie rozliczeniowym jednostki.

A225. MSB 540 (zmieniony) zapewnia dalsze wytyczne związane z szacunkami księgowymi dotyczącymi ryzyk, w odniesieniu do których same procedury wiarygodności nie dostarczają wystarczających odpowiednich dowodów badania⁶⁰. W odniesieniu do szacunków księgowych może nie być to ograniczone do automatycznego przetwarzania, ale może mieć również zastosowanie do złożonych modeli.

Oszacowanie ryzyka kontroli (Zob. par. 34)

A226. Plany audytora, aby przetestować skuteczność działania kontroli są oparte na oczekiwaniu, że kontrole działają skutecznie, co będzie stanowić podstawę oszacowania ryzyka kontroli przez audytora. Wstępne oczekiwanie skuteczności działania kontroli jest oparte na ocenie zaprojektowania oraz ustaleniu wdrożenia zidentyfikowanych kontroli w elemencie czynności kontrolnych przez audytora. Po przetestowaniu przez audytora skuteczności działania kontroli zgodnie z MSB 330, audytor będzie w stanie potwierdzić początkowe oczekiwanie co do skuteczności działania kontroli. Jeżeli kontrole nie działają tak skutecznie jak oczekiwano, wówczas audytor będzie musiał zweryfikować oszacowanie ryzyka kontroli zgodnie z paragrafem 37.

A227. Oszacowanie ryzyka kontroli przez audytora może zostać wykonane na różne sposoby w zależności od preferowanych technik lub metodyk badania i może być wyrażone na różne sposoby.

A228. Jeżeli audytor planuje przetestować skuteczność działania kontroli, konieczne może być, aby przetestować kombinację kontroli, aby potwierdzić oczekiwanie audytora, że kontrole działają skutecznie. Audytor może zaplanować przetestowanie zarówno bezpośrednich, jak i pośrednich

⁶⁰ MSB 540 (zmieniony), paragrafy A87-A89.

kontroli, w tym ogólnych kontroli IT, a jeżeli tak się stanie, to przy oszacowaniu ryzyka kontroli może wziąć pod uwagę łączny oczekiwany skutek kontroli. W zakresie, w jakim kontrola, która ma zostać przetestowana, nie odnosi się w pełni do oszacowanego ryzyka nieodłącznego, audytor ustala konsekwencje dla zaprojektowania dalszych procedur badania, aby ograniczyć ryzyko badania do akceptowalnie niskiego poziomu.

A229. Gdy audytor planuje przetestować skuteczność działania zautomatyzowanej kontroli, audytor może również zaplanować testowanie skuteczności działania stosownych ogólnych kontroli IT, które wspierają dalsze funkcjonowanie takiej zautomatyzowanej kontroli, aby odnieść się do ryzyk powstających na skutek wykorzystania IT oraz aby zapewnić podstawę dla oczekiwania audytora, że zautomatyzowana kontrola działała skutecznie przez cały okres. Gdy audytor spodziewa się, że powiązane ogólne kontrole IT są nieskuteczne, ustalenie to może mieć wpływ na oszacowanie przez audytora ryzyka kontroli na poziomie stwierdzeń, a dalsze procedury badania audytora mogą wymagać włączenia procedur wiarygodności, aby odnieść się do mających zastosowanie ryzyk powstających na skutek wykorzystania IT. Dalsze wytyczne dotyczące procedur, które audytor może wykonać w tych okolicznościach, zapewnia MSB 330⁶¹.

Ocena dowodów badania uzyskanych w ramach procedur oszacowania ryzyka (Zob. par. 35)

Dlaczego audytor ocenia dowody badania z procedur oszacowania ryzyka

A230. Dowody badania uzyskane z wykonania procedur oszacowania ryzyka zapewniają podstawę do identyfikacji i oszacowania ryzyk istotnego zniekształcenia. Zapewnia to podstawę do zaprojektowania przez audytora rodzaju, rozłożenia w czasie i zakresu dalszych procedur badania w reakcji na oszacowane ryzyka istotnego zniekształcenia na poziomie stwierdzeń, zgodnie z MSB 330. W związku z tym, dowody badania uzyskane z procedur oszacowania ryzyka zapewniają podstawę do identyfikacji i oszacowania ryzyk istotnego zniekształcenia, niezależnie od tego, czy zostały spowodowane oszustwem, czy błędem, na poziomie sprawozdania finansowego i na poziomie stwierdzeń.

Ocena dowodów badania

A231. Dowody badania z procedur oszacowania ryzyka obejmują zarówno informacje, które wspierają i potwierdzają stwierdzenia kierownictwa, jak i wszelkie informacje, które są sprzeczne z takimi stwierdzeniami⁶².

Zawodowy sceptycyzm

A232. Oceniając dowody badania z procedur oszacowania ryzyka, audytor rozważa, czy uzyskano wystarczające zrozumienie jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej i systemu kontroli wewnętrznej jednostki umożliwiające identyfikację ryzyk istotnego zniekształcenia, jak również, czy istnieją jakiegokolwiek sprzeczne ze sobą dowody, które mogą wskazywać na ryzyko istotnego zniekształcenia.

Grupy transakcji, salda kont i ujawnienia, które nie są znaczące, ale są istotne (Zob. par. 36)

A233. Jak wyjaśniono w MSB 320⁶³, podczas identyfikowania i oszacowania ryzyk istotnego zniekształcenia grup transakcji, sald kont i ujawnień rozważane są istotność i ryzyko badania. Ustalenie istotności przez audytora jest sprawą zawodowego osądu, na który wpływa postrzeganie

⁶¹ MSB 330, paragrafy A29-A31.

⁶² MSB 500, paragraf A5.

⁶³ MSB 320, paragraf A1.

przez audytora potrzeb użytkowników sprawozdania finansowego w zakresie informacji finansowych⁶⁴. Dla celów niniejszego MSB oraz paragrafu 18 w MSB 330, grupy transakcji, salda kont lub ujawnienia są istotne, jeżeli można byłoby racjonalnie oczekiwać, że pominięcie, zniekształcenie lub zaciemnienie informacji na ich temat mogłoby wpłynąć na decyzje ekonomiczne użytkowników podejmowane na podstawie sprawozdania finansowego jako całości.

- A234. Mogą występować grupy transakcji, salda kont lub ujawnienia, które są istotne, ale nie zostały określone jako znaczące grupy transakcji, salda kont lub ujawnienia (tj. nie zidentyfikowano żadnych stosownych stwierdzeń).

Przykład:

Jednostka może mieć ujawnienie dotyczące wynagrodzeń zarządu, dla którego audytor nie zidentyfikował ryzyka istotnego zniekształcenia. Audytor może jednak stwierdzić, że to ujawnienie jest istotne, opierając się na rozważaniach zawartych w paragrafie A233.

- A235. Procedury badania odnoszące się do grup transakcji, sald kont lub ujawnień, które są istotne, ale nie zostały określone jako znaczące, zostały omówione w MSB 330⁶⁵. Gdy grupa transakcji, saldo konta lub ujawnienie jest określone jako znaczące zgodnie z wymogami paragrafu 29, grupa transakcji, saldo konta lub ujawnienie stanowi również istotną grupę transakcji, saldo konta lub ujawnienie dla celów paragrafu 18 w MSB 330.

Weryfikacja oszacowania ryzyka (Zob. par. 37)

- A236. Podczas badania uwagę audytora mogą zwrócić nowe lub inne informacje, które różnią się znacząco od informacji, na których opierało się oszacowanie ryzyka.

Przykład:

Oszacowanie ryzyka przez jednostkę może być oparte na oczekiwaniu, że pewne kontrole działają skutecznie. Wykonując podczas badania testy tych kontroli, audytor może uzyskać dowody badania, że nie działały one skutecznie w stosownym czasie. Podobnie, wykonując procedury wiarygodności, audytor może wykryć zniekształcenia w kwotach lub o częstotliwości większej od spójnej z oszacowaniami ryzyka przez audytora. W takich okolicznościach oszacowanie ryzyka może nie odzwierciedlać odpowiednio prawdziwych okoliczności jednostki, a dalsze zaplanowane procedury badania mogą nie być skuteczne w wykryciu istotnych zniekształceń. Paragrafy 16 i 17 w MSB 330 zapewniają dalsze wytyczne dotyczące dokonywania oceny skuteczności działania kontroli.

Dokumentacja (Zob. par. 38)

- A237. Dla badań cyklicznych pewna część dokumentacji może być ponownie wykorzystana, zaktualizowana w miarę potrzeby, aby odzwierciedlić zmiany w działalności lub procesach jednostki.

- A238. Wśród innych rozważań, MSB 230 zauważa, że chociaż może nie istnieć jeden sposób udokumentowania zawodowego sceptycyzmu wykazywanego przez audytora, dokumentacja badania może jednak dostarczać dowodów na to, że audytor wykazuje zawodowy sceptycyzm⁶⁶. Na przykład, gdy dowody badania uzyskane z procedur oszacowania ryzyka zawierają dowody,

⁶⁴ MSB 320, paragraf 4.

⁶⁵ MSB 330, paragraf 18.

⁶⁶ MSB 230, paragraf A7.

które zarówno potwierdzają, jak i zaprzeczają stwierdzeniom kierownictwa, dokumentacja może obejmować sposób oceny tych dowodów przez audytora, w tym zawodowe osądy dokonane podczas dokonywania oceny czy dowody badania zapewniają odpowiednią podstawę do identyfikacji i oszacowania ryzyk istotnego zniekształcenia przez audytora. Przykłady innych wymogów zawartych w niniejszym MSB, dla których dokumentacja może dostarczyć dowodów stosowania zawodowego sceptycyzmu przez audytora, obejmują:

- paragraf 13, który wymaga, aby audytor zaprojektował i wykonał procedury oszacowania ryzyka w sposób, który jest bezstronny wobec uzyskiwania dowodów badania, które mogą potwierdzić istnienie ryzyk lub wobec wykluczenia dowodów badania, które mogą zaprzeczać istnieniu ryzyk,
- paragraf 17, który wymaga omówienia, w gronie kluczowych członków zespołu wykonującego zlecenie, zastosowania mających zastosowanie ramowych założeń sprawozdawczości finansowej i podatności sprawozdania finansowego jednostki na istotne zniekształcenie,
- paragrafy 19(b) i 20, które wymagają od audytora, aby uzyskał zrozumienie przyczyn wszelkich zmian zasad (polityki) rachunkowości jednostki oraz ocenił, czy zasady (polityka) rachunkowości jednostki są odpowiednie i spójne z mającymi zastosowanie ramowymi założeniami sprawozdawczości finansowej,
- paragrafy 21(b), 22(b), 23(b), 24(c), 25(c), 26(d) i 27, które wymagają, aby audytor ocenił na podstawie wymaganego uzyskanego zrozumienia, czy elementy systemu kontroli wewnętrznej jednostki są odpowiednie do okoliczności jednostki, uwzględniając charakter i złożoność jednostki oraz aby ustalił, czy zidentyfikowano jedną lub więcej słabości kontroli,
- paragraf 35, który wymaga, aby audytor wziął pod uwagę wszystkie dowody badania uzyskane z procedur oszacowania ryzyka, niezależnie od tego, czy są potwierdzające, czy sprzeczne ze stwierdzeniami dokonanymi przez kierownictwo oraz ocenił, czy dowody badania uzyskane z procedur oszacowania ryzyka zapewniają odpowiednią podstawę do identyfikacji i oszacowania ryzyk istotnego zniekształcenia, oraz
- paragraf 36, który wymaga, aby audytor ocenił, gdy ma to zastosowanie, czy ustalenie przez audytora, że nie istnieją ryzyka istotnego zniekształcenia dla istotnej grupy transakcji, salda konta lub ujawnienia, pozostaje właściwe.

Skalowalność

A239. Sposób dokumentowania wymogów określonych w paragrafie 38 jest ustalany przez audytora z wykorzystaniem zawodowego osądu.

A240. Aby wspierać uzasadnienia dokonanych trudnych osądów, może być wymagana bardziej szczegółowa dokumentacja, która jest wystarczająca, aby umożliwić doświadczonemu audytorowi, nieposiadającemu żadnego wcześniejszego doświadczenia w zakresie tego badania, zrozumienie rodzaju, rozłożenia w czasie i zakresu wykonanych procedur badania.

A241. Dla badań mniej złożonych jednostek forma i zakres dokumentacji mogą być proste i stosunkowo zwarte. Na formę i zakres dokumentacji audytora wpływa charakter, wielkość i złożoność jednostki oraz jej system kontroli wewnętrznej, dostępność informacji z jednostki oraz metodologia badania i technologia wykorzystywana podczas badania. Nie jest konieczne, aby dokumentować całość zrozumienia jednostki przez audytora oraz zagadnień z tym związanych. Kluczowe elementy⁶⁷ zrozumienia dokumentowane przez audytora mogą obejmować te, na których audytor oparł oszacowanie ryzyk istotnego zniekształcenia. Od audytora nie jest jednak

⁶⁷ MSB 230, paragraf 8.

wymagane, aby dokumentował każdy czynnik ryzyka nieodłącznego, który został wzięty pod uwagę podczas identyfikowania i oszacowania ryzyk istotnego zniekształcenia na poziomie stwierdzeń.

Przykład:

Podczas badania mniej złożonych jednostek dokumentacja badania może być włączona do dokumentacji audytora dotyczącej ogólnej strategii i planu badania⁶⁸. Podobnie, na przykład, wyniki oszacowania ryzyka mogą być udokumentowane oddzielenie lub mogą być udokumentowane jako część dokumentacji audytora dotyczącej dalszych procedur badania⁶⁹.

⁶⁸ MSB 300 *Planowanie badania sprawozdania finansowego*, paragrafy 7, 9 i A13.

⁶⁹ MSB 330, paragraf 28.

Załącznik 1

(Zob. par. A61–A67)

Rozważania dotyczące zrozumienia jednostki i jej modelu biznesowego

Niniejszy załącznik wyjaśnia cele i zakres modelu biznesowego jednostki oraz dostarcza przykłady zagadnień, które audytor może rozważyć uzyskując zrozumienie działań jednostki, które mogą być zawarte w modelu biznesowym. Zrozumienie przez audytora modelu biznesowego jednostki oraz w jaki sposób wpływa na niego strategia biznesowa i cele gospodarcze, może pomóc audytorowi w identyfikowaniu ryzyk gospodarczych, które mogą mieć wpływ na sprawozdanie finansowe. Ponadto, może to pomóc audytorowi w identyfikowaniu ryzyk istotnego zniekształcenia.

Cele i zakres modelu biznesowego jednostki

1. Model biznesowy jednostki opisuje sposób, w jaki jednostka rozważa na przykład swoją strukturę organizacyjną, prowadzenie lub zakres działalności, linie biznesowe (w tym konkurentów i jej klientów), procesy, możliwości wzrostu, globalizację, wymogi regulacyjne i technologie. Model biznesowy jednostki opisuje sposób, w jaki jednostka tworzy, zachowuje i ujmuje wartość finansową lub szerszą wartość dla swoich interesariuszy.
2. Strategie to podejścia, poprzez które kierownictwo planuje osiągnąć cele jednostki, w tym sposób, w jaki jednostka planuje odnieść się do ryzyk i szans, z którymi się mierzy. Strategie jednostki są zmieniane w czasie przez kierownictwo, aby odpowiedzieć na zmiany w jej celach oraz w wewnętrznych i zewnętrznych okolicznościach, w których prowadzi ona działalność.
3. Opis modelu biznesowego zazwyczaj obejmuje:
 - zakres działalności jednostki i dlaczego ją wykonuje,
 - strukturę i skalę działania jednostki,
 - rynki lub sfery geograficzne lub demograficzne, oraz części łańcucha wartości, w których działa, sposób, w jaki angażuje się w te rynki lub sfery (główne produkty, segmenty klientów i metody dystrybucji) oraz podstawy, na jakich konkuruje,
 - procesy biznesowe lub operacyjne jednostki (np. procesy inwestycyjne, finansowe i operacyjne) wykorzystywane w prowadzeniu jej działalności, koncentrujące się na tych częściach procesów biznesowych, które są ważne podczas tworzenia, utrzymania lub ujmowania wartości,
 - zasoby (np. finansowe, ludzkie, intelektualne, środowiskowe i technologiczne) oraz inne nakłady i relacje (np. z klientami, konkurentami, dostawcami i pracownikami), które są niezbędne lub ważne dla jej sukcesu,
 - w jaki sposób model biznesowy jednostki integruje wykorzystanie IT w jej kontaktach z klientami, dostawcami, kredytodawcami i innymi interesariuszami poprzez interfejsy IT i inne technologie.
4. Ryzyko gospodarcze może mieć bezpośrednie konsekwencje dla ryzyka istotnego zniekształcenia dla grup transakcji, sald kont oraz ujawnień na poziomie stwierdzeń lub na poziomie sprawozdania finansowego. Na przykład, ryzyko gospodarcze powstające na skutek znaczącego spadku wartości rynkowej nieruchomości może zwiększyć ryzyko istotnego zniekształcenia związane ze stwierdzeniem dotyczącym wyceny dla udzielającego średnioterminowych kredytów zabezpieczonych na nieruchomościach. Jednakże, to samo ryzyko, szczególnie w połączeniu z poważnym spowolnieniem koniunktury gospodarczej, które jednocześnie zwiększa na jego

kredytach bazowe ryzyko strat kredytowych w całym okresie kredytowania, może mieć również skutki długoterminowe. Wynikające z tego narażenie netto na straty kredytowe może budzić znaczące wątpliwości co do zdolności jednostki do kontynuowania działalności. Jeżeli taka sytuacja ma miejsce, może to mieć konsekwencje dla wniosku kierownictwa i audytora co do odpowiedniości wykorzystania przez jednostkę zasady kontynuacji działalności oraz ustalenia, czy występuje istotna niepewność. Czy ryzyko gospodarcze może skutkować ryzykiem istotnego zniekształcenia, rozważa się zatem w świetle okoliczności jednostki. Przykłady zdarzeń i uwarunkowań, które mogą powodować występowanie ryzyk istotnego zniekształcenia wskazano w **Załączniku 2**.

Działalność jednostki

5. Przykłady zagadnień, które audytor może rozważyć uzyskując zrozumienie działalności jednostki (zawarte w modelu biznesowym jednostki) obejmują:

(a) działalność gospodarcza, taka jak:

- charakter źródeł przychodów, produktów lub usług oraz rynków, w tym zaangażowanie w handel elektroniczny, takie jak sprzedaż internetowa i działania marketingowe,
- prowadzenie działalności (na przykład etapy i metody produkcji lub działania narażone na ryzyka środowiskowe),
- sojusze, wspólne przedsięwzięcia i działalność outsourcingowa,
- rozproszenie geograficzne i segmentacja branżowa,
- lokalizacja zakładów produkcyjnych, magazynów i biur oraz lokalizacja i ilość zapasów,
- kluczowi klienci i ważni dostawcy towarów i usług, ustalenia dotyczące zatrudnienia (w tym istnienie kontraktów związkowych, świadczeń emerytalnych i innych świadczeń po okresie zatrudnienia, ustalenia dotyczące opcji na akcje lub premii motywacyjnych oraz regulacje rządowe związane ze sprawami zatrudnienia),
- działalność i wydatki w zakresie badań i rozwoju,
- transakcje ze stronami powiązanymi,

(b) inwestycje i działalność inwestycyjna, takie jak:

- planowane lub niedawno zrealizowane przejęcia lub zbycia,
- inwestycje i zbycie papierów wartościowych oraz pożyczki,
- działalność w zakresie inwestycji kapitałowych,
- inwestycje w jednostkach nie objętych konsolidacją, w tym w niekontrolowanych spółkach osobowych, wspólnych przedsięwzięciach i niekontrolowanych jednostkach specjalnego przeznaczenia,

(c) finansowanie i działalność finansowa, taka jak:

- struktura właścicielska głównych jednostek zależnych i stowarzyszonych, w tym struktury konsolidowane i niekonsolidowane,
- struktura zadłużenia i związane z tym warunki, w tym pozabilansowe umowy finansowania i umowy leasingowe,

- beneficjenci rzeczywiści (na przykład lokalni, zagraniczni, o uznanej reputacji i doświadczeniu biznesowym) oraz strony powiązane,
- korzystanie z pochodnych instrumentów finansowych.

Charakter jednostek specjalnego przeznaczenia

6. Jednostka specjalnego przeznaczenia (czasami określana jako wehikuł specjalnego przeznaczenia) to jednostka, która jest zazwyczaj ustanawiana w wąskim i ściśle określonym celu, takim jak osiągnięcie skutku w postaci leasingu lub sekurytyzacji aktywów finansowych lub prowadzenie działalności badawczej i rozwojowej. Może mieć formę korporacji, zarządu powierniczego, spółki osobowej lub podmiotu nieposiadającego osobowości prawnej. Jednostka, w imieniu której utworzono jednostkę specjalnego przeznaczenia, może często przenosić aktywa na taką jednostkę (na przykład jako część transakcji zaprzestania ujmowania aktywów finansowych), uzyskiwać prawo do użytkowania jej aktywów lub świadczenia na jej rzecz usług, podczas gdy inne strony mogą zapewnić jej finansowanie. Jak wskazuje MSB 550, w niektórych okolicznościach, jednostka specjalnego przeznaczenia może być stroną powiązaną z jednostką.¹
7. Ramowe założenia sprawozdawczości finansowej często określają szczegółowe warunki, które są uważane za stanowienie kontroli lub okoliczności, w których jednostka specjalnego przeznaczenia powinna być rozważana dla celów konsolidacji. Interpretacja wymogów takich ramowych założeń często wymaga szczegółowej wiedzy na temat stosownych umów z udziałem jednostki specjalnego przeznaczenia.

¹ MSB 550, paragraf A7.

Załącznik 2

(Zob. par. 12(f), 19(c), A7–A8, A85–A89)

Zrozumienie czynników ryzyka nieodłącznego

Niniejszy załącznik zapewnia dalsze wyjaśnienia dotyczące czynników ryzyka nieodłącznego, jak również zagadnień, które audytor może rozważyć podczas uzyskiwania zrozumienia i zastosowania czynników ryzyka nieodłącznego podczas identyfikowania i oszacowania ryzyk istotnego zniekształcenia na poziomie stwierdzeń.

Czynniki ryzyka nieodłącznego

1. Czynniki ryzyka nieodłącznego to cechy zdarzeń lub warunków, które wpływają na podatność stwierdzenia dotyczącego grupy transakcji, salda konta lub ujawnienia na zniekształcenia, niezależnie od tego, czy zostały one spowodowane oszustwem, czy błędem, a przed rozważeniem kontroli. Czynniki takie mogą być jakościowe lub ilościowe i obejmują złożoność, subiektywizm, zmianę, niepewność lub podatność na zniekształcenie wynikające ze stronniczości kierownictwa lub innych czynników ryzyka oszustwa¹, o ile mają one wpływ na ryzyko nieodłączne. Uzyskując zrozumienie jednostki i jej otoczenia oraz mających zastosowanie ramowych założeń sprawozdawczości finansowej i zasad (polityki) rachunkowości jednostki, zgodnie z paragrafami 19(a)-(b), audytor posiada również zrozumienie, w jaki sposób czynniki ryzyka nieodłącznego wpływają na podatność stwierdzeń na zniekształcenie podczas sporządzania sprawozdania finansowego.
2. Czynniki ryzyka nieodłącznego związane ze sporządzaniem informacji wymaganych przez mające zastosowanie ramowe założenia sprawozdawczości finansowej (zwane w niniejszym paragrafie „wymaganyymi informacjami”) obejmują:
 - *Złożoność* – powstaje na skutek albo charakteru informacji, albo sposobu, w jaki sporządzane są wymagane informacje, w tym, gdy takie procesy przygotowawcze są z natury swej trudniejsze do zastosowania. Na przykład, złożoność może powstać:
 - podczas kalkulowania rezerw na rabaty dla dostawców, ponieważ może być konieczne, aby wziąć pod uwagę różne warunki handlowe z wieloma różnymi dostawcami lub wiele powiązanych ze sobą warunków handlowych, spośród których wszystkie są stosowne dla kalkulowania należnych rabatów, lub
 - gdy istnieje wiele potencjalnych źródeł danych, o różnych cechach wykorzystywanych podczas dokonywania szacunku księgowego, przetwarzanie tych danych obejmuje wiele powiązanych ze sobą kroków, a zatem dane te są z natury swej trudniejsze do zidentyfikowania, pozyskania, dostępu, zrozumienia lub przetworzenia.
 - *Subiektywizm* – wynika z nieodłącznych ograniczeń zdolności do sporządzenia wymaganych informacji w sposób obiektywny, ze względu na ograniczenia w dostępności wiedzy lub informacji, które mogą wymagać od kierownictwa dokonania wyboru lub subiektywnego osądu dotyczącego przyjęcia właściwego podejścia oraz wynikających z niego informacji, które należy uwzględnić w sprawozdaniu finansowym. Ze względu na różne podejścia do sporządzania wymaganych informacji, różne rezultaty mogłyby

¹ MSB 240, paragrafy A24–A27.

wynikać z właściwego zastosowania wymogów mających zastosowanie ramowych założeń sprawozdawczości finansowej. Wraz ze wzrostem ograniczeń w zakresie wiedzy lub danych, zwiększy się również subiektywizm osądów, które mogłyby zostać dokonane przez osoby posiadające odpowiednią wiedzę i niezależne, a także zróżnicowanie możliwych rezultatów tych osądów.

- *Zmiana* – wynika ze zdarzeń lub warunków, które na przestrzeni czasu mają wpływ na działalność jednostki lub na ekonomiczne, księgowe, regulacyjne, branżowe lub inne aspekty środowiska, w którym jednostka działa, gdy skutki tych zdarzeń lub warunków są odzwierciedlone w wymaganych informacjach. Takie zdarzenia lub warunki mogą wystąpić w trakcie okresów sprawozdawczości finansowej lub pomiędzy tymi okresami. Na przykład, zmiana może wynikać z rozwoju w wymogach mających zastosowanie ramowych założeń sprawozdawczości finansowej lub samej jednostki i jej modelu biznesowego, lub środowiska, w którym jednostka działa. Taka zmiana może mieć wpływ na założenia i osądy kierownictwa, w tym na wybór przez kierownictwo zasad (polityki) rachunkowości lub w jaki sposób dokonywane są szacunki księgowe, lub ustalone związane z nimi ujawnienia.
 - *Niepewność* – powstaje, gdy wymagane informacje nie mogą zostać sporządzone tylko na podstawie wystarczająco dokładnych i wyczerpujących danych, które można zweryfikować poprzez bezpośrednie obserwacje. W takich okolicznościach może zaistnieć potrzeba przyjęcia podejścia, w którym zastosowano dostępną wiedzę, aby sporządzić informacje wykorzystując wystarczająco dokładne i wyczerpujące możliwe do zaobserwowania dane, w dostępnym zakresie, oraz racjonalne założenia poparte najwłaściwszymi dostępnymi danymi, gdy ich nie ma. Ograniczenia w dostępności wiedzy lub danych, które nie znajdują się pod kontrolą kierownictwa (z zastrzeżeniem ograniczeń kosztowych, gdzie ma to zastosowanie) są źródłami niepewności i nie można wyeliminować ich wpływu na sporządzanie wymaganych informacji. Na przykład, niepewność szacunków powstaje, gdy nie można precyzyjnie określić wymaganej kwoty pieniężnej, a wynik szacunku nie jest znany przed dniem ukończenia sprawozdania finansowego.
 - *Podatność na zniekształcenie spowodowane stronniczością kierownictwa lub innymi czynnikami ryzyka oszustwa w zakresie, w jakim wpływają one na ryzyko nieodłączne* – podatność na stronniczość kierownictwa wynika z warunków, które stwarzają podatność na celowe lub niezamierzone niezachowanie przez kierownictwo neutralności podczas sporządzania informacji. Stronniczość kierownictwa jest często związana z pewnymi warunkami, które mogą potencjalnie powodować, że kierownictwo nie zachowa neutralności w dokonywaniu osądu (wskaźniki potencjalnej stronniczości kierownictwa), co mogłoby prowadzić do istotnego zniekształcenia informacji, które byłoby oszustwem, gdyby było zamierzone. Wskaźniki takie obejmują zachęty lub naciski w zakresie, w jakim wpływają one na ryzyko nieodłączne (na przykład w wyniku motywacji do osiągnięcia pożądanego rezultatu, takiego jak pożądaný cel zysku lub wskaźnik kapitałowy) oraz możliwość niezachowania neutralności. Czynniki stosowne dla podatności na zniekształcenie spowodowane oszustwem w formie oszukańczej sprawozdawczości finansowej lub sprzeniewierzenia aktywów zostały opisane w paragrafach A1 do A5 w MSB 240.
3. Gdy złożoność jest czynnikiem ryzyka nieodłącznego, może istnieć nieodłączna potrzeba bardziej złożonych procesów sporządzania informacji, a takie procesy mogą być z natury swej trudniejsze do zastosowania. W wyniku tego, ich stosowanie może wymagać specjalistycznych umiejętności lub wiedzy, a także może wymagać wykorzystania eksperta kierownictwa.

4. Gdy osąd kierownictwa jest bardziej subiektywny, może również wzrosnąć podatność na zniekształcenie spowodowane stronniczością kierownictwa, niezależnie od tego, czy jest ona nieumyślna, czy celowa. Na przykład, podczas dokonywania szacunków księgowych, które zostały zidentyfikowane jako obarczone wysoką niepewnością oszacowania, może być zastosowany znaczący osąd kierownictwa, a wnioski dotyczące metod, danych i założeń mogą odzwierciedlać niezamierzoną lub celową stronniczość kierownictwa.

Przykłady zdarzeń lub warunków, które mogą powodować występowanie ryzyk istotnego zniekształcenia

5. Poniżej podano przykłady zdarzeń (w tym transakcji) i warunków, które mogą wskazywać na istnienie ryzyk istotnego zniekształcenia sprawozdania finansowego, na poziomie sprawozdania finansowego lub na poziomie stwierdzeń. Przykłady przedstawione według czynnika ryzyka nieodłącznego obejmują szeroki zakres zdarzeń i warunków, jednakże nie wszystkie zdarzenia i warunki są stosowne dla każdego zlecenia badania, a lista przykładów niekoniecznie jest pełna. Zdarzenia i warunki zostały podzielone na kategorie według czynnika ryzyka nieodłącznego, który może mieć największy wpływ w danych okolicznościach. Co ważne, ze względu na wzajemne powiązania między czynnikami ryzyka nieodłącznego, przykładowe zdarzenia i warunki prawdopodobnie będą również podlegać innym czynnikom ryzyka nieodłącznego lub inne czynniki ryzyka nieodłącznego będą na nie wpływać w różnym stopniu.

Stosowny czynnik ryzyka nieodłącznego:	Przykłady zdarzeń lub warunków, które mogą wskazywać na występowanie ryzyk istotnego zniekształcenia na poziomie stwierdzeń:
Złożoność	Regulacyjne: - Operacje, które podlegają wysokiemu poziomowi złożonych regulacji. Model biznesowy: - Istnienie złożonych aliansów i wspólnych przedsięwzięć. Mające zastosowanie ramowe założenia sprawozdawczości finansowej: - Wyceny księgowe, które obejmują złożone procesy. Transakcje: - Korzystanie z finansowania pozabilansowego, jednostek specjalnego przeznaczenia i innych złożonych porozumień finansowych.
Subiektywizm	Mające zastosowanie ramowe założenia sprawozdawczości finansowej: - Szeroki zakres możliwych kryteriów wyceny szacunków księgowych. Na przykład, ujmowanie przez kierownictwo odpisów amortyzacyjnych lub przychodów i kosztów budowy. - Wybór przez kierownictwo techniki lub modelu wyceny aktywów trwałych, takich jak nieruchomości inwestycyjne.
Zmiana	Warunki ekonomiczne: Działalność w regionach niestabilnych gospodarczo, na przykład w krajach o znaczącej dewaluacji waluty lub gospodarkach o wysokiej inflacji.

Stosowny czynnik ryzyka nieodłącznego:	Przykłady zdarzeń lub warunków, które mogą wskazywać na występowanie ryzyk istotnego zniekształcenia na poziomie stwierdzeń:
	Rynki: - Działalność narażona na zmienność rynków, na przykład handel kontraktami terminowymi. Utrata klientów: - Kontynuacja działalności i kwestie płynności, w tym utrata znaczących klientów. Model branżowy: - Zmiany w branży, w której jednostka prowadzi działalność. Model biznesowy: - Zmiany w łańcuchu dostaw. - Opracowywanie lub oferowanie nowych produktów lub usług, lub przechodzenie do nowych linii biznesowych. Geografia: - Ekspansja do nowych lokalizacji. Struktura jednostki: - Zmiany w jednostce, takie jak duże przejęcia lub reorganizacje, lub inne nietypowe zdarzenia. - Jednostki lub segmenty działalności, które prawdopodobnie zostaną sprzedane. Kompetencje zasobów ludzkich: - Zmiany kluczowego personelu, w tym odejścia kluczowych członków kierownictwa. IT: - Zmiany w środowisku IT. - Instalacja znaczących nowych systemów IT związanych ze sprawozdawczością finansową. Mające zastosowanie ramowe założenia sprawozdawczości finansowej: - Zastosowanie nowych ogłoszonych wymogów rachunkowych. Kapitał: - Nowe ograniczenia dostępności kapitału i kredytów. Regulacyjne: - Rozpoczęcie dochodzeń w sprawie działalności lub wyników finansowych jednostki przez organy regulacyjne lub rządowe. - Wpływ nowego ustawodawstwa związanego z ochroną środowiska.

Stosowny czynnik ryzyka nieodłącznego:	Przykłady zdarzeń lub warunków, które mogą wskazywać na występowanie ryzyk istotnego zniekształcenia na poziomie stwierdzeń:
Niepewność	Sprawozdawczość: - Zdarzenia lub transakcje, które wiążą się ze znaczącą niepewnością wyceny, w tym szacunki księgowe i związane z nimi ujawnienia. - Trwające postępowania sądowe i zobowiązania warunkowe, na przykład gwarancje związane ze sprzedażą, gwarancje finansowe i rekultywacja środowiska.
Podatność na zniekształcenia spowodowane stronniczością kierownictwa lub innymi czynnikami ryzyka oszustwa, o ile mają one wpływ na ryzyko nieodłączne.	Sprawozdawczość: - Sposobność, aby kierownictwo i pracownicy zaangażowali się w oszukańczą sprawozdawczość finansową, w tym pomijanie lub zaciemnianie znaczących informacji w ujawnieniach. Transakcje: - Znaczące transakcje ze stronami powiązanymi. - Znacząca ilość nierutynowych lub niesystematycznych transakcji, w tym transakcji pomiędzy spółkami wewnątrz grupy kapitałowej oraz dużych transakcji dotyczących przychodów na koniec okresu. - Transakcje, które są rejestrowane na podstawie zamiarów kierownictwa, na przykład refinansowanie zadłużenia, aktywa przeznaczone do sprzedaży i klasyfikacja zbywalnych papierów wartościowych.

Inne zdarzenia lub warunki, które mogą wskazywać na ryzyka istotnego zniekształcenia na poziomie sprawozdania finansowego:

- brak personelu posiadającego odpowiednie umiejętności w zakresie rachunkowości i sprawozdawczości finansowej,
- słabości kontroli – w szczególności w środowisku kontroli, procesie oszacowania ryzyka i procesie monitorowania, a zwłaszcza te, do których nie odniosło się kierownictwo,
- zniekształcenia w przeszłości, historia błędów lub znacząca kwota korekt na koniec okresu.

Załącznik 3

(Zob. par. 12(m), 21-26, A90-A181)

Zrozumienie systemu kontroli wewnętrznej jednostki

1. System kontroli wewnętrznej jednostki może być odzwierciedlony w polityce i podręcznikach procedur, systemach i formularzach oraz zawartych w nich informacjach i jest realizowany przez ludzi. System kontroli wewnętrznej jednostki jest wdrażany przez kierownictwo, osoby sprawujące nadzór i innych pracowników w oparciu o strukturę jednostki. System kontroli wewnętrznej jednostki może być zastosowany do modelu działalności jednostki, struktury podmiotu prawnego lub ich połączenia, na podstawie decyzji kierownictwa, osób sprawujących nadzór lub innych pracowników oraz w kontekście wymogów prawnych lub regulacyjnych.
2. Niniejszy załącznik zawiera dalsze wyjaśnienia dotyczące elementów oraz ograniczeń systemu kontroli wewnętrznej jednostki, opisanych w paragrafach 12(m), 21-26 oraz A90-A181, ponieważ odnoszą się one do badania sprawozdań finansowych.
3. W systemie kontroli wewnętrznej jednostki zawarte są aspekty odnoszące się do celów sprawozdawczych jednostki, w tym jej celów sprawozdawczości finansowej, ale może on również obejmować aspekty odnoszące się do jej celów w zakresie działalności lub zgodności, gdy takie aspekty są stosowne dla sprawozdawczości finansowej.

Przykład:

Kontrole zgodności z przepisami prawa i regulacjami mogą być stosowne dla sprawozdawczości finansowej, gdy takie kontrole są stosowne dla sporządzania przez jednostkę ujawnień dotyczących zobowiązań warunkowych w sprawozdaniu finansowym.

Elementy systemu kontroli wewnętrznej jednostki*Środowisko kontroli*

4. Środowisko kontroli obejmuje funkcje nadzoru i zarządzania oraz postawy, świadomość i działania osób sprawujących nadzór i kierownictwa w zakresie systemu kontroli wewnętrznej jednostki oraz jego znaczenia w jednostce. Środowisko kontroli nadaje ton organizacji, wpływając na świadomość kontroli jej personelu i zapewnia ogólną podstawę działania pozostałych elementów systemu kontroli wewnętrznej jednostki.
5. Na świadomość kontroli w jednostce mają wpływ osoby sprawujące nadzór, ponieważ jedną z ich ról jest równoważenie nacisków na kierownictwo w odniesieniu do sprawozdawczości finansowej, które mogą powstawać na skutek wymagań rynku lub systemów wynagrodzeń. Na skuteczność zaprojektowania środowiska kontroli w odniesieniu do udziału osób sprawujących nadzór wpływ mają zatem takie sprawy, jak:
 - ich niezależność od kierownictwa i zdolność do oceny działań kierownictwa,
 - czy rozumieją transakcje gospodarcze jednostki,
 - zakres, w jakim oceniają, czy sprawozdanie finansowe zostało sporządzone zgodnie z mającymi zastosowanie ramowymi założeniami sprawozdawczości finansowej, w tym, czy sprawozdanie finansowe zawiera adekwatne ujawnienia.
6. Środowisko kontroli obejmuje następujące elementy:

- (a) *Jak realizowane są przez kierownictwo takie obowiązki, jak stworzenie i utrzymywanie kultury jednostki oraz wykazywanie zaangażowania kierownictwa na rzecz uczciwości i wartości etycznych.* Skuteczność kontroli nie może wznosić się ponad uczciwość i wartości etyczne osób, które je tworzą, zarządzają nimi i monitorują je. Uczciwość i etyczne zachowanie są wynikiem standardów etycznych i postępowania jednostki lub kodeksów postępowania, sposobu ich komunikowania (np. poprzez oświadczenia dotyczące polityki) oraz sposobu, w jaki są one wspierane w praktyce (np. poprzez działania kierownictwa, aby eliminować lub osłabiać zachęty lub pokusy, które mogłyby skłonić personel do angażowania się w nieuczciwe, nielegalne lub nieetyczne działania). Komunikowanie polityk jednostki w zakresie uczciwości i wartości etycznych może obejmować komunikowanie pracownikom standardów postępowania poprzez oświadczenia dotyczące polityki i kodeksy postępowania oraz poprzez przykład.
- (b) *Gdy osoby sprawujące nadzór są oddzielone od kierownictwa, w jaki sposób osoby sprawujące nadzór wykazują niezależność od kierownictwa i sprawują nadzór nad systemem kontroli wewnętrznej w jednostce.* Osoby sprawujące nadzór mają wpływ na świadomość kontroli w jednostce. Rozważania mogą obejmować, czy istnieje wystarczająca liczba osób, które są niezależne od kierownictwa oraz obiektywne w swoich ocenach i podejmowaniu decyzji; w jaki sposób osoby sprawujące nadzór identyfikują i przyjmują odpowiedzialność za nadzór oraz czy osoby sprawujące nadzór zachowują odpowiedzialność za nadzór nad projektowaniem, wdrażaniem i kierowaniem systemem kontroli wewnętrznej w jednostce przez kierownictwo. Znaczenie odpowiedzialności osób sprawujących nadzór jest uznane w kodeksach postępowania oraz innych przepisach prawa i regulacjach lub wytycznych opracowanych na rzecz osób sprawujących nadzór. Inne obowiązki osób sprawujących nadzór obejmują nadzór nad zaprojektowaniem i skutecznym działaniem procedur zgłaszania naruszeń.
- (c) *W jaki sposób jednostka przydziela uprawnienia i odpowiedzialność w dążeniu do swoich celów.* Może to obejmować rozważania dotyczące:
- kluczowych obszarów uprawnień i odpowiedzialności oraz odpowiednich linii raportowania,
 - polityk związanych z odpowiednimi praktykami biznesowymi, wiedzą i doświadczeniem kluczowego personelu oraz zasobami zapewnionymi, aby wykonać obowiązki, oraz
 - polityk i komunikacji nakierowanych na zapewnienie, że wszyscy pracownicy rozumieją cele jednostki, wiedzą, jak ich indywidualne działania są ze sobą powiązane i przyczyniają się do realizacji tych celów, a także rozumieją, w jaki sposób i za co będą rozliczani.
- (d) *W jaki sposób jednostka przyciąga, rozwija i zatrzymuje kompetentne osoby zgodnie ze swoimi celami.* Obejmuje to również sposób, w jaki jednostka zapewnia, że osoby posiadają wiedzę i umiejętności niezbędne do realizacji zadań, które określają pracę danej osoby, taki jak:
- standardy rekrutacji najbardziej wykwalifikowanych osób – z naciskiem na wykształcenie, wcześniejsze doświadczenie zawodowe, dotychczasowe osiągnięcia oraz dowody uczciwości i etycznego zachowania,
 - polityki szkoleniowe, które komunikują przyszłe role i odpowiedzialności, w tym takie praktyki, jak programy szkoleniowe i seminaria, które ilustrują oczekiwane poziomy wykonania i zachowania, oraz

- okresowe oceny wyników kierujące awansami, które pokazują zaangażowanie jednostki w awansowanie wykwalifikowanego personelu na wyższe poziomy odpowiedzialności.
- (e) *W jaki sposób jednostka rozlicza poszczególne osoby z ich odpowiedzialności w dążeniu do celów systemu kontroli wewnętrznej jednostki.* Można to osiągnąć, na przykład, poprzez:
- mechanizmy komunikacji i rozliczania poszczególnych osób z wykonywania obowiązków w zakresie kontroli oraz wdrażania działań naprawczych, kiedy jest to potrzebne,
 - ustanowienie miar wyników działalności, zachęt i nagród dla osób odpowiedzialnych za system kontroli wewnętrznej jednostki, w tym sposób oceny tych miar i zachowanie ich stosowności,
 - w jaki sposób presje związane z osiągnięciem celów kontroli wpływają na obowiązki poszczególnych osób i miary wyników działalności, oraz
 - w jaki sposób poszczególne osoby są w razie potrzeby dyscyplinowane.

Odpowiedniość powyższych zagadnień będzie różna dla każdej jednostki w zależności od jej wielkości, złożoności jej struktury i charakteru działalności.

Proces oszacowania ryzyka przez jednostkę

7. Proces oszacowania ryzyka przez jednostkę jest iteratywnym procesem identyfikowania i analizowania ryzyk dla osiągnięcia celów jednostki i stanowi podstawę do określenia, w jaki sposób kierownictwo lub osoby sprawujące nadzór określają ryzyka, którymi należy zarządzać.
8. Dla celów sprawozdawczości finansowej, proces oszacowania ryzyka przez jednostkę obejmuje sposób, w jaki kierownictwo identyfikuje ryzyka gospodarcze stosowne dla sporządzania sprawozdania finansowego zgodnie z mającymi zastosowanie w jednostce ramowymi założeniami sprawozdawczości finansowej, dokonuje oszacowania ich znaczenia, ocenia prawdopodobieństwo ich wystąpienia oraz decyduje o działaniach podejmowanych, aby zarządzać nimi i ich skutkami. Na przykład, proces oszacowania ryzyka przez jednostkę może odnosić się do tego, w jaki sposób jednostka rozważa możliwość wystąpienia niezarejestrowanych transakcji lub identyfikuje i analizuje znaczące szacunki ujęte w sprawozdaniu finansowym.
9. Ryzyka stosowne dla wiarygodnej sprawozdawczości finansowej obejmują zdarzenia zewnętrzne i wewnętrzne, transakcje lub okoliczności, które mogą wystąpić i niekorzystnie wpłynąć na zdolność jednostki do inicjowania, rejestrowania, przetwarzania i raportowania informacji finansowych spójnych ze stwierdzeniami kierownictwa w sprawozdaniu finansowym. Kierownictwo może inicjować plany, programy lub działania, aby odnieść się do konkretnych ryzyk lub może zdecydować się podjąć ryzyko ze względu na koszty lub inne okoliczności. Ryzyka mogą powstać lub ulec zmianie ze względu na okoliczności takie jak następujące:
 - *Zmiany w funkcjonującym środowisku.* Zmiany w środowisku regulacyjnym, gospodarczym lub operacyjnym mogą skutkować zmianami w presji konkurencyjnej i znacząco różnymi ryzykami.
 - *Nowy personel.* Nowy personel może skupiać się na czymś innym lub wykazywać inne zrozumienie systemu kontroli wewnętrznej jednostki.
 - *Nowy lub zmodernizowany system informacyjny.* Znaczące i szybkie zmiany w systemie informacyjnym mogą zmienić ryzyko związane z systemem kontroli wewnętrznej jednostki.

- *Szybki wzrost.* Znacząca i szybka ekspansja działalności może nadwyrężyć kontrole i zwiększyć ryzyko załamania kontroli.
- *Nowa technologia.* Włączenie nowych technologii do procesów produkcyjnych lub systemu informacyjnego może zmienić ryzyko związane z systemem kontroli wewnętrznej jednostki.
- *Nowe modele biznesowe, produkty lub działania.* Wejście w obszary działalności lub transakcje, w których jednostka ma niewielkie doświadczenie, może wprowadzać nowe ryzyka związane z systemem kontroli wewnętrznej jednostki.
- *Restrukturyzacje przedsiębiorstwa.* Restrukturyzacja może towarzyszyć redukcje zatrudnienia oraz zmiany w nadzorze i podziale obowiązków, które mogą zmienić ryzyko związane z systemem kontroli wewnętrznej jednostki.
- *Rozszerzona działalność zagraniczna.* Ekspansja lub nabycie jednostek zagranicznych niesie nowe i często niepowtarzalne ryzyka, które mogą wpłynąć na kontrolę wewnętrzną, na przykład dodatkowe lub zmienione ryzyka wynikające z transakcji w walutach obcych.
- *Nowe ogłoszone wymogi księgowe.* Przyjęcie nowych zasad (polityki) rachunkowości lub zmiana zasad (polityki) rachunkowości może mieć wpływ na ryzyka związane ze sporządzaniem sprawozdania finansowego.
- *Wykorzystanie IT.* Ryzyka związane z:
 - utrzymaniem integralności przetwarzania danych i informacji,
 - ryzykami strategii biznesowej jednostki, które powstają, jeżeli strategia IT jednostki nie wspiera skutecznie strategii biznesowej jednostki, lub
 - zmianami lub przerwami w środowisku IT jednostki lub rotacją personelu IT lub gdy jednostka nie dokonuje niezbędnych aktualizacji środowiska IT, lub aktualizacje takie nie są przeprowadzane terminowo.

Proces monitorowania systemu kontroli wewnętrznej jednostki

10. Proces monitorowania systemu kontroli wewnętrznej jednostki jest procesem ciągłym, aby ocenić skuteczność systemu kontroli wewnętrznej jednostki oraz podjąć terminowo niezbędne działania naprawcze. Proces monitorowania systemu kontroli wewnętrznej jednostki może obejmować prowadzenie bieżących działań, odrębne oceny (przeprowadzane okresowo) lub jakieś połączenie tych dwóch elementów. Bieżące działania monitorujące są często wbudowane w zwykłą, powtarzalną działalność jednostki i mogą obejmować normalne działania w zakresie zarządzania i nadzoru. Prawdopodobnie proces jednostki będzie miał różny zakres i częstotliwość w zależności od oszacowania ryzyk przez jednostkę.
11. Cele i zakres funkcji audytu wewnętrznego obejmują zazwyczaj działania zaprojektowane, aby oceniać lub monitorować skuteczność systemu kontroli wewnętrznej jednostki¹. Proces monitorowania systemu kontroli wewnętrznej jednostki może obejmować takie działania, jak przegląd przez kierownictwo czy uzgodnienia sald bankowych są terminowo sporządzane, ocena przez audytorów wewnętrznych zgodności pracowników sprzedaży z politykami jednostki w zakresie warunków umów sprzedaży oraz nadzór działu prawnego nad zgodnością z politykami jednostki w zakresie etyki lub praktyk biznesowych. Monitoring prowadzony jest również, aby zapewnić, że kontrole nadal skutecznie działają na przestrzeni czasu. Na przykład, jeżeli nie jest

¹ MSB 610 (zmieniony w 2013 r.) oraz Załącznik 4 do tego MSB zapewniają dalsze wytyczne związane z audytem wewnętrznym.

monitorowana terminowość i dokładność uzgodnień sald bankowych, personel prawdopodobnie przestanie je sporządzać.

12. Kontrole związane z procesem monitorowania systemu kontroli wewnętrznej jednostki, w tym te, które monitorują podstawowe kontrole automatyczne, mogą być zautomatyzowane lub ręczne, lub też mogą stanowić połączenie obu tych metod. Na przykład, jednostka może korzystać ze zautomatyzowanych kontroli monitorujących dostęp do pewnych technologii łącznie ze zautomatyzowanymi raportami nietypowych działań dla kierownictwa, które ręcznie bada zidentyfikowane anomalie.
13. Podczas dokonywania rozróżnienia pomiędzy czynnością monitorowania i kontrolą związaną z systemem informacyjnym rozważa się podstawowe szczegóły tej czynności, zwłaszcza gdy działalność ta wiąże się z pewnym poziomem przeglądu nadzorczego. Przeglądy nadzorcze nie są automatycznie klasyfikowane jako czynności monitorowania i może być kwestią osądu, czy przegląd jest klasyfikowany jako kontrola związana z systemem informacyjnym, czy jako czynność monitorowania. Na przykład celem miesięcznej kontroli kompletności byłoby wykrywanie i korygowanie błędów, gdy w ramach czynności monitorowania pytano by, dlaczego występują błędy i przypisałyby kierownictwu odpowiedzialność za naprawę procesu, aby zapobiec przyszłym błędom. Mówiąc prościej, kontrola związana z systemem informacyjnym odpowiada na konkretne ryzyko, podczas gdy czynność monitorowania ocenia, czy kontrole wewnątrz każdego z pięciu elementów systemu kontroli wewnętrznej jednostki działają zgodnie z założeniami.
14. Czynności monitorowania mogą obejmować wykorzystanie informacji pochodzących z komunikacji ze stronami zewnętrznymi, które mogą wskazywać problemy lub podkreślać obszary wymagające poprawy. Klienci domyślnie potwierdzają dane rozliczeniowe, płacąc swoje faktury lub składając reklamacje dotyczące swoich opłat. Ponadto regulatorzy mogą komunikować się z jednostką odnośnie do spraw, które wpływają na funkcjonowanie systemu kontroli wewnętrznej jednostki, na przykład komunikacja dotycząca badań przeprowadzanych przez bankowe organy regulacyjne. Kierownictwo może również rozważyć w ramach wykonywania czynności monitorowania wszelkie komunikacje dotyczące systemu kontroli wewnętrznej jednostki pochodzące od audytorów zewnętrznych.

System informacyjny i komunikacja

15. System informacyjny stosowny dla sporządzania sprawozdań finansowych składa się z czynności i polityk oraz dokumentacji księgowej i pomocniczej, zaprojektowanych i utworzonych, aby:
 - inicjować, rejestrować i przetwarzać transakcje jednostki (jak również ujmować, przetwarzać i ujawniać informacje o zdarzeniach i warunkach innych niż transakcje) oraz zachować rozliczalność za powiązane aktywa, zobowiązania i kapitał własny,
 - rozwiązać nieprawidłowe przetwarzanie transakcji, na przykład automatyczne pliki zawieszonych i procedury stosowane, aby terminowo wyjaśniać zawieszone pozycje,
 - przetwarzać i rozliczać obojętne systemu lub ominięcia kontroli,
 - włączyć informacje pochodzące z przetwarzania transakcji do księgi głównej (np. przeniesienie skumulowanych transakcji z księgi pomocniczej),

- ujmować i przetwarzać informacje stosowne dla sporządzenia sprawozdania finansowego w odniesieniu do zdarzeń i warunków innych niż transakcje, takich jak amortyzacja aktywów i zmiany w odzyskiwalności aktywów, oraz
 - zapewnić, że informacje, których ujawnienie jest wymagane przez mające zastosowanie ramowe założenia sprawozdawczości finansowej są gromadzone, rejestrowane, przetwarzane, sumowane i odpowiednio raportowane w sprawozdaniu finansowym.
16. Procesy biznesowe jednostki obejmują działania zaprojektowane, aby:
- opracować, nabyć, wyprodukować, sprzedać i rozdystrybuować produkty i usługi jednostki,
 - zapewnić zgodność z przepisami prawa i regulacjami oraz
 - zarejestrować informacje, w tym informacje księgowe i związane ze sprawozdawczością finansową.
- Procesy biznesowe skutkują transakcjami, które są rejestrowane, przetwarzane i raportowane przez system informacyjny.
17. Jakość informacji wpływa na zdolność kierownictwa do podejmowania właściwych decyzji podczas zarządzania i kontrolowania działalności jednostki oraz sporządzania wiarygodnych raportów finansowych.
18. Komunikacja, która obejmuje zapewnienie zrozumienia ról i odpowiedzialności poszczególnych osób, typowych dla systemu kontroli wewnętrznej jednostki, może przybrać takie formy, jak podręczniki polityk, podręczniki rachunkowości i sprawozdawczości finansowej i memoranda. Komunikacja może także odbywać się elektronicznie, ustnie lub poprzez działania kierownictwa.
19. Komunikowanie przez jednostkę ról i odpowiedzialności w zakresie sprawozdawczości finansowej oraz znaczących spraw związanych ze sprawozdawczością finansową obejmuje zapewnienie zrozumienia ról i obowiązków poszczególnych osób, typowych dla systemu kontroli wewnętrznej jednostki, stosownych dla sprawozdawczości finansowej. Może to obejmować takie sprawy, jak zakres, w którym personel rozumie, w jaki sposób jego działania w systemie informacyjnym wiążą się z pracą innych osób oraz sposoby zgłaszania wyjątków do odpowiednio wyższego poziomu w jednostce.

Czynności kontrolne

20. Kontrole w elemencie czynności kontrolnych są identyfikowane zgodnie z paragrafem 26. Kontrole takie obejmują kontrole przetwarzania informacji oraz ogólne kontrole IT, z których obie mogą mieć charakter ręczny lub automatyczny. Im większy jest zakres kontroli automatycznych lub kontroli obejmujących zautomatyzowane aspekty, które kierownictwo wykorzystuje i na których polega w odniesieniu do swojej sprawozdawczości finansowej, tym ważniejsze może stać się dla jednostki wdrożenie ogólnych kontroli IT odnoszących się do ciągłego funkcjonowania zautomatyzowanych aspektów kontroli przetwarzania informacji. Kontrole w elemencie czynności kontrolnych mogą dotyczyć następujących aspektów:
- *Autoryzacja i zatwierdzenia.* Autoryzacja potwierdza, że transakcja jest ważna (tj. stanowi rzeczywiste zdarzenie gospodarcze lub mieści się w granicach polityki jednostki). Autoryzacja przybiera zazwyczaj formę zatwierdzenia przez kierownictwo wyższego szczebla lub weryfikacji i ustalenia, czy transakcja jest ważna. Na przykład, osoba nadzorująca zatwierdza sprawozdanie z wydatków po dokonaniu przeglądu, czy wydatki wydają się uzasadnione i mieszczą się w granicach polityki. Przykładem zautomatyzowanego zatwierdzenia jest sytuacja, gdy fakturowany koszt jednostkowy jest automatycznie porównywany z powiązaniem kosztem jednostkowym w zamówieniu na

zakup w ramach ustalonego wcześniej poziomu tolerancji. Faktury mieszczące się w przedziale tolerancji są automatycznie zatwierdzane do zapłaty. Faktury wykraczające poza poziom tolerancji są oznaczane w celu przeprowadzenia dodatkowego dochodzenia.

- *Uzgodnienia* – Uzgodnienia porównują dwa lub więcej elementów danych. Jeżeli zostaną zidentyfikowane różnice, podejmuje się działania, aby doprowadzić do uzgodnienia danych. Uzgodnienia zazwyczaj dotyczą kompletności lub dokładności przetwarzania transakcji.
- *Weryfikacje* – Weryfikacje porównują dwie lub więcej pozycji ze sobą lub porównują pozycję z polityką i prawdopodobnie będą obejmować działania następcze, gdy te dwie pozycje nie pasują do siebie lub pozycja nie jest spójna z polityką. Weryfikacje zasadniczo odnoszą się do kompletności, dokładności lub ważności przetwarzania transakcji.
- *Kontrole fizyczne lub logiczne, w tym te, które odnoszą się do zabezpieczenia aktywów przed nieuprawnionym dostępem, nabyciem, wykorzystaniem lub zbyciem.* Kontrole, które obejmują:
 - fizyczne bezpieczeństwo aktywów, w tym adekwatne zabezpieczenia, takie jak infrastruktura zabezpieczająca dostęp do aktywów i zapisów,
 - zezwolenie na dostęp do programów komputerowych i plików danych (tj. dostęp logiczny),
 - okresowe przeliczanie i porównywanie z kwotami wykazanymi w dokumentacji kontrolnej (na przykład, porównywanie wyników spisów z natury gotówki, papierów wartościowych i zapasów z dokumentacją księgową).

Zakres, w jakim kontrole fizyczne, mające na celu zapobiegać kradzieży aktywów, są stosowne do wiarygodności sporządzania sprawozdania finansowego zależy od takich okoliczności, jak wtedy, gdy aktywa są wysoce podatne na przywłaszczenie.

- *Podział obowiązków* – Przypisanie różnym osobom obowiązków w zakresie autoryzacji transakcji, rejestrowania transakcji i utrzymywania pieczy nad aktywami. Podział obowiązków ma na celu ograniczenie sposobności umożliwiającej jakiegokolwiek osobie znalezienie się w takiej roli, aby jednocześnie popełniła i ukryła błędy lub oszustwo w toku normalnego wykonywania przez nią obowiązków.

Na przykład, kierownik zatwierdzający sprzedaż kredytową nie jest odpowiedzialny za prowadzenie ewidencji należności lub obsługę przyjęć gotówki. Jeżeli jedna osoba jest w stanie wykonać wszystkie te czynności, osoba ta mogłaby na przykład stworzyć fikcyjną sprzedaż, która mogłaby nie zostać wykryta. Podobnie, sprzedawcy nie powinni mieć możliwości modyfikować plików z cenami produktów lub stawek prowizji.

Czasami podział nie jest praktyczny, opłacalny lub wykonalny. Na przykład mniejsze i mniej złożone jednostki mogą nie dysponować wystarczającymi zasobami, aby osiągnąć idealny podział, a koszty zatrudnienia dodatkowych pracowników mogą być zaporowe. W takich sytuacjach kierownictwo może wprowadzić kontrole alternatywne. W powyższym przykładzie, jeżeli sprzedawca może modyfikować pliki z cenami produktów, można wprowadzić kontrolę wykrywającą, aby personel niezwiązany z funkcją sprzedaży okresowo dokonywał przeglądu, czy i w jakich okolicznościach sprzedawca zmienił ceny.

21. Pewne kontrole mogą zależeć od istnienia odpowiednich kontroli nadzorczych ustanowionych przez kierownictwo lub osoby sprawujące nadzór. Na przykład kontrole autoryzacyjne mogą być delegowane na podstawie ustalonych wytycznych, takich jak kryteria inwestycyjne określone

przez osoby sprawujące nadzór; alternatywnie, niestandardowe transakcje, takie jak duże nabycia lub zbycia, mogą wymagać szczególnej zgody na wysokim poziomie, w tym w niektórych przypadkach zgody udziałowców lub akcjonariuszy.

Ograniczenia kontroli wewnętrznej

22. System kontroli wewnętrznej jednostki, niezależnie od tego, jak skuteczny, może jednostce dostarczyć jedynie racjonalną pewność dotyczącą osiągnięcia celów sprawozdawczości finansowej jednostki. Na prawdopodobieństwo ich osiągnięcia wpływają nieodłączne ograniczenia kontroli wewnętrznej. Obejmują one realia, że ludzki osąd w podejmowaniu decyzji może być błędny oraz że mogą wystąpić awarie w systemie kontroli wewnętrznej jednostki z powodu błędu ludzkiego. Na przykład, może wystąpić błąd w projekcie lub w zmianie kontroli. Podobnie, działanie kontroli może nie być skuteczne, tak jak w sytuacji, gdy informacje tworzone na potrzeby systemu kontroli wewnętrznej jednostki (na przykład raport odstępstw) nie są skutecznie wykorzystywane, gdyż osoba odpowiedzialna za przegląd informacji nie rozumie ich celu lub nie podejmuje odpowiednich działań.
23. Ponadto, kontrole można obejść poprzez zмовę dwóch lub większej liczby osób lub poprzez niewłaściwe obejście kontroli przez kierownictwo. Na przykład, kierownictwo może zawrzeć z klientami poboczne umowy, które zmieniają postanowienia i warunki standardowych umów sprzedaży jednostki, co może skutkować niewłaściwym ujmowaniem przychodów. Możliwe jest także obejście lub wyłączenie mechanizmów sprawdzających zawartych w aplikacji IT, które są zaprojektowane, aby identyfikować i raportować transakcje przekraczające określone limity kredytowe.
24. Ponadto kierownictwo, projektując i wdrażając kontrole, może dokonać osądu co do rodzaju i zakresu kontroli, które zdecydowało się wdrożyć oraz rodzaju i zakresu ryzyk, które zdecydowało się podjąć.

Załącznik 4

(Zob. par. 14(a), 24(a)(ii), A25–A28, A118)

Rozważania dotyczące zrozumienia funkcji audytu wewnętrznego jednostki

Niniejszy załącznik zawiera dalsze rozważania dotyczące zrozumienia funkcji audytu wewnętrznego jednostki, gdy taka funkcja istnieje.

Cele i zakres funkcji audytu wewnętrznego

1. Cele i zakres funkcji audytu wewnętrznego, charakter jej obowiązków oraz jej status wewnątrz organizacji, w tym uprawnienia i odpowiedzialność tej funkcji, różnią się znacząco i zależą od wielkości, złożoności i struktury jednostki oraz od wymogów kierownictwa i gdy ma to zastosowanie, osób sprawujących nadzór. Sprawy te mogą być ustalone w karcie audytu wewnętrznego lub zakresie zadań.
2. Obowiązki funkcji audytu wewnętrznego mogą obejmować wykonywanie procedur i dokonywanie oceny wyników, aby dostarczać kierownictwu i osobom sprawującym nadzór zapewnienia dotyczącego zaprojektowania i skuteczności zarządzania ryzykiem, systemu kontroli wewnętrznej jednostki i procesów nadzoru. Jeżeli tak jest, to funkcja audytu wewnętrznego może odgrywać ważną rolę w procesie monitorowania systemu kontroli wewnętrznej w jednostce. Jednak obowiązki funkcji audytu wewnętrznego mogą być skoncentrowane na ocenie gospodarności, efektywności i skuteczności działań, i jeżeli tak jest, praca tej funkcji może nie mieć bezpośredniego związku ze sprawozdawczością finansową jednostki.

Zapytania kierowane do funkcji audytu wewnętrznego

3. Jeżeli jednostka posiada funkcję audytu wewnętrznego, zapytania do odpowiednich osób w ramach tej funkcji mogą dostarczyć informacji przydatnych dla audytora podczas uzyskiwania zrozumienia jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej i systemu kontroli wewnętrznej jednostki, a także podczas identyfikowania i oszacowania ryzyk istotnego zniekształcenia na poziomie sprawozdania finansowego i na poziomie stwierdzeń. Podczas wykonywania swojej pracy, funkcja audytu wewnętrznego prawdopodobnie uzyskuje wgląd w działalność jednostki oraz ryzyka gospodarcze i może dysponować ustaleniami opartymi na swojej pracy, takimi jak zidentyfikowane słabości kontroli lub ryzyka, które mogą zapewnić wartościowy wkład w zrozumienie przez audytora jednostki i jej otoczenia, mających zastosowanie ramowych założeń sprawozdawczości finansowej, systemu kontroli wewnętrznej jednostki, w dokonanie przez audytora oszacowania ryzyka lub w inne aspekty badania. Zapytania audytora są w związku z tym kierowane bez względu na to, czy audytor zamierza, czy nie, wykorzystać pracę funkcji audytu wewnętrznego, aby zmienić rodzaj lub rozłożenie w czasie albo ograniczyć zakres procedur badania do wykonania¹. Szczególnie stosowne zapytania mogą dotyczyć spraw, które funkcja audytu wewnętrznego podnosiła w rozmowach z osobami sprawującymi nadzór oraz wyników procesu oszacowania ryzyka dokonanego przez tę funkcję.
4. Jeżeli na podstawie odpowiedzi na zapytania audytora okaże się, że istnieją ustalenia, które mogą być stosowne dla sprawozdawczości finansowej jednostki oraz badania sprawozdania finansowego, audytor może uznać, że właściwym będzie przeczytanie związanych z nimi raportów funkcji audytu wewnętrznego. Przykłady raportów funkcji audytu wewnętrznego, które

¹ Stosowne wymogi są zawarte w MSB 610 (zmienionym w 2013 r.).

mogą być stosowne, obejmują dokumenty dotyczące strategii i planowania tej funkcji oraz raporty, które zostały sporządzone dla kierownictwa lub osób sprawujących nadzór opisujące ustalenia funkcji audytu wewnętrznego dokonane w trakcie sprawdzania.

5. Dodatkowo, zgodnie z MSB 240², jeżeli funkcja audytu wewnętrznego dostarcza audytorowi informacje dotyczące jakichkolwiek rzeczywistych, podejrzewanych lub zarzucanych oszustw, audytor bierze to pod uwagę podczas identyfikacji przez audytora ryzyka istotnego zniekształcenia spowodowanego oszustwem.
6. Odpowiednimi osobami z funkcji audytu wewnętrznego, do których kierowane są zapytania, są te osoby, które zgodnie z osądem audytora, mają odpowiednią wiedzę, doświadczenie oraz uprawnienia, takie jak kierownik zarządzający audytem wewnętrznym lub, zależnie od okoliczności, inni pracownicy tej funkcji. Audytor może także uznać za właściwe, aby odbywać okresowe spotkania z tymi osobami.

Rozważenie funkcji audytu wewnętrznego w zrozumieniu środowiska kontroli

7. W ramach zrozumienia środowiska kontroli, audytor może rozważyć, w jaki sposób kierownictwo zareagowało na ustalenia i rekomendacje funkcji audytu wewnętrznego, dotyczące zidentyfikowanych słabości kontroli stosownych dla sporządzenia sprawozdania finansowego, w tym czy i w jaki sposób takie reakcje zostały wdrożone oraz czy zostały one następnie ocenione przez funkcję audytu wewnętrznego.

Zrozumienie roli, jaką funkcja audytu wewnętrznego pełni w procesie monitorowania systemu kontroli wewnętrznej jednostki

8. Jeżeli charakter obowiązków i działań atestacyjnych funkcji audytu wewnętrznego są związane ze sprawozdawczością finansową jednostki, audytor może być także w stanie wykorzystać pracę funkcji audytu wewnętrznego, aby zmienić rodzaj lub rozłożenie w czasie, lub ograniczyć zakres, procedur badania, które mają zostać wykonane bezpośrednio przez audytora podczas uzyskiwania dowodów badania. Bardziej prawdopodobne jest, że audytorzy będą w stanie wykorzystać pracę funkcji audytu wewnętrznego jednostki, gdy okaże się, na przykład, na podstawie doświadczenia z poprzednich badań lub procedur oszacowania ryzyka przez audytora, że jednostka posiada funkcję audytu wewnętrznego, która jest wyposażona w adekwatne i odpowiednie zasoby do złożoności jednostki i rodzaju jej działalności, a także jej sprawozdawczość ma bezpośredni związek z osobami sprawującymi nadzór.
9. Jeżeli, na podstawie wstępnego zrozumienia przez audytora funkcji audytu wewnętrznego, audytor przewiduje wykorzystanie pracy funkcji audytu wewnętrznego, aby zmienić rodzaj lub rozłożenie w czasie lub ograniczyć zakres procedur badania do wykonania, stosuje się MSB 610 (zmieniony w 2013 roku).
10. Jak dodatkowo omówiono w MSB 610 (zmienionym w 2013 roku), działania funkcji audytu wewnętrznego są odrębne od innych kontroli monitorujących, które mogą być stosowne dla sprawozdawczości finansowej, takich jak przeglądy informacji rachunkowości zarządczej, które zostały zaprojektowane, aby przyczyniać się do zapobiegania lub wykrywania zniekształceń w jednostce.
11. Ustalenie, na początku wykonywania zlecenia, komunikacji z odpowiednimi osobami z funkcji audytu wewnętrznego jednostki oraz prowadzenie takiej komunikacji podczas zlecenia, może ułatwiać skuteczną wymianę informacji. Stwarza to środowisko, w którym audytor może zostać poinformowany o znaczących sprawach, które mogą zwrócić uwagę funkcji audytu

² MSB 240, paragraf 19.

wewnętrznego, gdy takie sprawy mogą wpływać na pracę audytora. MSB (PL) 200 przedstawia znaczenie planowania i wykonywania przez audytora badania z zawodowym sceptycyzmem³, w tym wyczulenia na informacje kwestionujące wiarygodność dokumentów i odpowiedzi na zapytania, które mają być użyte jako dowody badania. W związku z tym, komunikacja z funkcją audytu wewnętrznego podczas zlecenia może dać audytorom wewnętrznym szansę na zwrócenie uwagi audytora na takie informacje. Audytor jest więc w stanie wziąć pod uwagę takie informacje podczas identyfikacji i oszacowania ryzyk istotnego zniekształcenia.

³ MSB (PL) 200, paragraf 7.

Załącznik 5

(Zob. par. 25(a), 26(b)–(c), A94, A166–A172)

Rozważania dotyczące zrozumienia technologii informacyjnych (IT)

W niniejszym załączniku przedstawiono dalsze zagadnienia, które audytor może rozważyć uzyskując zrozumienie wykorzystania IT przez jednostkę w jej systemie kontroli wewnętrznej.

Zrozumienie wykorzystania technologii informacyjnych przez jednostkę w elementach systemu kontroli wewnętrznej jednostki

1. System kontroli wewnętrznej jednostki obejmuje elementy ręczne i automatyczne. (tj. kontrole ręczne i automatyczne oraz inne zasoby wykorzystywane w systemie kontroli wewnętrznej jednostki). Połączenie elementów ręcznych i automatycznych jednostki różni się w zależności od charakteru i złożoności wykorzystania IT przez jednostkę. Wykorzystanie IT przez jednostkę wpływa na sposób, w jaki informacje stosowne dla sporządzenia sprawozdania finansowego zgodnie z mającymi zastosowanie ramowymi założeniami sprawozdawczości finansowej są przetwarzane, przechowywane i komunikowane, a tym samym wpływa na sposób, w jaki system kontroli wewnętrznej w jednostce jest zaprojektowany i wdrożony. Każdy element systemu kontroli wewnętrznej w jednostce może wykorzystywać w pewnym zakresie IT.

Zazwyczaj, IT przynoszą korzyści dla systemu kontroli wewnętrznej jednostki poprzez umożliwienie jednostce:

- spójnego stosowania określonych z góry zasad biznesowych oraz wykonywania złożonych kalkulacji podczas przetwarzania dużych wolumenów transakcji lub danych,
 - poprawy terminowości, dostępności i dokładności informacji,
 - ułatwienia dodatkowych analiz informacji,
 - ulepszenia zdolności monitorowania wykonywania działalności jednostki oraz jej polityk i procedur,
 - zmniejszenia ryzyka obejścia kontroli oraz
 - ulepszenia możliwości osiągnięcia skutecznego podziału obowiązków poprzez wprowadzenie kontroli bezpieczeństwa w aplikacjach IT, bazach danych i systemach operacyjnych.
2. Cechy elementów ręcznych lub automatycznych są stosowne dla identyfikacji i oszacowania przez audytora ryzyk istotnego zniekształcenia oraz dla dalszych procedur badania opartych na tym oszacowaniu. Kontrole automatyczne mogą być bardziej wiarygodne niż kontrole ręczne, ponieważ nie można ich tak łatwo ominąć, zignorować lub obejść oraz są one także mniej podatne na proste błędy i pomyłki. Kontrole automatyczne mogą być bardziej skuteczne niż kontrole ręczne w następujących okolicznościach:
 - wysoki wolumen powtarzających się transakcji lub w sytuacjach, gdy błędów, które można przewidzieć lub ich oczekiwać, można zapobiegać lub wykrywać je i korygować poprzez automatyzację,
 - kontrole, gdy szczególne sposoby wykonywania kontroli mogą być adekwatnie zaprojektowane i zautomatyzowane.

Zrozumienie wykorzystania przez jednostkę technologii informacyjnych w systemie informacyjnym (Zob. par. 25(a))

3. System informacyjny jednostki może obejmować wykorzystanie ręcznych i automatycznych elementów, które wpływają także na sposób, w jaki transakcje są inicjowane, rejestrowane, przetwarzane i raportowane. W szczególności, procedury inicjowania, rejestrowania, przetwarzania i raportowania transakcji mogą być egzekwowane poprzez aplikacje IT wykorzystywane przez jednostkę oraz sposób, w jaki jednostka skonfigurowała te aplikacje. Ponadto rejestry w formie informacji cyfrowych mogą zastąpić lub uzupełnić rejestry w formie dokumentów papierowych.
4. Uzyskując zrozumienie środowiska IT stosownego dla przepływu transakcji i przetwarzania informacji w systemie informacyjnym, audytor gromadzi informacje o charakterze i cechach wykorzystywanych aplikacji IT, a także o pomocniczej infrastrukturze IT i IT. Poniższa tabela zawiera przykłady kwestii, które audytor może rozważyć uzyskując zrozumienie środowiska IT i zawiera przykłady typowych cech środowisk IT opartych na złożoności aplikacji IT wykorzystywanych w systemie informacyjnym jednostki. Jednakże takie cechy są orientacyjne i mogą się różnić w zależności od charakteru konkretnych aplikacji IT wykorzystywanych przez jednostkę.

	Przykłady typowych cech:		
	Niezłożonego oprogramowania komercyjnego	Średniej wielkości i umiarkowanie złożonego oprogramowania komercyjnego lub aplikacji IT	Dużych lub złożonych aplikacji IT (np. systemów ERP)
Zagadnienia związane z zakresem automatyzacji i wykorzystaniem danych:			
Zakres automatycznych procedur przetwarzania i złożoność tych procedur, w tym, czy istnieje wysoce zautomatyzowane przetwarzanie bez użycia formy papierowej.	Nie dotyczy	Nie dotyczy	Rozbudowane i często złożone procedury automatyczne
Zakres polegania przez jednostkę na raportach generowanych przez system podczas przetwarzania informacji.	Prosta zautomatyzowana logika raportowania	Prosta stosowna zautomatyzowana logika raportowania	Złożona zautomatyzowana logika raportowania; oprogramowanie do tworzenia raportów
Sposób wprowadzania danych (tj. wprowadzanie ręczne, wprowadzanie przez klienta lub	Ręczne wprowadzanie danych	Niewielka liczba wprowadzanych danych lub proste interfejsy	Duża liczba wprowadzanych danych lub złożone interfejsy

	Przykłady typowych cech:		
	Niezłożonego oprogramowania komercyjnego	Średniej wielkości i umiarkowanie złożonego oprogramowania komercyjnego lub aplikacji IT	Dużych lub złożonych aplikacji IT (np. systemów ERP)
dostawcę, lub wczytywanie plików).			
W jaki sposób IT ułatwia komunikację pomiędzy aplikacjami, bazami danych lub innymi aspektami środowiska IT, wewnątrz i zewnątrz, jeżeli jest to właściwe, poprzez interfejsy systemowe.	Brak automatycznych interfejsów (tylko ręczne wprowadzanie)	Niewielka liczba wprowadzanych danych lub proste interfejsy	Duża liczba wprowadzanych danych lub złożone interfejsy
Wolumen i złożoność danych w formie cyfrowej przetwarzanych przez system informacyjny, w tym, czy dokumentacja księgowa lub inne informacje są przechowywane w formie cyfrowej oraz lokalizacja przechowywanych danych.	Niewielki wolumen danych lub proste dane, które mogą być zweryfikowane ręcznie; dane dostępne lokalnie	Niewielki wolumen danych lub proste dane	Duży wolumen danych lub dane złożone; hurtownie danych ¹ ; korzystanie z wewnętrznych lub zewnętrznych dostawców usług IT (np. przechowywanie lub hosting danych przez strony trzecie)
Zagadnienia związane z aplikacjami IT i infrastrukturą IT:			
Rodzaj aplikacji (np. aplikacja komercyjna z niewielkim dostosowaniem lub bez dostosowania lub aplikacja wysoce dostosowana lub wysoce zintegrowana, która mogła zostać zakupiona	Zakupiona aplikacja z niewielkim dostosowaniem lub bez dostosowania	Zakupiona aplikacja lub prosta starsza aplikacja lub niskiej klasy aplikacje ERP z niewielkim dostosowaniem lub bez dostosowania	Opracowane dostosowane aplikacje lub bardziej złożone systemy ERP ze znaczącym dostosowaniem

¹ Hurtownia danych jest zazwyczaj opisywana jako centralne repozytorium zintegrowanych danych z jednego lub wielu różnych źródeł (takich jak wiele baz danych), z których mogą być generowane raporty lub które mogą być wykorzystywane przez jednostkę do innych działań związanych z analizą danych. Program do sporządzania raportów to aplikacja IT, która jest wykorzystywana do pobierania danych z jednego lub kilku źródeł (takich jak hurtownia danych, baza danych lub aplikacja IT) i prezentowania danych w konkretnym formacie.

	Przykłady typowych cech:		
	Nie złożonego oprogramowania komercyjnego	Średniej wielkości i umiarkowanie złożonego oprogramowania komercyjnego lub aplikacji IT	Dużych lub złożonych aplikacji IT (np. systemów ERP)
i dostosowana lub opracowana we własnym zakresie).			
Złożoność charakteru aplikacji IT i podstawowej infrastruktury IT.	Małe, proste rozwiązanie oparte na laptopie lub serwerze klienta	Rozwinięty i stabilny komputer typu mainframe, mały lub prosty serwer klienta, oprogramowanie jako usługa w chmurze	Złożony komputer typu mainframe, duży lub złożony serwer klienta, podłączony do sieci, infrastruktura jako usługa w chmurze
Czy występuje hosting świadczony przez stronę trzecią lub outsourcing IT.	W przypadku outsourcingu, kompetentny, dojrzały, sprawdzony dostawca (np. dostawca chmury)	W przypadku outsourcingu, kompetentny, dojrzały, sprawdzony dostawca (np. dostawca chmury)	Kompetentny, dojrzały, sprawdzony dostawca dla pewnych aplikacji oraz nowy lub początkujący dostawca dla innych
Czy jednostka korzysta ze wschodzących technologii, które mają wpływ na jej sprawozdawczość finansową.	Brak wykorzystania wschodzących technologii	Ograniczone wykorzystanie wschodzących technologii w niektórych aplikacjach	Mieszane wykorzystanie wschodzących technologii na różnych platformach
Zagadnienia związane z procesami IT:			
Personel zaangażowany w utrzymanie środowiska IT (liczba i poziom umiejętności zasobów wsparcia IT, które zarządzają bezpieczeństwem i zmianami w środowisku IT).	Niewielu pracowników o ograniczonej wiedzy IT, aby przetwarzać aktualizacje dostawcy i zarządzać dostępem	Ograniczony personel z umiejętnościami IT / przeznaczony do IT	Przeznaczone działy IT z wykwalifikowanym personelem, w tym z umiejętnościami programowania
Złożoność procesów zarządzania prawami dostępu.	Pojedyncza osoba z dostępem administracyjnym zarządza prawami dostępu	Kilka osób z dostępem administracyjnym zarządza prawami dostępu	Złożone procesy zarządzane przez dział IT w zakresie praw dostępu

	Przykłady typowych cech:		
	Niezłożonego oprogramowania komercyjnego	Średniej wielkości i umiarkowanie złożonego oprogramowania komercyjnego lub aplikacji IT	Dużych lub złożonych aplikacji IT (np. systemów ERP)
Złożoność bezpieczeństwa w środowisku IT, w tym podatność aplikacji IT, baz danych i innych aspektów środowiska IT na ryzyka cybernetyczne, w szczególności w przypadku występowania transakcji internetowych lub transakcji z wykorzystaniem zewnętrznych interfejsów.	Prosty dostęp na miejscu, bez zewnętrznych elementów sieciowych	Niektóre aplikacje internetowe o przede wszystkim prostych zabezpieczeniach, opartych na rolach	Wiele platform z dostępem sieciowym i złożonymi modelami zabezpieczeń
Czy dokonano zmian w programie w sposobie przetwarzania informacji i zakres takich zmian w badanym okresie.	Oprogramowanie komercyjne bez zainstalowanego kodu źródłowego	Niektóre aplikacje komercyjne bez kodu źródłowego i inne dojrzałe aplikacje z niewielką liczbą zmian lub z prostymi zmianami; tradycyjny cykl życia rozwoju systemów	Nowe zmiany lub duża liczba zmian lub złożone zmiany, kilka cykli rozwojowych każdego roku
Zakres zmian w środowisku IT (np. nowe aspekty środowiska IT lub znaczące zmiany w aplikacjach IT lub w podstawowej infrastrukturze IT).	Zmiany ograniczone do aktualizacji wersji oprogramowania komercyjnego	Zmiany składają się z aktualizacji oprogramowania komercyjnego, aktualizacji wersji ERP lub ulepszeń starszych aplikacji	Nowe zmiany lub duża liczba zmian lub złożone zmiany, kilka cykli rozwojowych każdego roku, obszerne dostosowanie ERP
Czy miała miejsce duża konwersja danych w danym okresie, a jeżeli tak, charakter i znaczenie dokonanych zmian oraz w jaki sposób dokonano konwersji.	Aktualizacje oprogramowania dostarczane przez dostawcę; brak cech konwersji danych do aktualizacji	Drobne aktualizacje wersji dla aplikacji oprogramowania komercyjnego z ograniczonymi konwertowanymi danymi	Duża aktualizacja wersji, nowe wydanie, zmiana platformy

Wschodzące technologie

5. Jednostki mogą wykorzystywać wschodzące technologie (np. łańcuch blokowy, robotyka lub sztuczna inteligencja), ponieważ takie technologie mogą stwarzać konkretne możliwości zwiększenia efektywności operacyjnych lub poprawy sprawozdawczości finansowej. Gdy w systemie informacyjnym jednostki wykorzystywane są wschodzące technologie stosowne dla sporządzania sprawozdań finansowych, audytor może włączyć takie technologie do identyfikacji aplikacji IT i innych aspektów środowiska IT, które podlegają ryzykom powstającym na skutek wykorzystania IT. O ile wschodzące technologie mogą być postrzegane jako bardziej skomplikowane lub bardziej złożone w porównaniu z istniejącymi technologiami, obowiązki audytora w odniesieniu do aplikacji IT i ogólne kontrole IT zidentyfikowane zgodnie z paragrafem 26(b)-(c) pozostają niezmienione.

Skalowalność

6. Uzyskanie zrozumienia środowiska IT jednostki może być łatwiejsze do osiągnięcia w przypadku mniej złożonej jednostki, która korzysta z oprogramowania komercyjnego oraz gdy jednostka nie ma dostępu do kodu źródłowego, aby dokonać jakichkolwiek zmian w programie. Jednostki takie mogą nie posiadać dedykowanych zasobów IT, ale mogą posiadać osobę wyznaczoną do pełnienia roli administratora w celu przyznawania pracownikom dostępu lub instalowania dostarczanych przez dostawcę aktualizacji aplikacji IT. Szczególne zagadnienia, które audytor może rozważyć uzyskując zrozumienie charakteru pakietu komercyjnego oprogramowania księgowego, którym może być pojedyncza aplikacja IT wykorzystywana przez mniej złożoną jednostkę w jej systemie informacyjnym, mogą obejmować:
- zakres, w jakim oprogramowanie jest dobrze ugruntowane i ma reputację za wiarygodność,
 - zakres, w jakim jednostka może modyfikować kod źródłowy oprogramowania, aby włączyć dodatkowe moduły (tj. dodatki) do oprogramowania bazowego lub dokonywać bezpośrednich zmian w danych,
 - charakter i zakres modyfikacji, które zostały wprowadzone do oprogramowania. Chociaż jednostka może nie być w stanie zmodyfikować kodu źródłowego oprogramowania, wiele pakietów oprogramowania pozwala na jego konfigurację (np. ustawienie lub zmianę parametrów raportowania). Zazwyczaj nie wiąże się to z modyfikacjami kodu źródłowego, jednakże audytor może rozważyć zakres, w jakim jednostka jest w stanie skonfigurować oprogramowanie podczas rozważania kompletności i dokładności informacji wytworzonych przez oprogramowanie, które są wykorzystywane jako dowody badania, oraz
 - zakres, w jakim można uzyskać bezpośredni dostęp do danych związanych ze sporządzeniem sprawozdania finansowego (tj. bezpośredni dostęp do bazy danych bez użycia aplikacji IT) oraz wolumen przetwarzanych danych. Im większy jest wolumen danych, tym bardziej prawdopodobne jest, że jednostka może potrzebować kontroli, które odnoszą się do zachowania integralności danych, co może obejmować ogólne kontrole IT dotyczące nieuprawnionego dostępu i zmian w danych.
7. Złożone środowiska IT mogą zawierać wysoce dostosowane lub wysoce zintegrowane aplikacje IT i dlatego ich zrozumienie może wymagać większego wysiłku. Procesy sprawozdawczości finansowej lub aplikacje IT mogą być zintegrowane z innymi aplikacjami IT. Integracja taka może obejmować aplikacje IT, które są wykorzystywane w działalności gospodarczej jednostki oraz które dostarczają informacje do aplikacji IT stosownych dla przepływów transakcji i przetwarzania informacji w systemie informacyjnym jednostki. W takich okolicznościach, pewne aplikacje IT wykorzystywane w działalności gospodarczej jednostki mogą być również

stosowne dla sporządzania sprawozdania finansowego. Złożone środowiska IT mogą również wymagać dedykowanych działów IT, które posiadają ustrukturyzowane procesy IT wspierane przez personel posiadający umiejętności w zakresie rozwoju oprogramowania i utrzymania środowiska IT. W innych przypadkach jednostka może wykorzystywać wewnętrznych lub zewnętrznych dostawców usług do zarządzania pewnymi aspektami swojego środowiska IT lub procesami IT w jego ramach (np. hosting przez stronę trzecią).

Identyfikowanie aplikacji IT, które podlegają ryzykom powstającym na skutek wykorzystania IT

8. Poprzez zrozumienie charakteru i złożoności środowiska IT jednostki, w tym charakteru i zakresu kontroli przetwarzania informacji, audytor może ustalić, na których aplikacjach IT jednostka polega, aby dokładnie przetwarzać i utrzymywać integralność informacji finansowych. Identyfikacja aplikacji IT, na których polega jednostka, może mieć wpływ na decyzję audytora o przetestowaniu automatycznych kontroli w ramach takich aplikacji IT, przy założeniu, że takie automatyczne kontrole odnoszą się do zidentyfikowanych ryzyk istotnego zniekształcenia. Odwrotnie, jeżeli jednostka nie polega na aplikacji IT, jest małe prawdopodobieństwo, aby kontrole automatyczne w ramach takiej aplikacji IT były odpowiednie lub wystarczająco dokładne dla celów testów skuteczności działania. Kontrole automatyczne, które mogą być zidentyfikowane zgodnie z paragrafem 26(b), mogą obejmować na przykład automatyczne obliczenia lub kontrole danych wejściowych, przetwarzania i danych wyjściowych, takie jak trójstronne dopasowanie zamówienia zakupu, dokumentu przewozowego sprzedawcy i faktury sprzedawcy. Gdy kontrole automatyczne zostały zidentyfikowane przez audytora i audytor ustala poprzez zrozumienie środowiska IT, że jednostka polega na aplikacji IT, która obejmuje te automatyczne kontrole, prawdopodobieństwo zidentyfikowania przez audytora aplikacji IT jako tej podlegającej ryzykom powstającym na skutek wykorzystania IT może być większe.
9. Rozważając, czy aplikacje IT, dla których audytor zidentyfikował automatyczne kontrole, podlegają ryzykom powstającym na skutek wykorzystania IT, audytor prawdopodobnie rozważy, czy i w jakim zakresie jednostka może mieć dostęp do kodu źródłowego, który umożliwia kierownictwu wprowadzenie zmian w programach do takich kontroli lub w aplikacjach IT. Stosowne rozważania mogą obejmować również zakres, w jakim jednostka dokonuje zmian w programach lub konfiguracji oraz zakres, w jakim procesy IT w związku z takimi zmianami są sformalizowane. Audytor prawdopodobnie rozważy również ryzyko niewłaściwego dostępu do danych lub ich zmiany.
10. Raporty generowane przez system, które audytor może zamierzać wykorzystać jako dowody badania, mogą obejmować na przykład raport wiekowania należności handlowych lub raport dotyczący wyceny zapasów. W przypadku takich raportów audytor może uzyskać dowody badania dotyczące kompletności i dokładności raportów poprzez testy wiarygodności danych wejściowych i wyjściowych zawartych w raporcie. W innych przypadkach audytor może zaplanować przetestowanie skuteczności działania kontroli w zakresie sporządzenia i utrzymania raportu i w takim przypadku aplikacja IT, z której raport został sporządzony, prawdopodobnie będzie podlegała ryzykom powstającym na skutek wykorzystania IT. Dodatkowo do testowania kompletności i dokładności raportu, audytor może zaplanować przetestowanie skuteczności działania ogólnych kontroli IT, które odnoszą się do ryzyk związanych z niewłaściwymi lub nieautoryzowanymi zmianami w programie lub zmianami danych w raporcie.
11. Niektóre aplikacje IT mogą zawierać w sobie funkcjonalności sporządzania sprawozdań, podczas gdy niektóre jednostki mogą również korzystać z odrębnych aplikacji do sporządzania sprawozdań (tj. programów do sporządzania sprawozdań). W takich przypadkach audytor może być zmuszony ustalić źródła raportów generowanych przez system (tj. aplikacji, która

- przygotowuje raport oraz źródeł danych wykorzystywanych przez raport) w celu określenia aplikacji IT podlegających ryzykom powstającym na skutek wykorzystania IT.
12. Źródłami danych wykorzystywanymi przez aplikacje IT mogą być bazy danych, do których na przykład dostęp może mieć tylko aplikacja IT lub personel IT posiadający uprawnienia do administrowania bazami danych. W innych przypadkach źródłem danych może być hurtownia danych, która sama w sobie może być uważana za aplikację IT podlegającą ryzykom powstającym na skutek wykorzystania IT.
 13. Audytor mógł zidentyfikować ryzyko, dla którego same procedury wiarygodności nie są wystarczające ze względu na wykorzystywanie przez jednostkę wysoce zautomatyzowanego i elektronicznego przetwarzania transakcji, które może obejmować wiele zintegrowanych aplikacji IT. W takich okolicznościach kontrole zidentyfikowane przez audytora będą prawdopodobnie obejmowały kontrole automatyczne. Ponadto, jednostka może polegać na ogólnych kontrolach IT, aby zachować integralność przetwarzanych transakcji oraz innych informacji wykorzystywanych do ich przetwarzania. W takich przypadkach aplikacje IT związane z przetwarzaniem i przechowywaniem informacji będą prawdopodobnie podlegały ryzykom powstającym na skutek wykorzystania IT.

Obliczenia dla użytkownika końcowego

14. Chociaż dowody badania mogą również mieć formę danych wyjściowych generowanych przez system, które są wykorzystywane w obliczeniach wykonywanych za pomocą narzędzia obliczeniowego dla użytkownika końcowego (np. oprogramowanie wykorzystujące arkusz kalkulacyjny lub proste bazy danych), narzędzia takie nie są zazwyczaj identyfikowane jako aplikacje IT w kontekście paragrafu 26(b). Projektowanie i wdrażanie kontroli w zakresie dostępu i zmian w narzędziach obliczeniowych dla użytkownika końcowego może stanowić wyzwanie i takie kontrole rzadko są równoważne lub równie skuteczne jak ogólne kontrole IT. Audytor może raczej rozważyć połączenie kontroli przetwarzania informacji, biorąc pod uwagę cel i złożoność obliczeń wykonywanych dla użytkownika końcowego, takich jak:
 - kontrole przetwarzania informacji dotyczące inicjowania i przetwarzania danych źródłowych, w tym stosowne kontrole automatyczne lub kontrole interfejsu do punktu, z którego dane są pobierane (tj. hurtowni danych),
 - kontrole mające na celu sprawdzenie, że logika funkcjonuje zgodnie z założeniami, na przykład kontrole, które są „dowodem” pozyskania danych, takie jak uzgodnienie raportu z danymi, z których został on utworzony, porównanie poszczególnych danych z raportu ze źródłem i odwrotnie oraz kontrole sprawdzające formuły lub makra, lub
 - wykorzystanie narzędzi oprogramowania do walidacji, które systematycznie sprawdzają formuły lub makra, takich jak narzędzia integralności arkusza kalkulacyjnego.

Skalowalność

15. Zdolność jednostki do utrzymania integralności informacji przechowywanych i przetwarzanych w systemie informacyjnym może różnić się w zależności od złożoności i wolumenu powiązanych transakcji oraz innych informacji. Im większa jest złożoność i wolumen danych, które wspierają znaczącą grupę transakcji, saldo konta lub ujawnienie, tym mniej prawdopodobne może się stać, że jednostka utrzyma integralność tych informacji wyłącznie poprzez kontrole przetwarzania informacji (np. kontrole danych wejściowych i wyjściowych lub kontrole przeglądowe). Staje się również mniej prawdopodobne, że audytor będzie w stanie uzyskać dowody badania dotyczące kompletności i dokładności takich informacji wyłącznie poprzez testy wiarygodności, gdy informacje takie są wykorzystywane jako dowody badania. W niektórych okolicznościach, gdy

wolumen i złożoność transakcji są mniejsze, kierownictwo może mieć kontrolę przetwarzania informacji, która jest wystarczająca, aby zweryfikować dokładność i kompletność danych (np. poszczególne przetwarzane i rozliczane zlecenia sprzedaży mogą być uzgadniane z kopią papierową pierwotnie wprowadzoną do aplikacji IT). Gdy jednostka polega na ogólnych kontrolach IT, aby zachować integralność pewnych informacji wykorzystywanych przez aplikacje IT, audytor może stwierdzić, że aplikacje IT, które utrzymują te informacje, podlegają ryzykom powstającym na skutek wykorzystania IT.

Przykładowe cechy aplikacji IT, która prawdopodobnie nie podlega ryzykom powstającym na skutek IT	Przykładowe cechy aplikacji IT, która prawdopodobnie podlega ryzykom powstającym na skutek IT
• Aplikacje samodzielne. • Wolumen danych (transakcji) nie jest znaczący. • Funkcjonalność aplikacji nie jest złożona. • Każda transakcja jest wspierana przez oryginalną dokumentację w formie kopii papierowej.	• Aplikacje są połączone za pośrednictwem interfejsu. • Wolumen danych (transakcji) jest znaczący. • Funkcjonalność aplikacji jest złożona, ponieważ: – aplikacja automatycznie inicjuje transakcje oraz – istnieje wiele złożonych obliczeń leżących u podstaw automatycznych wpisów.
Aplikacja IT prawdopodobnie nie podlega ryzykom powstającym na skutek IT, ponieważ: • wolumen danych nie jest znaczący i w związku z tym kierownictwo nie polega na ogólnych kontrolach IT, aby przetwarzać lub utrzymywać dane, • kierownictwo nie polega na automatycznych kontrolach ani innych zautomatyzowanych funkcjonalnościach. Audytor nie zidentyfikował kontroli automatycznych zgodnie z paragrafem 26(a), • chociaż kierownictwo wykorzystuje w swoich kontrolach raporty generowane przez system, nie polega na tych raportach. Zamiast tego uzgadnia raporty z dokumentacją w formie kopii papierowej i weryfikuje obliczenia w raportach, • audytor będzie bezpośrednio testować informacje przedstawione przez jednostkę, wykorzystywane jako dowody badania.	Aplikacja IT prawdopodobnie podlega ryzykom powstającym na skutek IT, ponieważ: • kierownictwo polega na systemie aplikacji, aby przetwarzać lub utrzymywać dane, ponieważ wolumen danych jest znaczący, • kierownictwo polega na systemie aplikacji, aby wykonywać pewne kontrole automatyczne, które audytor również zidentyfikował.

Inne aspekty środowiska IT, które podlegają ryzykom powstającym na skutek wykorzystania IT

16. Gdy audytor identyfikuje aplikacje IT, które podlegają ryzykom powstającym na skutek wykorzystania IT, inne aspekty środowiska IT zazwyczaj również podlegają ryzykom

powstającym na skutek wykorzystania IT. Infrastruktura IT obejmuje bazy danych, system operacyjny i sieć. Bazy danych przechowują dane wykorzystywane przez aplikacje IT i mogą składać się z wielu powiązanych ze sobą tabel danych. Dostęp do danych w bazach danych może być również uzyskany bezpośrednio przez systemy zarządzania bazami danych przez personel IT lub innych pracowników posiadających uprawnienia administratorów. System operacyjny jest odpowiedzialny za zarządzanie komunikacją pomiędzy sprzętem, aplikacjami IT i innym oprogramowaniem używanym w sieci. W ten sposób aplikacje IT i bazy danych mogą być bezpośrednio dostępne poprzez system operacyjny. Sieć jest wykorzystywana w infrastrukturze IT do przesyłania danych oraz do dzielenia informacji, zasobów i usług poprzez wspólne łącze komunikacyjne. Sieć ustanawia również zazwyczaj warstwę zabezpieczeń logicznych (udostępnianą poprzez system operacyjny) dla dostępu do podstawowych zasobów.

17. Gdy audytor identyfikuje aplikacje IT jako podlegające ryzykom powstającym na skutek IT, baza(-y) danych, w której(-ych) przechowywane są dane przetwarzane przez zidentyfikowane aplikacje IT, zwykle również jest(są) identyfikowana(-e). Podobnie, ponieważ zdolność do działania aplikacji IT jest często uzależniona od systemu operacyjnego, a aplikacje IT i bazy danych mogą być bezpośrednio dostępne z systemu operacyjnego, system operacyjny zazwyczaj podlega ryzykom powstającym na skutek wykorzystania IT. Sieć może być zidentyfikowana, gdy jest centralnym punktem dostępu do zidentyfikowanych aplikacji IT i powiązanych z nimi baz danych lub gdy aplikacja IT współdziała z dostawcami lub stronami zewnętrznymi przez Internet lub gdy sieciowe aplikacje IT zostały zidentyfikowane przez audytora.

Identyfikowanie ryzyk powstających na skutek wykorzystania IT i ogólnych kontroli IT

18. Przykłady ryzyk powstających na skutek wykorzystania IT obejmują ryzyka związane z niewłaściwym poleganiem na aplikacjach IT, które nieprawidłowo przetwarzają dane, przetwarzają niedokładne dane lub oba przypadki łącznie, takie jak:
 - nieautoryzowany dostęp do danych, który może skutkować zniszczeniem danych lub nieprawidłowymi zmianami danych, w tym rejestracją nieautoryzowanych lub nieistniejących transakcji, lub niedokładnym rejestrowaniem transakcji; szczególne ryzyka mogą powstać, gdy wielu użytkowników ma dostęp do wspólnej bazy danych,
 - możliwość uzyskania przez personel IT przywilejów dostępu wykraczających poza te, które są niezbędne do wykonywania powierzonych im obowiązków, łamiąc tym samym podział obowiązków,
 - nieautoryzowane zmiany danych w plikach głównych,
 - nieautoryzowane zmiany w aplikacjach IT lub innych aspektach środowiska IT,
 - niedokonywanie niezbędnych zmian w aplikacjach IT lub innych aspektach środowiska IT,
 - niewłaściwa interwencja ręczna,
 - potencjalna utrata danych lub brak możliwości dostępu do danych, gdy jest to wymagane.
19. Rozważania audytora dotyczące nieupoważnionego dostępu mogą obejmować ryzyka związane z nieupoważnionym dostępem przez strony wewnętrzne lub zewnętrzne (często określane jako ryzyka związane z bezpieczeństwem cybernetycznym). Takie ryzyka nie muszą koniecznie dotyczyć sprawozdawczości finansowej, ponieważ środowisko IT jednostki może również obejmować aplikacje IT i powiązane z nimi dane, które odnoszą się do potrzeb operacyjnych lub potrzeb w zakresie zgodności. Należy zauważyć, że incydenty cybernetyczne występują zazwyczaj w pierwszej kolejności w warstwach sieci obwodowej i wewnętrznej, które zazwyczaj są dalej usuwane z aplikacji IT, baz danych i systemów operacyjnych, które mają wpływ na

sporządzenie sprawozdania finansowego. W związku z tym, jeżeli zidentyfikowano informacje na temat naruszenia bezpieczeństwa, audytor zazwyczaj rozważa zakres, w jakim takie naruszenie potencjalnie mogło wpłynąć na sprawozdawczość finansową. Jeżeli może to mieć wpływ na sprawozdawczość finansową, audytor może podjąć decyzję o uzyskaniu zrozumienia i przetestowaniu powiązanych kontroli, aby ustalić potencjalny wpływ lub zakres potencjalnych zniekształceń sprawozdania finansowego lub może ustalić, że jednostka zapewniła adekwatne ujawnienia w związku z takim naruszeniem bezpieczeństwa.

20. Ponadto przepisy prawa i regulacje, które mogą mieć bezpośredni lub pośredni wpływ na sprawozdanie finansowe jednostki, mogą obejmować przepisy o ochronie danych. Rozważania dotyczące zgodności jednostki z takimi przepisami prawa lub regulacją, zgodnie z MSB 250 (zmienionym), mogą obejmować zrozumienie procesów IT jednostki oraz ogólnych kontroli IT, które jednostka wdrożyła, aby odnieść się do stosownych przepisów prawa lub regulacji.
21. Ogólne kontrole IT są wdrażane, aby odnieść się do ryzyk powstających na skutek wykorzystania IT. W związku z tym podczas identyfikowania ogólnych kontroli IT audytor wykorzystuje uzyskane zrozumienie zidentyfikowanych aplikacji IT i innych aspektów środowiska IT oraz mających zastosowanie ryzyk powstających na skutek wykorzystania IT. W niektórych przypadkach jednostka może wykorzystywać wspólne procesy IT w całym swoim środowisku IT lub w ramach pewnych aplikacji IT i w takim przypadku można zidentyfikować powszechne ryzyka powstające na skutek wykorzystania IT oraz powszechne ogólne kontrole IT.
22. Ogólnie, prawdopodobnie zostanie zidentyfikowana większa liczba ogólnych kontroli IT związanych z aplikacjami IT i bazami danych niż w przypadku innych aspektów środowiska IT. Wynika to z faktu, że aspekty te są najbliższe związane z przetwarzaniem i utrzymywaniem informacji w systemie informacyjnym jednostki. Identyfikując ogólne kontrole IT, audytor może rozważyć kontrole działań zarówno użytkowników końcowych, jak i personelu IT jednostki lub dostawców usług IT.
23. **Załącznik 6** zawiera dalsze wyjaśnienia charakteru ogólnych kontroli IT, które są zazwyczaj wdrażane dla różnych aspektów środowiska IT. Ponadto dostarczono przykłady ogólnych kontroli IT dla różnych procesów IT.

Załącznik 6

(Zob. par. 26(c), A173–A174)

Rozważania dotyczące zrozumienia ogólnych kontroli IT

Niniejszy załącznik przedstawia dalsze zagadnienia, które audytor może rozważyć podczas uzyskiwania zrozumienia ogólnych kontroli IT.

1. Rodzaj ogólnych kontroli IT, które są zazwyczaj wdrażane dla każdego z aspektów środowiska IT:
 - (a) Aplikacje

Ogólne kontrole IT w warstwie aplikacji IT będą skorelowane z charakterem i zakresem funkcjonalności aplikacji oraz ścieżkami dostępu dozwolonymi w technologii. Na przykład więcej kontroli będzie stosowne dla wysoce zintegrowanych aplikacji IT ze złożonymi opcjami bezpieczeństwa niż w starszych aplikacjach IT wspierających niewielką liczbę sald kont z metodami dostępu wyłącznie poprzez transakcje.
 - (b) Baza Danych

Ogólne kontrole IT w warstwie bazy danych zazwyczaj odnoszą się do ryzyk powstających na skutek wykorzystania IT związanych z nieupoważnioną aktualizacją informacji sprawozdawczości finansowej w bazie danych poprzez bezpośredni dostęp do bazy danych lub wykonanie skryptu lub programu.
 - (c) System Operacyjny

Ogólne kontrole IT w warstwie systemu operacyjnego zazwyczaj odnoszą się do ryzyk powstających na skutek wykorzystania IT związanych z dostępem administracyjnym, co może ułatwić obejście innych kontroli. Obejmuje to takie działania, jak naruszanie uprawnień innych użytkowników, dodawanie nowych, nieuprawnionych użytkowników, ładowanie złośliwego oprogramowania lub wykonywanie skryptów lub innych nieautoryzowanych programów.
 - (d) Sieć

Ogólne kontrole IT w warstwie sieciowej zazwyczaj odnoszą się do ryzyk powstających na skutek wykorzystania IT związanych z segmentacją sieci, zdalnym dostępem i uwierzytelnianiem. Kontrole sieci mogą być stosowne, gdy jednostka posiada aplikacje internetowe wykorzystywane w sprawozdawczości finansowej. Kontrole sieci mogą być stosowne, gdy jednostka utrzymuje znaczące relacje z partnerami biznesowymi lub korzysta z outsourcingu od stron trzecich, co może zwiększyć transmisję danych i potrzebę zdalnego dostępu.
2. Przykłady ogólnych kontroli IT, które mogą występować, organizowanych przez proces IT, obejmują:
 - (a) Proces zarządzania dostępem:
 - o *Uwierzytelnienie*

Kontrole zapewniające, że użytkownik uzyskujący dostęp do aplikacji IT lub innego aspektu środowiska IT korzysta z własnych uprawnień użytkownika do logowania (tj. użytkownik nie korzysta z uprawnień innego użytkownika).

- *Autoryzacja*
Kontrole, które umożliwiają użytkownikom dostęp do informacji niezbędnych do wykonywania ich obowiązków służbowych i niczego więcej, co ułatwia odpowiedni podział obowiązków.
 - *Aktywacja*
Kontrole nadawania uprawnień nowym użytkownikom oraz modyfikacji uprawnień dostępu istniejących użytkowników.
 - *Dezaktywacja*
Kontrole usuwania dostępu użytkownika po zakończeniu lub przeniesieniu.
 - *Uprzywilejowany dostęp*
Kontrole dostępu użytkowników administracyjnych lub o szerokich uprawnieniach.
 - *Przegląd dostępu użytkowników*
Kontrole ponownej certyfikacji lub oceny dostępu użytkownika dla bieżącej autoryzacji w danym okresie.
 - *Kontrole konfiguracji zabezpieczeń*
Każda technologia ma na ogół kluczowe ustawienia konfiguracyjne, które pomagają ograniczyć dostęp do środowiska.
 - *Dostęp Fizyczny*
Kontrole fizycznego dostępu do centrum danych i sprzętu, ponieważ taki dostęp może być wykorzystany do obejścia innych kontroli.
- (b) Proces zarządzania programem lub innymi zmianami w środowisku IT:
- *Proces zarządzania zmianami*
Kontrole nad procesem projektowania, programowania, testowania i migracji zmian do środowiska produkcyjnego (tj. do użytkownika końcowego).
 - *Podział obowiązków w związku z migracją zmian*
Kontrole, które segregują dostęp, aby dokonać migracji zmian do środowiska produkcyjnego.
 - *Rozwój lub nabycie lub wdrożenie systemów*
Kontrole wstępnego rozwijania lub wdrażania aplikacji IT (lub w odniesieniu do innych aspektów środowiska IT).
 - *Konwersja danych*
Kontrole konwersji danych podczas rozwijania, wdrażania lub aktualizacji środowiska IT.
- (c) Proces zarządzania działalnością IT
- *Planowanie pracy*
Kontrole dostępu do harmonogramu i inicjowania zadań lub programów, które mogą mieć wpływ na sprawozdawczość finansową.

- *Monitorowanie zadań*

Kontrole w celu monitorowania zadań lub programów sprawozdawczości finansowej pod kątem ich pomyślnej realizacji.

- *Kopie zapasowe i odzyskiwanie*

Kontrole w celu zapewnienia, aby kopie zapasowe danych sprawozdawczości finansowej były tworzone zgodnie z planem oraz aby takie dane były dostępne i aby zapewniona była możliwość dostępu do tych danych w celu ich terminowego odzyskania w przypadku przestoju lub ataku.

- *Wykrywanie włamań*

Kontrole w celu monitorowania podatności na zagrożenia i/lub włamania do środowiska IT.

Poniższa tabela ilustruje przykłady ogólnych kontroli IT, aby odnieść się do przykładów ryzyk powstających na skutek wykorzystania IT, w tym dla różnych aplikacji IT na podstawie ich charakteru.

Proces	Ryzyka	Kontrole	Aplikacje IT		
Proces IT	Przykładowe ryzyka powstające na skutek wykorzystania IT	Przykład ogólnych kontroli IT	Niezłożone oprogramowanie komercyjne – Mające zastosowanie (tak / nie)	Średniej wielkości i umiarkowane złożone oprogramowanie komercyjne lub aplikacje IT – Mające zastosowanie (tak / nie)	Duże lub złożone aplikacje IT (np. systemy ERP) – Mające zastosowanie (tak / nie)
Zarządzanie dostępem	Uprawnienia dostępu użytkowników w: Użytkownicy mają uprawnienia dostępu wykraczające poza te, które są niezbędne, aby wykonać przydzielone im obowiązki, co może stworzyć niewłaściwy	Kierownictwo zatwierdza charakter i zakres uprawnień dostępu użytkownika dla nowych i zmodyfikowanych dostępu użytkowników, w tym standardowe profile/role w aplikacji, krytyczne transakcje w zakresie sprawozdawczości finansowej	Tak – zamiast opisanych poniżej przeglądów dostępu użytkownika	Tak	Tak

Proces	Ryzyka	Kontrole	Aplikacje IT		
Proces IT	Przykładowe ryzyka powstające na skutek wykorzystania IT	Przykład ogólnych kontroli IT	Niezłożone oprogramowanie komercyjne – Mające zastosowanie (tak / nie)	Średniej wielkości i umiarkowanie złożone oprogramowanie komercyjne lub aplikacje IT – Mające zastosowanie (tak / nie)	Duże lub złożone aplikacje IT (np. systemy ERP) – Mające zastosowanie (tak / nie)
	podział obowiązków.	oraz podział obowiązków			
		Dostęp dla zakończonych lub przeniesionych użytkowników jest usuwany lub modyfikowany w odpowiednim czasie	Tak – zamiast poniższych przeglądów dostępu użytkownika	Tak	Tak
		Okresowo weryfikowany jest dostęp użytkownika	Tak – zamiast powyższych kontroli aktywacji/dezaktywacji	Tak – dla pewnych aplikacji	Tak
		Podział obowiązków jest monitorowany, a dostęp powodujący konflikt jest albo usuwany, albo przypisywany do kontroli łagodzących ryzyko, które są dokumentowane i testowane	Nie dotyczy – brak segregacji umożliwionej przez system	Tak – dla pewnych aplikacji	Tak
		Dostęp na poziomie uprzywilejowanym (np. administratorzy)	Tak – prawdopodobnie nie tylko w warstwie aplikacji IT	Tak – w aplikacji IT i w pewnych warstwach	Tak – we wszystkich warstwach środowiska

Proces	Ryzyka	Kontrole	Aplikacje IT		
Proces IT	Przykładowe ryzyka powstające na skutek wykorzystania IT	Przykład ogólnych kontroli IT	Niezłożone oprogramowanie komercyjne – Mające zastosowanie (tak / nie)	Średniej wielkości i umiarkowanie złożone oprogramowanie komercyjne lub aplikacje IT – Mające zastosowanie (tak / nie)	Duże lub złożone aplikacje IT (np. systemy ERP) – Mające zastosowanie (tak / nie)
		konfiguracji, danych i bezpieczeństwa) jest autoryzowany i odpowiednio ograniczony		środowiska IT dla platformy	IT dla platformy
Zarządzanie dostępem	Bezpośredni dostęp do danych: Nieodpowiednie zmiany wprowadzane są bezpośrednio w danych finansowych za pomocą środków innych niż transakcje w aplikacji.	Dostęp do plików danych aplikacji lub obiektów/tabel/ danych bazy danych jest ograniczony do uprawnionego personelu, na podstawie ich zakresu obowiązków i przydzielonej roli i taki dostęp jest zatwierdzany przez kierownictwo	Nie dotyczy	Tak – dla pewnych aplikacji i baz danych	Tak
Zarządzanie dostępem	Ustawienia systemu: Systemy nie są adekwatnie skonfigurowane lub aktualizowane, aby ograniczyć dostęp do systemu dla	Dostęp jest autoryzowany za pomocą niepowtarzalnych identyfikatorów użytkowników i haseł lub innych metod jako mechanizm potwierdzający, że użytkownicy	Tak – tylko autoryzowane hasłem	Tak – kombinacja hasła i wieloczynnikowej autoryzacji	Tak

Proces	Ryzyka	Kontrole	Aplikacje IT		
Proces IT	Przykładowe ryzyka powstające na skutek wykorzystania IT	Przykład ogólnych kontroli IT	Niezłożone oprogramowanie komercyjne – Mające zastosowanie (tak / nie)	Średniej wielkości i umiarkowanie złożone oprogramowanie komercyjne lub aplikacje IT – Mające zastosowanie (tak / nie)	Duże lub złożone aplikacje IT (np. systemy ERP) – Mające zastosowanie (tak / nie)
	odpowiednio uprawnionych i odpowiednich użytkowników.	są uprawnieni do uzyskania dostępu do systemu. Parametry hasła odpowiadają standardom firmowym lub branżowym (np. minimalna długość i złożoność hasła, wygaśnięcie, blokada konta)			
		Kluczowe atrybuty konfiguracji zabezpieczeń są odpowiednio wdrożone	Nie dotyczy – nie istnieją żadne konfiguracje zabezpieczeń technicznych	Tak – dla pewnych aplikacji i baz danych	Tak
Zarządzanie zmianami	Zmiany w aplikacji: Dokonuje się niewłaściwych zmian w systemach lub programach aplikacji, które zawierają stosowne kontrole automatyczne (tj.	Zmiany w aplikacji są odpowiednio testowane i zatwierdzane przed wprowadzeniem ich do środowiska produkcyjnego	Nie dotyczy – zweryfikowano by, że żaden kod źródłowy nie jest zainstalowany	Tak – dla oprogramowania niekomercyjnego	Tak
		Dostęp do wdrożenia zmian w środowisku produkcyjnym aplikacji jest	Nie dotyczy	Tak – dla oprogramowania niekomercyjnego	Tak

Proces	Ryzyka	Kontrole	Aplikacje IT		
Proces IT	Przykładowe ryzyka powstające na skutek wykorzystania IT	Przykład ogólnych kontroli IT	Niezłożone oprogramowanie komercyjne – Mające zastosowanie (tak / nie)	Średniej wielkości i umiarkowane złożone oprogramowanie komercyjne lub aplikacje IT – Mające zastosowanie (tak / nie)	Duże lub złożone aplikacje IT (np. systemy ERP) – Mające zastosowanie (tak / nie)
	konfigurowane ustawienia, zautomatyzowane algorytmy, zautomatyzowane obliczenia i zautomatyzowaną ekstrakcję danych) lub logikę raportowania.	odpowiednio ograniczony i oddzielony od środowiska rozwojowego			
Zarządzanie zmianą	Zmiany w bazie danych: Nieodpowiednie zmiany są dokonywane w strukturze bazy danych i relacji pomiędzy danymi.	Zmiany w bazie danych są odpowiednio testowane i zatwierdzane przed przeniesieniem ich do środowiska produkcyjnego	Nie dotyczy – żadne zmiany w bazie danych nie są dokonywane w jednostce	Tak – dla oprogramowania niekomercyjnego	Tak
Zarządzanie zmianą	Zmiany w oprogramowaniu systemowym: W oprogramowaniu systemowym (np. w systemie operacyjnym, sieci, oprogramowa	Zmiany w oprogramowaniu systemowym są odpowiednio testowane i zatwierdzane przed przeniesieniem ich do środowiska produkcyjnego	Nie dotyczy – żadne zmiany w oprogramowaniu systemowym nie są dokonywane w jednostce	Tak	Tak

Proces	Ryzyka	Kontrole	Aplikacje IT		
Proces IT	Przykładowe ryzyka powstające na skutek wykorzystania IT	Przykład ogólnych kontroli IT	Niezłożone oprogramowanie komercyjne – Mające zastosowanie (tak / nie)	Średniej wielkości i umiarkowane złożone oprogramowanie komercyjne lub aplikacje IT – Mające zastosowanie (tak / nie)	Duże lub złożone aplikacje IT (np. systemy ERP) – Mające zastosowanie (tak / nie)
	niu do zarządzania zmianami, oprogramowaniu kontroli dostępu) dokonywane są niewłaściwe zmiany.				
Zarządzanie zmianą	Konwersja danych: Dane konwertowane ze starszych systemów lub poprzednich wersji wprowadzają błędne dane, jeżeli konwersja przenosi dane niekompletne, nadmiarowe, przestarzałe lub niedokładne.	Kierownictwo zatwierdza wyniki konwersji danych (np. czynności bilansowania i uzgadniania) ze starego systemu aplikacji lub struktury danych na nowy system aplikacji lub strukturę danych i monitoruje, czy konwersja jest wykonywana zgodnie z ustalonymi politykami i procedurami konwersji	Nie dotyczy – zastąpiony przez kontrole ręczne	Tak	Tak
Operacje IT	Sieć: Sieć nie zabezpiecza adekwatnie przed	Dostęp jest autoryzowany poprzez niepowtarzalne	Nie dotyczy – nie istnieje odrębna metoda	Tak	Tak

Proces	Ryzyka	Kontrole	Aplikacje IT		
Proces IT	Przykładowe ryzyka powstające na skutek wykorzystania IT	Przykład ogólnych kontroli IT	Niezłożone oprogramowanie komercyjne – Mające zastosowanie (tak / nie)	Średniej wielkości i umiarkowane złożone oprogramowanie komercyjne lub aplikacje IT – Mające zastosowanie (tak / nie)	Duże lub złożone aplikacje IT (np. systemy ERP) – Mające zastosowanie (tak / nie)
	uzyskaniem przez nieautoryzowanych użytkowników w niewłaściwym o dostępu do systemów informacyjnych.	identyfikatory użytkowników i hasła lub inne metody jako mechanizm potwierdzający, że użytkownicy są uprawnieni do uzyskania dostępu do systemu. Parametry hasła są zgodne z politykami i standardami firmowymi lub zawodowymi (np. minimalna długość i złożoność hasła, wygaśnięcie, blokada konta)	autoryzowani a sieciowego		
		Architektura sieci oddziela segmenty aplikacji internetowych od sieci wewnętrznej, skąd dostępne są stosowne aplikacje ICFR	Nie dotyczy – nie zastosowano segmentacji sieci	Tak – z osądem	Tak – z osądem
		Okresowo skany wrażliwości obwodu sieci	Nie dotyczy	Tak – z osądem	Tak – z osądem

Proces	Ryzyka	Kontrole	Aplikacje IT		
Proces IT	Przykładowe ryzyka powstające na skutek wykorzystania IT	Przykład ogólnych kontroli IT	Niezłożone oprogramowanie komercyjne – Mające zastosowanie (tak / nie)	Średniej wielkości i umiarkowane złożone oprogramowanie komercyjne lub aplikacje IT – Mające zastosowanie (tak / nie)	Duże lub złożone aplikacje IT (np. systemy ERP) – Mające zastosowanie (tak / nie)
		wykonywane są przez zespół zarządzający siecią, który bada również potencjalne wrażliwości			
		Okresowo generowane są alarmy, aby powiadomić o zagrożeniach zidentyfikowanych przez systemy wykrywania włamań. Zagrożenia te są badane przez zespół zarządzający siecią	Nie dotyczy	Tak – z osądem	Tak – z osądem
		Wdrożono kontrole, aby ograniczyć dostęp do wirtualnej sieci prywatnej (VPN) do autoryzowanych i odpowiednich użytkowników	Nie dotyczy – brak VPN	Tak – z osądem	Tak – z osądem
Operacje IT	Tworzenie kopii zapasowych i odzyskiwani	Regularnie tworzone są kopie zapasowe danych	Nie dotyczy – poleganie przez zespół finansowy na	Tak	Tak

Proces	Ryzyka	Kontrole	Aplikacje IT		
Proces IT	Przykładowe ryzyka powstające na skutek wykorzystania IT	Przykład ogólnych kontroli IT	Niezłożone oprogramowanie komercyjne – Mające zastosowanie (tak / nie)	Średniej wielkości i umiarkowane złożone oprogramowanie komercyjne lub aplikacje IT – Mające zastosowanie (tak / nie)	Duże lub złożone aplikacje IT (np. systemy ERP) – Mające zastosowanie (tak / nie)
	e danych: Danych finansowych nie można odzyskać ani uzyskać dostępu do nich w odpowiednim czasie w przypadku utraty danych.	finansowych zgodnie z ustalonym harmonogramem i z ustaloną częstotliwością	ręcznych kopiach zapasowych		
Operacje IT	Planowanie zadań: Systemy produkcyjne, programy lub zadania powodują niedokładne, niekompletne lub nieuprawnione przetwarzanie danych.	Tylko uprawnieni użytkownicy mają dostęp do aktualizacji zadań pakietowych (w tym zadań interfejsu) w oprogramowaniu do planowania zadań	Nie dotyczy – brak zadań pakietowych	Tak – dla pewnych aplikacji	Tak
		Krytyczne systemy, programy lub zadania są monitorowane, a błędy przetwarzania są korygowane, aby zapewnić ich pomyślną realizację.	Nie dotyczy – brak monitorowania zadań	Tak – dla pewnych aplikacji	Tak

International Foundation for Ethics and Audit™ (IFEATM), International Auditing and Assurance Standards Board (IAASB®) oraz International Federation of Accountants® (IFAC®) nie ponoszą odpowiedzialności za straty poniesione przez osoby, które działają lub powstrzymują się od działania w oparciu o materiały zawarte w niniejszej publikacji, bez względu na to, czy straty te zostały spowodowane zaniedbaniem, czy w inny sposób.

Międzynarodowe Standardy Badania (International Standards on Auditing, ISA), Międzynarodowy Standard Badania dla badań sprawozdań finansowych mniej złożonych jednostek (International Standard on Auditing for Audits of Financial Statements of Less Complex Entities, ISA for LCE), Międzynarodowe Standardy Usług Atestacyjnych (International Standards on Assurance Engagements, ISAE), Międzynarodowe Standardy Usług Przeglądu (International Standards on Review Engagements, ISRE), Międzynarodowe Standardy Usług Pokrewnych (International Standards on Related Services, ISRS), Międzynarodowe Standardy Zarządzania Jakością (International Standards on Quality Management, ISQM), Wskazówki Praktyczne dotyczące badania (International Auditing Practice Notes), dokumenty do dyskusji (Exposure Drafts, Consultation Papers) oraz inne publikacje IAASB są publikowane przez IFAC, która jest również posiadaczem odnośnych praw autorskich.

Copyright © sierpień 2024 r., International Federation of Accountants (IFAC). Wszelkie prawa zastrzeżone. Niniejszą publikację można pobrać na własny użytek niekomercyjny (tj. do korzystania w celach zawodowych lub naukowych) ze strony internetowej www.iaasb.org. Tłumaczenie, powielanie, przechowywanie lub udostępnianie, bądź wykorzystywanie niniejszego dokumentu w podobny sposób wymaga pisemnej zgody.

Nazwy: „International Auditing and Assurance Standards Board”, „International Standards on Auditing”, „International Standards on Assurance Engagements”, „International Standards on Review Engagements”, „International Standards on Related Services”, „International Standards on Quality Control”, „International Auditing Practice Notes”, „IAASB”, „ISA”, „ISAE”, „ISRE”, „ISRS”, „ISQC”, „ISQM”, „IAPN” oraz logotyp IAASB są znakami towarowymi IFAC lub zarejestrowanymi znakami towarowymi i usługowymi IFAC w Stanach Zjednoczonych i w innych krajach. Nazwy: „International Foundation for Ethics and Audit” i „IFEATM” są znakami towarowymi IFEA lub zarejestrowanymi znakami towarowymi i usługowymi IFEA w Stanach Zjednoczonych i w innych krajach.

Struktury i procesy wspierające działalność IAASB są wspierane przez International Foundation for Ethics and Audit™ (IFEATM).

Informacje na temat praw autorskich, znaków towarowych i pozwoleń można znaleźć na permissions lub uzyskać pod adresem permissions@ifac.org.

Niniejszy Międzynarodowy Standard Badania (MSB) 315 (zmieniony w 2019 r.) *Identyfikacja i oszacowanie ryzyk istotnego zniekształcenia*, uchwalony przez International Auditing and Assurance Standards Board (IAASB) i opublikowany w języku angielskim przez International Federation of Accountants (IFAC) w sierpniu 2024 roku, został przetłumaczony na język polski przez Polską Izbę Biegłych Rewidentów (PIBR) w grudniu 2025 roku i jest powielany za zgodą IFAC. Proces tłumaczenia Międzynarodowych Standardów Badania (MSB) był rozważany przez IFAC i tłumaczenie zostało przeprowadzone zgodnie z „Policy Statement—Policy for Translating Publications of the International Federation of Accountants”. Zatwierdzonym tekstem wszystkich Międzynarodowych Standardów Badania (MSB) jest tekst opublikowany przez IFAC w języku angielskim. IFAC nie ponosi odpowiedzialności za dokładność i kompletność tłumaczenia ani za działania, które mogą z tego wynikać.

Tekst Międzynarodowego Standardu Badania (MSB) 315 (zmienionego w 2019 r.) *Identyfikacja i oszacowanie ryzyk istotnego zniekształcenia* w języku angielskim © 2024 by IFAC. Wszelkie prawa zastrzeżone.

Tekst Międzynarodowego Standardu Badania (MSB) 315 (zmienionego w 2019 r.) *Identyfikacja i oszacowanie ryzyk istotnego zniekształcenia* w języku polskim © 2025 by IFAC. Wszelkie prawa zastrzeżone.

Tytuł oryginału: International Standard on Auditing (ISA) 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement*. Handbook IAASB 2023-2024. ISBN: 978-1-60815-573-6

Aby uzyskać zgodę na powielanie, przechowywanie lub przesyłanie, albo w inny podobny sposób wykorzystywać niniejszy dokument, napisz na adres: permissions@ifac.org.



529 Fifth Avenue, New York, NY 10017
T +1 (212) 286-9344 F +1 (212) 286-9570
www.iaasb.org

ISBN: 978-1-60815-591-0

Znaki towarowe oraz zarejestrowane znaki towarowe i usługowe

International Auditing and Assurance Standards Board®

IAASB®



International Standards on Auditing®

International Standard on Auditing for Audits of Financial Statements
of Less Complex Entities™

International Standards on Assurance Engagements™

International Standards on Review Engagements™

International Standards on Related Services™

International Standards on Quality Management™

International Auditing Practice Notes™

ISA®

ISA for LCE™

ISAE™

ISRE™

ISRS™

ISQM™

IAPN™