

Spis treści

O autorze	13
Przedmowa	15
 CZĘŚĆ I. PODSTAWY WSPÓŁCZESNEGO AUDYTU WEWNĘTRZNEGO	 23
Rozdział 1. Podstawy audytu	25
1.1. Historia i początki audytu	27
1.2. Struktura książki	31
Rozdział 2. Powszechny zakres wiedzy audytu wewnętrznego	34
2.1. Co to jest CBOK? Doświadczenia z innych profesji	35
2.2. CBOK Fundacji Badawczej Instytutu Audytorów Wewnętrznych	37
2.3. Co powinien wiedzieć audytor wewnętrzny	42
2.4. Dalszy rozwój CBOK współczesnego audytu	43
 CZĘŚĆ II. ZNACZENIE MECHANIZMÓW KONTROLI WEWNĘTRZNEJ	 45
Rozdział 3. Zasady ramowe kontroli wewnętrznej: standard COSO	47
3.1. Znaczenie skutecznych mechanizmów kontroli wewnętrznej	48
3.2. Standardy kontroli wewnętrznej: tło historyczne	50
3.3. Zdarzenia prowadzące do powołania Komisji Treadwaya	53
3.4. Zasady ramowe kontroli wewnętrznej COSO	58
3.5. Pozostałe wymiary zasad ramowych kontroli wewnętrznej COSO	81
3.6. Wymagania w zakresie CBOK audytu	82
Rozdział 4. Ustawa Sarbanesa–Oxleya i jej następstwa	83
4.1. Kluczowe elementy ustawy Sarbanesa–Oxleya	84
4.2. Dokonywanie przeglądów wymaganych w sekcji 404 na podstawie standardu AS 5	111

4.3. Zasady standardu AS 5 a audyt wewnętrzny	123
4.4. Oddziaływanie ustawy Sarbanesa–Oxleya	126
Rozdział 5. Kolejne zasady ramowe kontroli wewnętrznej: CobiT	128
5.1. Wprowadzenie do CobiT	129
5.2. Zasady ramowe CobiT.	132
5.3. Zastosowanie CobiT w ocenie mechanizmów kontroli wewnętrznej	137
5.4. Stosowanie CobiT w świetle ustawy SOX	151
5.5. Wytyczne w zakresie zasad ramowych zapewnienia CobiT	155
5.6. Szersze spojrzenie na CobiT	156
Rozdział 6. Zarządzanie ryzykiem: COSO ERM	157
6.1. Podstawy zarządzania ryzykiem	158
6.2. COSO ERM: Zarządzanie ryzykiem w przedsiębiorstwie	172
6.3. Kluczowe elementy COSO ERM	175
6.4. Inne wymiary COSO ERM: Cele zarządzania ryzykiem w przedsiębiorstwie	195
6.5. Ryzyko na poszczególnych poziomach organizacyjnych.	199
6.6. Podsumowanie informacji o COSO ERM	201
6.7. Audyt ryzyka i procesów COSO ERM	202
6.8. Szersze spojrzenie na zarządzanie ryzykiem i COSO ERM.	203
 CZĘŚĆ III. PLANOWANIE I PRZEPROWADZANIE AUDYTU WEWNĘTRZNEGO	 207
Rozdział 7. Przeprowadzanie skutecznego audytu wewnętrznego	209
7.1. Organizacja i planowanie audytu wewnętrznego	210
7.2. Czynności przygotowawcze audytu wewnętrznego	211
7.3. Rozpoczęcie audytu wewnętrznego	218
7.4. Opracowanie i przygotowanie programów audytu	225
7.5. Przeprowadzanie audytu wewnętrznego	232
7.6. Podsumowanie działań audytu w terenie.	241
7.7. Przeprowadzanie indywidualnego audytu wewnętrznego.	242
Rozdział 8. Standardy profesjonalnej praktyki audytu wewnętrznego	244
8.1. Standardy profesjonalnej praktyki audytu wewnętrznego	245
8.2. Treść standardów IIA	249
8.3. Kodeksy etyki: IIA oraz ISACA	259
Rozdział 9. Testowanie i ocena wyników audytu	263
9.1. Zbieranie odpowiednich dowodów audytu	263
9.2. Techniki szacowania i oceny w audycie	264
9.3. Eksperycki dobór próby w audycie wewnętrznym	267
9.4. Statystyczny dobór próby – wstęp	269

9.5. Dobór próby na podstawie jednostki monetarnej	293
9.6. Dobór ilościowy i warstwowy dobór ilościowy	299
9.7. Inne techniki doboru próby w audycie	302
9.8. Skuteczne wykorzystanie doboru próby w audycie	304
Rozdział 10. Programy audytu oraz określenie przestrzeni audytu	309
10.1. Określenie zakresu i celów przestrzeni audytu wewnętrznego	310
10.2. Ocena możliwości i celów audytu wewnętrznego	315
10.3. Ograniczenia czasowe i co do zasobów w przestrzeni audytu	317
10.4. „Sprzedawanie” przestrzeni audytu komitetowi audytu oraz kadry zarządzającej	318
10.5. Tworzenie programów audytu: kluczowe elementy przestrzeni audytu	320
10.6. Przestrzeń audytu i utrzymanie programu	326
Rozdział 11. Samoocena kontroli i benchmarking	328
11.1. Znaczenie samooceny kontroli	329
11.2. Model CSA	330
11.3. Uruchomienie procesu CSA	331
11.4. Ocena wyników CSA	338
11.5. Benchmarking a audyt wewnętrzny	339
11.6. Lepsze zrozumienie działań audytu wewnętrznego.	345
CZĘŚĆ IV. ORGANIZOWANIE DZIAŁAŃ AUDYTU WEWNĘTRZNEGO I ZARZĄDZANIE NIMI	349
Rozdział 12. Regulaminy i tworzenie działu audytu wewnętrznego	351
12.1. Zakładanie działu audytu wewnętrznego	352
12.2. Regulamin audytu: uprawnienia komitetu i kierownictwa audytu	353
12.3. Budowanie zespołu audytu wewnętrznego	354
12.4. Metody organizacji działu audytu wewnętrznego	363
12.5. Zasady i procedury audytu wewnętrznego.	372
12.6. Rozwój zawodowy: Budowanie silnego działu audytu wewnętrznego	374
Rozdział 13. Kluczowe kompetencje audytu wewnętrznego	376
13.1. Znaczenie kluczowych kompetencji audytu wewnętrznego	377
13.2. Umiejętności przeprowadzania wywiadu	378
13.3. Umiejętności analityczne	379
13.4. Umiejętności testowania i analizy	380
13.5. Umiejętności dokumentowania	382
13.6. Sformułowane zalecenia oraz działania korygujące	383
13.7. Umiejętności komunikacyjne	386
13.8. Umiejętności negocjacyjne	387

13.9. Gotowość do nauki	389
13.10. Znaczenie podstawowych kompetencji audytora wewnętrznego	390
Rozdział 14. Znajomość zarządzania projektami	391
14.1. Procesy zarządzania projektami	392
14.2. Zarządzanie programami i portfelem w PMBOK	401
14.3. Model dojrzałości organizacyjnej procesu	405
14.4. Korzystanie z zarządzania projektami w celu opracowania skutecznych planów audytu wewnętrznego	407
14.5. Najlepsze praktyki zarządzania projektami a audyt wewnętrzny	408
Rozdział 15. Planowanie i przeprowadzenie audytu	409
15.1. Zrozumieć otoczenie: rozpoczęcie audytu	410
15.2. Dokumentowanie audytu i zrozumienie środowiska kontroli wewnętrznej	412
15.3. Odpowiednie przeprowadzenie procedur audytu	414
15.4. Podsumowanie audytu	415
15.5. Przeprowadzenie audytu	416
Rozdział 16. Dokumentowanie rezultatów przez modelowanie procesów i sporządzanie dokumentów roboczych	418
16.1. Wymagania dotyczące dokumentacji audytu	419
16.2. Modelowanie procesu niezbędne dla audytorów	420
16.3. Dokumenty robocze audytu	425
16.4. Zarządzanie dokumentami audytu	440
16.5. Znaczenie dokumentacji audytu	442
Rozdział 17. Raportowanie wyników audytu	443
17.1. Cele i rodzaje sprawozdań z audytu	444
17.2. Opublikowane sprawozdania z audytu	446
17.3. Cykl sprawozdawczości w ramach audytu	460
17.4. Skuteczne sposoby komunikacji w działaniach audytu	468
17.5. Sprawozdania i zrozumienie roli ludzi w procesie audytu	471
CZĘŚĆ V. WPŁYW TECHNOLOGII INFORMATYCZNYCH NA AUDYT	473
Rozdział 18. Ogólne zabezpieczenia systemów informatycznych i najlepsze praktyki ITIL	475
18.1. Znaczenie ogólnej kontroli IT	476
18.2. Usługa klient-serwer oraz ogólne mechanizmy kontroli mniejszych systemów	477
18.3. Komponenty i zabezpieczenia głównego systemu oraz starych systemów	490
18.4. Przeglądy ogólnych zabezpieczeń w klasycznych systemach	498

18.5. Wsparcie techniczne ITIL i dobre praktyki infrastruktury pomocniczej	504
18.6. Dobre praktyki obsługi technicznej	515
18.7. Audyt zarządzania infrastrukturą informatyczną	524
18.8. Wymagania CBOK stawiane audytorowi w odniesieniu do ogólnych zabezpieczeń informatycznych	525
Rozdział 19. Przegląd i ocena mechanizmów bezpieczeństwa aplikacji informatycznych	527
19.1. Elementy zabezpieczeń aplikacji informatycznych	528
19.2. Wybór aplikacji do przeglądu	540
19.3. Wstępne kroki przeprowadzenia przeglądu mechanizmów kontrolnych aplikacji	541
19.4. Zakończenie audytu mechanizmów kontrolnych aplikacji informatycznej	547
19.5. Przykład przeglądu aplikacji: system budżetowania klient-serwer	555
19.6. Audyt programów w trakcie tworzenia	558
19.7. Znaczenie przeglądu mechanizmów kontrolnych w programach informatycznych	566
Rozdział 20. Zapewnienie cyberbezpieczeństwa i prywatności	568
20.1. Podstawy bezpieczeństwa sieci informatycznych	569
20.2. Zagadnienia związane z prywatnością systemów informatycznych	578
20.3. Audyt bezpieczeństwa i prywatności informatycznej	581
20.4. Bezpieczeństwo i prywatność w dziale audytu	582
20.5. Podstawy PCI-DSS	588
20.6. Rola audytu dotycząca prywatności i cyberbezpieczeństwa	590
Rozdział 21. Narzędzia i techniki komputerowe stosowane w audycie	591
21.1. Rozumienie komputerowych narzędzi i technik wspomagających audyt	592
21.2. Określenie potrzeby zastosowania narzędzi CAATT	595
21.3. Narzędzia oprogramowania CAATT	599
21.4. Wybór odpowiednich procesów CAATT	615
21.5. Etapy tworzenia skutecznego CAATT	616
21.6. Wykorzystanie CAATT do zebrania dowodów	617
Rozdział 22. Planowanie ciągłości biznesowej i odzyskiwanie sprawności po awarii systemu informatycznego	619
22.1. Awaria informatyczna i planowanie ciągłości biznesowej dzisiaj	620
22.2. Przegląd procesów planowania ciągłości biznesowej	623
22.3. Tworzenie planu ciągłości działania informatycznego (BCP)	630
22.4. Planowanie ciągłości biznesowej i umowy poziomu świadczenia usług	640

22.5. Nowsze technologie planowania ciągłości biznesowej: techniki mirroringu danych	641
22.6. Przegląd planów ciągłości działania	643
22.7. Przyszłość planowania ciągłości działania firmy	643
CZĘŚĆ VI. AUDYT A ZARZĄDZANIE PRZEDSIĘBIORSTWEM	645
Rozdział 23. Komunikacja z komitetem audytu rady nadzorczej	647
23.1. Rola komitetu audytu	648
23.2. Organizacja i karty komitetu audytu	649
23.3. Ekspert finansowy komitetu audytu a audyt	654
23.4. Obowiązki komitetu audytu wobec audytu	656
23.5. Komitet audytu i jego zewnętrzni audytorzy	662
23.6. Programy informatora i kodeksy postępowania.	663
23.7. Inne zadania komitetu audytu	664
Rozdział 24. Etyka i programy informatorów	665
24.1. Zasady etyczne, zgodność i ład korporacyjny w przedsiębiorstwie	666
24.2. Kodeks postępowania w przedsiębiorstwie	673
24.3. Funkcja informatora i infolinia	678
24.4. Przeprowadzanie audytu funkcjonowania etyki w przedsiębiorstwie	682
24.5. Poprawa praktyk ładu korporacyjnego	683
Rozdział 25. Wykrywanie oszustw i prewencja	685
25.1. Zrozumienie i rozpoznanie oszustwa	686
25.2. Oznaki oszustwa, na które audytorzy powinni zwrócić uwagę	687
25.3. Rola rachunkowości publicznej w wykrywaniu oszustw.	691
25.4. Standardy IIA dotyczące wykrywania nadużyć i prowadzenia dochodzenia	693
25.5. Dochodzenia w sprawie nadużyć prowadzone przez audytorów	696
25.6. Procesy zapobiegania oszustwom informatycznym	697
25.7. Wykrycie oszustwa przez audytora	700
Rozdział 26. Wymagania zgodności z HIPAA, GLBA i innymi ustawami	701
26.1. HIPAA: ochrona zdrowia i dużo więcej	702
26.2. Zasady audytu według ustawy Gramma-Leacha-Bliley	710
26.3. Wymagania innych przepisów dotyczących poufności i bezpieczeństwa danych osobowych	715
CZĘŚĆ VII. PROFESJONALNY AUDYTOR WEWNĘTRZNY	719
Rozdział 27. Certyfikaty zawodowe: CIA, CISA i inne	721
27.1. Wymagania stawiane Certyfikowanemu audytorowi wewnętrznemu	722

27.2. Co oprócz CIA: inne certyfikaty IIA	733
27.3. Wymagania dotyczące certyfikatu audytora systemów informatycznych (CISA)	738
27.4. Certyfikacja na tytuł <i>Certified Information Security Manager®</i>	740
27.5. Certyfikowany biegły ds. przestępstw i nadużyć gospodarczych	741
27.6. Certyfikat w dziedzinie bezpieczeństwa teleinformatycznego CISSP	743
27.7. Certyfikat audytora ASQ	743
27.8. Inne certyfikaty audytorów	745
Rozdział 28. Audytorzy jako konsultanci przedsiębiorstwa	746
28.1. Standardy zespołu audytu działającego jako grupa doradcza przedsiębiorstwa	747
28.2. Rozpoczęcie świadczenia usług konsultingowych przez zespół audytu	749
28.3. Zapewnienie rozdzielenia obowiązków z zakresu audytu i doradztwa	751
28.4. Najlepsze praktyki konsultingowe	754
28.5. Rozszerzone usługi audytu świadczone kierownictwu	760
Rozdział 29. Ciągłe badanie zapewnienia zgodności i XBRL	761
29.1. Wdrożenie ciągłego badania zapewnienia zgodności	763
29.2. Korzyści czerpane z narzędzi CAA	771
29.3. XBRL: rozszerzalny język sprawozdawczości finansowej oparty na Internecie	772
29.4. Hurtownie danych, wydobywanie danych i OLAP	776
29.5. Nowe technologie, ciągłe zamknięcie ksiąg a audyt	782
CZĘŚĆ VIII. WYMAGANIA CBOK DOTYCZĄCE PROFESJONALNEJ KONWERGENCJI AUDYTU	785
Rozdział 30. ISO 27001, ISO 9000 i inne normy międzynarodowe.	787
30.1. Znaczenie standardów ISO w dzisiejszym globalnym świecie	788
30.2. Przegląd norm ISO	791
30.3. Audyt systemów zarządzania jakością ISO.19011	804
30.4. Normy ISO a audytorzy	806
Rozdział 31. Audyt zapewnienia jakości i normy ASQ	807
31.1. Obowiązki i odpowiedzialność audytorów jakości	808
31.2. Rola audytora jakości	810
31.3. Wykonanie audytów jakości ASQ	813
31.4. Audytorzy jakości a audytor IIA	817
31.5. Przeglądy zapewnienia jakości wykonywane przez funkcje audytu	817

31.6. Uruchomienie przeglądu QA audytu	824
31.7. Przyszłe kierunki prowadzenia audytu zapewnienia jakości	837
Rozdział 32. Six Sigma i odchudzone techniki	839
32.1. Historia i koncepcje Six Sigma	840
32.2. Wdrożenie Six Sigma	842
32.3. Odchudzona Six Sigma	849
32.4. Audyt procesów Six Sigma	852
32.5. Six Sigma w działalności audytorów	853
Rozdział 33. Międzynarodowe standardy audytu i rachunkowości	856
33.1. Międzynarodowe standardy audytu i rachunkowości: jak do tego doszliśmy?	857
33.2. Konwergencja standardów sprawozdawczości finansowej	860
33.3. IFRS: co audytorzy muszą wiedzieć	862
33.4. Międzynarodowe normy audytu	863
33.5. Kolejne etapy w normach dotyczących audytu	864
Rozdział 34. CBOK dla współczesnego audytora	865
34.1. Część pierwsza: Podstawy współczesnego audytu wewnętrznego	866
34.2. Część druga: Znaczenie mechanizmów kontroli wewnętrznej	866
34.3. Część trzecia: Planowanie i przeprowadzanie audytu wewnętrznego	867
34.4. Część czwarta: Organizowanie działań audytu wewnętrznego i zarządzanie nimi	868
34.5. Część piąta: Wpływ technologii informatycznych na audyt	869
34.6. Część szósta: Audyt a zarządzanie przedsiębiorstwem	870
34.7. Część siódma: Profesjonalny audytor wewnętrzny	871
34.8. Część ósma: Wymagania CBOK dotyczące profesjonalnej konwergencji audytu	871
34.9. CBOK dla audytorów	872
Indeks	873