ISACA®
Trust in, and value from, information systems

COBIT®

Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi

COBIT® 5

AN ISACA® FRAMEWORK

ISACA®
Licząca 95 tysięcy członków w 160 krajach ISACA (*www.isaca.org*) jest czołową ogólnoświatową organizacją dostarczającą wiedzę, wystawiającą certyfikaty, prowadzącą szkolenia i inne działania na rzecz wiarygodności i bezpieczeństwa systemów przetwarzających informacje, ładu korporacyjnego i zarządzania IT w przedsiębiorstwach, a także zarządzania ryzykiem i zapewnienia zgodności z przepisami prawa w obszarze IT. ISACA organizuje także społeczność osób zainteresowanych tymi zagadnieniami. Założona w 1969 roku niezależna organizacja non-profit ISACA jest gospodarzem międzynarodowych konferencji, wydaje periodyk *ISACA® Journal* oraz opracowuje międzynarodowe normy audytu i kontroli systemów przetwarzających informacje, które pomagają członkom w budowaniu zaufania do systemów informatycznych i uzyskiwaniu z nich wartości. Stowarzyszenie przyczynia się do podnoszenia wiedzy i rozwoju umiejętności z dziedziny IT oraz poświadcza je poprzez przyznawanie liczących się na całym świecie certyfikatów — audytora systemów informatycznych (Certified Information Systems Auditor® (CISA®), certyfikowanego kierownika ds. bezpieczeństwa informacji Certified Information Security Manager® — CISM®), certyfikowanego specjalisty w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie (Certified in the Governance of Enterprise IT® — CGEIT®) oraz certyfikowanego specjalisty w zakresie ryzyka i kontroli systemów informatycznych (Certified in Risk and Information Systems Control™ — CRISC™). ISACA nieustannie aktualizuje metodykę COBIT®, adresowaną do specjalistów IT i menedżerów przedsiębiorstw odpowiedzialnych za nadzór nad IT i zarządzanie IT — w szczególności w dziedzinach audytu, bezpieczeństwa, ryzyka, kontroli oraz generowania wartości biznesowej.

Disclaimer
ISACA has designed this publication, COBIT® 5 (the 'Work'), primarily as an educational rosource for governance of enterprise IT (GEIT), assurance, risk and security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure of test, security professionals should apply their own professional judgement to the specific circumstances presented by the particular systems of information technology environment.

Quality Statement
This Work is translated into Polish from the English language version of COBIT® 5 by the ISACA® Warsaw Chapter with the permission of ISACA®. The ISACA® Warsaw Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

Zastrzeżenie
ISACA opracowała i wydała niniejszy przewodnik COBIT 5 („Opracowanie") głównie jako publikację o charakterze edukacyjnym przeznaczoną dla specjalistów w dziedzinie nadzoru nad technologiami informatycznymi w przedsiębiorstwie (GEIT), audytu, ryzyka i bezpieczeństwa technologii informatycznych. ISACA nie gwarantuje, że zastosowanie się do jakichkolwiek wskazówek zawartych w Opracowaniu zapewni korzystne rezultaty. Nie należy zakładać, że Opracowanie zawiera wszystkie właściwe informacje, procedury i testy, które są odpowiednio ukierunkowane na uzyskanie takich samych rezultatów. Aby ustalić adekwatność określonych informacji, procedur lub testów zawartych w Opracowaniu, specjaliści ds. bezpieczeństwa powinni kierować się własną oceną specyficznych warunków działania konkretnych systemów lub środowisk IT.

Oświadczenie dotyczące jakości
Niniejsza publikacja została przełożona na język polski z anglojęzycznej wersji przewodnika COBIT 5 przez warszawski oddział ISACA (ISACA Warsaw Chapter) za zgodą ISACA. Za dokładność i wierność przekładu odpowiada wyłącznie warszawski oddział ISACA (ISACA Warsaw Chapter).

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 Stany Zjednoczone
Telefon: +1.847.253.1545
Faks: +1.847.253.1443
E-mail: *info@isaca.org*
Witryna internetowa: *www.isaca.org*

Prześlij informację zwrotną: *www.isaca.org/cobit*
Weź udział w Centrum Wiedzy ISACA (ang. Knowledge Center): *www.isaca.org/knowledge-center*
Śledź informacje o stowarzyszeniu ISACA w serwisie Twitter: *https://twitter.com/ISACANews*
Dołącz do dyskusji o metodyce COBIT w serwisie Twitter: #COBIT
Dołącz do ISACA w serwisie LinkedIn: ISACA (strona oficjalna), *http://linkd.in/ISACAOfficial*
Polub profil ISACA na Facebooku: *www.facebook.com/ISACAHQ*

COBIT® 5
ISBN 978-1-60420-514-5
8

Podziękowania

ISACA pragnie złożyć podziękowania następującym osobom i instytucjom:

Grupa robocza COBIT 5 (2009–2011)
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Global Business Services, Stany Zjednoczone, Współprzewodniczący
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MInstISP,
Ravenswood Consultants Ltd., Wielka Brytania, Współprzewodniczący
Pippa G. Andrews, CISA, ACA, CIA, KPMG, Australia
Elisabeth Judit Antonsson, CISM, Nordea Bank, Szwecja
Steven A. Babb, CGEIT, CRISC, Betfair, Wielka Brytania
Steven De Haes, Ph.D., University of Antwerp Management School, Belgia
Peter Harrison, CGEIT, FCPA, IBM Australia Ltd., Australia
Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria
Robert D. Johnson, CISA, CISM, CGEIT, CRISC, CISSP, Bank of America, Stany Zjednoczone
Erik H.J.M. Pols, CISA, CISM, Shell International-ITCI, Holandia
Vernon Richard Poole, CISM, CGEIT, Sapphire, Wielka Brytania
Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq & Associates, Indie

Zespół autorów
Floris Ampe, CISA, CGEIT, CIA, ISO 27000, PwC, Belgia
Gert du Preez, CGEIT, PwC, Kanada
Stefanie Grijp, PwC, Belgia
Gary Hardy, CGEIT, IT Winners, Republika Południowej Afryki
Bart Peeters, PwC, Belgia
Geert Poels, Ghent University, Belgia
Dirk Steuperaert, CISA, CGEIT, CRISC, IT In Balance BVBA, Belgia

Uczestnicy warsztatów
Gary Baker, CGEIT, CA, Kanada
Brian Barnier, CGEIT, CRISC, ValueBridge Advisors, Stany Zjednoczone
Johannes Hendrik Botha, MBCS-CITP, FSM, getITright Skills Development, Republika Południowej Afryki
Ken Buechler, CGEIT, CRISC, PMP, Great-West Life, Kanada
Don Caniglia, CISA, CISM, CGEIT, FLMI, Stany Zjednoczone
Mark Chaplin, Wielka Brytania
Roger Debreceny, Ph.D., CGEIT, FCPA, University of Hawaii at Manoa, Stany Zjednoczone
Mike Donahue, CISA, CISM, CGEIT, CFE, CGFM, CICA, Towson University, Stany Zjednoczone
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Szwajcaria
Bob Frelinger, CISA, CGEIT, Oracle Corporation, Stany Zjednoczone
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, Stany Zjednoczone
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, Stany Zjednoczone
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Nicole Lanza, CGEIT, IBM, Stany Zjednoczone
Philip Le Grand, PRINCE2, Ideagen Plc, Wielka Brytania
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, Stany Zjednoczone
Stuart MacGregor, Real IRM Solutions (Pty) Ltd., Republika Południowej Afryki
Christian Nissen, CISM, CGEIT, FSM, CFN People, Dania
Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, Wielka Brytania
Eddy J. Schuermans, CGEIT, ESRAS bvba, Belgia
Michael Semrau, RWE Germany, Niemcy
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Australia
Alan Simmonds, TOGAF9, TCSA, PreterLex, Wielka Brytania
Cathie Skoog, CISM, CGEIT, CRISC, IBM, Stany Zjednoczone
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Kanada
Roger Southgate, CISA, CISM, Wielka Brytania
Nicky Tiesenga, CISA, CISM, CGEIT, CRISC, IBM, Stany Zjednoczone
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgia
Greet Volders, CGEIT, Voquals N.V., Belgia
Christopher Wilken, CISA, CGEIT, PwC, Stany Zjednoczone
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, Wielka Brytania

Podziękowania (*ciąg dalszy*)

Recenzenci
Mark Adler, CISA, CISM, CGEIT, CRISC, Commercial Metals Company, Stany Zjednoczone
Wole Akpose, Ph.D., CGEIT, CISSP, Morgan State University, Stany Zjednoczone
Krzysztof Baczkiewicz, CSAM, CSOX, Eracent, Polska
Roland Bah, CISA, MTN Cameroon, Kamerun
Dave Barnett, CISSP, CSSLP, Stany Zjednoczone
Max Blecher, CGEIT, Virtual Alliance, Republika Południowej Afryki
Ricardo Bria, CISA, CGEIT, CRISC, Meycor GRC, Argentyna
Dirk Bruyndonckx, CISA, CISM, CGEIT, CRISC, MCA, KPMG Advisory, Belgia
Donna Cardall, Wielka Brytania
Debra Chiplin, Investors Group, Kanada
Sara Cosentino, CA, Great-West Life, Kanada
Kamal N. Dave, CISA, CISM, CGEIT, Hewlett Packard, Stany Zjednoczone
Philip de Picker, CISA, MCA, National Bank of Belgium, Belgia
Abe Deleon, CISA, IBM, Stany Zjednoczone
Stephen Doyle, CISA, CGEIT, Department of Human Services, Australia
Heidi L. Erchinger, CISA, CRISC, CISSP, System Security Solutions, Inc., Stany Zjednoczone
Rafael Fabius, CISA, CRISC, Urugwaj
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Szwajcaria
Bob Frelinger, CISA, CGEIT, Oracle Corporation, Stany Zjednoczone
Yalcin Gerek, CISA, CGEIT, CRISC, ITIL Expert, ITIL V3 Trainer, PRINCE2, ISO/IEC 20000 Consultant, Turcja
Edson Gin, CISA, CISM, CFE, CIPP, SSCP, Stany Zjednoczone
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, Stany Zjednoczone
Marcelo Hector Gonzalez, CISA, CRISC, Banco Central Republic Argentina, Argentyna
Erik Guldentops, University of Antwerp Management School, Belgia
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, Stany Zjednoczone
Angelica Haverblad, CGEIT, CRISC, ITIL, Verizon Business, Szwecja
Kim Haverblad, CISM, CRISC, PCI QSA, Verizon Business, Szwecja
J. Winston Hayden, CISA, CISM, CGEIT, CRISC, Republika Południowej Afryki
Eduardo Hernandez, ITIL V3, HEME Consultores, Meksyk
Jorge Hidalgo, CISA, CISM, CGEIT, ATC, Lic. Sistemas, Argentyna
Michelle Hoben, Media 24, Republika Południowej Afryki
Linda Horosko, Great-West Life, Kanada
Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants, Wielka Brytania
Grant Irvine, Great-West Life, Kanada
Monica Jain, CGEIT, CSQA, CSSBB, Southern California Edison, Stany Zjednoczone
John E. Jasinski, CISA, CGEIT, SSBB, ITIL Expert, Stany Zjednoczone
Masatoshi Kajimoto, CISA, CRISC, Japonia
Joanna Karczewska, CISA, Polska
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Arabia Saudyjska
Eddy Khoo S.K., Prudential Services Asia, Malezja
Marty King, CISA, CGEIT, CPA, Blue Cross Blue Shield NC, Stany Zjednoczone
Alan S. Koch, ITIL Expert, PMP, ASK Process Inc., Stany Zjednoczone
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Jason D. Lannen, CISA, CISM, TurnKey IT Solutions, LLC, Stany Zjednoczone
Nicole Lanza, CGEIT, IBM, Stany Zjednoczone
Philip Le Grand, PRINCE2, Ideagen Plc, Wielka Brytania
Kenny Lee, CISA, CISM, CISSP, Bank of America, Stany Zjednoczone
Brian Lind, CISA, CISM, CRISC, Topdanmark Forsikring A/S, Dania
Bjarne Lonberg, CISSP, ITIL, A.P. Moller-Maersk, Dania
Stuart MacGregor, Real IRM Solutions (Pty) Ltd., Republika Południowej Afryki
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, Stany Zjednoczone
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, Wielka Brytania
Cindy Marcello, CISA, CPA, FLMI, Great-West Life & Annuity, Stany Zjednoczone
Nancy McCuaig, CISSP, Great-West Life, Kanada
John A. Mitchell, Ph.D., CISA, CGEIT, CEng, CFE, CITP, FBCS, FCIIA, QiCA, LHS Business Control, Wielka Brytania
Makoto Miyazaki, CISA, CPA, Bank of Tokyo-Mitsubishi, UFJ Ltd., Japonia
Lucio Augusto Molina Focazzio, CISA, CISM, CRISC, ITIL, niezależny konsultant, Kolumbia

Podziękowania *(ciąg dalszy)*

Recenzenci *(ciąg dalszy)*
Christian Nissen, CISM, CGEIT, FSM, ITIL Expert, CFN People, Dania
Tony Noblett, CISA, CISM, CGEIT, CISSP, Stany Zjednoczone
Ernest Pages, CISA, CGEIT, MCSE, ITIL, Sciens Consulting LLC, Stany Zjednoczone
Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, Wielka Brytania
Tom Patterson, CISA, CGEIT, CRISC, CPA, IBM, Stany Zjednoczone
Robert Payne, CGEIT, MBL, MCSSA, PrM, Lode Star Strategy Consulting, Republika Południowej Afryki
Andy Piper, CISA, CISM, CRISC, PRINCE2, ITIL, Barclays Bank Plc, Wielka Brytania
Andre Pitkowski, CGEIT, CRISC, OCTAVE, ISO27000LA, ISO31000LA, APIT Consultoria de Informatica Ltd., Brazylia
Dirk Reimers, Hewlett-Packard, Niemcy
Steve Reznik, CISA, ADP Inc., Stany Zjednoczone
Robert Riley, CISSP, University of Notre Dame, Stany Zjednoczone
Martin Rosenberg, Ph.D., Cloud Governance Ltd., Wielka Brytania
Claus Rosenquist, CISA, CISSP, Nets Holding, Dania
Jeffrey Roth, CISA, CGEIT, CISSP, L-3 Communications, Stany Zjednoczone
Cheryl Santor, CISSP, CNA, CNE, Metropolitan Water District, Stany Zjednoczone
Eddy J. Schuermans, CGEIT, ESRAS bvba, Belgia
Michael Semrau, RWE Germany, Niemcy
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Australia
Alan Simmonds, TOGAF9, TCSA, PreterLex, Wielka Brytania
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Kanada
Jennifer Smith, CISA, CIA, Salt River Pima Maricopa Indian Community, Stany Zjednoczone
Marcel Sorouni, CISA, CISM, CISSP, ITIL, CCNA, MCDBA, MCSE, Bupa Australia, Australia
Roger Southgate, CISA, CISM, Wielka Brytania
Mark Stacey, CISA, FCA, BG Group Plc, Wielka Brytania
Karen Stafford Gustin, MLIS, London Life Insurance Company, Kanada
Delton Sylvester, Silver Star IT Governance Consulting, Republika Południowej Afryki
Katalin Szenes, CISA, CISM, CGEIT, CISSP, University Obuda, Węgry
Halina Tabacek, CGEIT, Oracle Americas, Stany Zjednoczone
Nancy Thompson, CISA, CISM, CGEIT, IBM, Stany Zjednoczone
Kazuhiro Uehara, CISA, CGEIT, CIA, Hitachi Consulting Co., Ltd., Japonia
Rob van der Burg, Microsoft, Holandia
Johan van Grieken, CISA, CGEIT, CRISC, Deloitte, Belgia
Flip van Schalkwyk, Centre for e-Innovation, Western Cape Government, Republika Południowej Afryki
Jinu Varghese, CISA, CISSP, ITIL, OCA, Ernst & Young, Kanada
Andre Viviers, MCSE, IT Project+, Media 24, Republika Południowej Afryki
Greet Volders, CGEIT, Voquals N.V., Belgia
David Williams, CISA, Westpac, Nowa Zelandia
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, Wielka Brytania
Amanda Xu, PMP, Southern California Edison, Stany Zjednoczone
Tichaona Zororo, CISA, CISM, CGEIT, Standard Bank, Republika Południowej Afryki

Recenzenci przekładu na język polski
Adam Rafajeński, CISA, CISM, CGEIT, CRISC, Polska
Michał Jobski, CGEIT, COBIT5 Implementation, ITIL Expert, Polska
Łukasz Nowak, Łukasz Nowak, PMP, PMI-ACP, Public Consulting Group, Polska
Paweł Gula, Polska
Piotr Dzwonkowski,CISA, CISM, CRISC, LINKIES. Management Consulting Polska, Polska

Zarząd ISACA
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (obecnie na emeryturze), Stany Zjednoczone, Międzynarodowy Przewodniczący
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grecja, Wiceprzewodniczący
Gregory T. Grocholski, CISA, The Dow Chemical Co., Stany Zjednoczone, Wiceprzewodniczący
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, rząd stanu Queensland, Australia, Wiceprzewodniczący
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., Indie, Wiceprzewodniczący
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., Stany Zjednoczone, Wiceprzewodniczący

Podziękowania (*ciąg dalszy*)

Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Wiceprzewodnicząca
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (obecnie na emeryturze), Stany Zjednoczone, były Międzynarodowy Przewodniczący
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Federacja Rosyjska, była Międzynarodowa Przewodnicząca
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, Wielka Brytania, Dyrektor
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgia, Dyrektor

Panel wiedzy
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgia, Przewodniczący
Michael A. Berardi Jr., CISA, CGEIT, Bank of America, Stany Zjednoczone
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapur
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, Stany Zjednoczone
Jon Singleton, CISA, FCA, Auditor General of Manitoba (obecnie na emeryturze), Kanada
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, Francja

Komitet metodyki (2009–2012)
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, Francja, Przewodniczący
Georges Ataya, CISA, CISM, CGEIT, CRISC, CISSP, Solvay Brussels School of Economics and Management, Belgia, były Wiceprezes
Steven A. Babb, CGEIT, CRISC, Betfair, Wielka Brytania
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapur
Sergio Fleginsky, CISA, Akzo Nobel, Urugwaj
John W. Lainhart IV, CISA, CISM, CGEIT, CRISC, IBM Global Business Services, Stany Zjednoczone
Mario C. Micallef, CGEIT, CPAA, FIA, Malta
Anthony P. Noble, CISA, CCP, Viacom, Stany Zjednoczone
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., Wielka Brytania
Robert G. Parker, CISA, CA, CMC, FCA, Deloitte & Touche LLP (obecnie na emeryturze), Kanada
Rolf M. von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, Forfa AG, Szwajcaria
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia
Robert E. Stroud, CGEIT, CA Inc., Stany Zjednoczone

Specjalne wyróżnienie
ISACA Los Angeles Chapter za wsparcie finansowe

Jednostki powiązane i sponsorzy **ISACA oraz IT Governance Institute® (ITGI®)**
Amerykański Instytut Biegłych Rewidentów
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Institute of Management Accountants Inc.
Oddziały ISACA
ITGI France
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

Enterprise GRC Solutions Inc.
Hewlett-Packard
IBM
Symantec Corp.

Spis treści

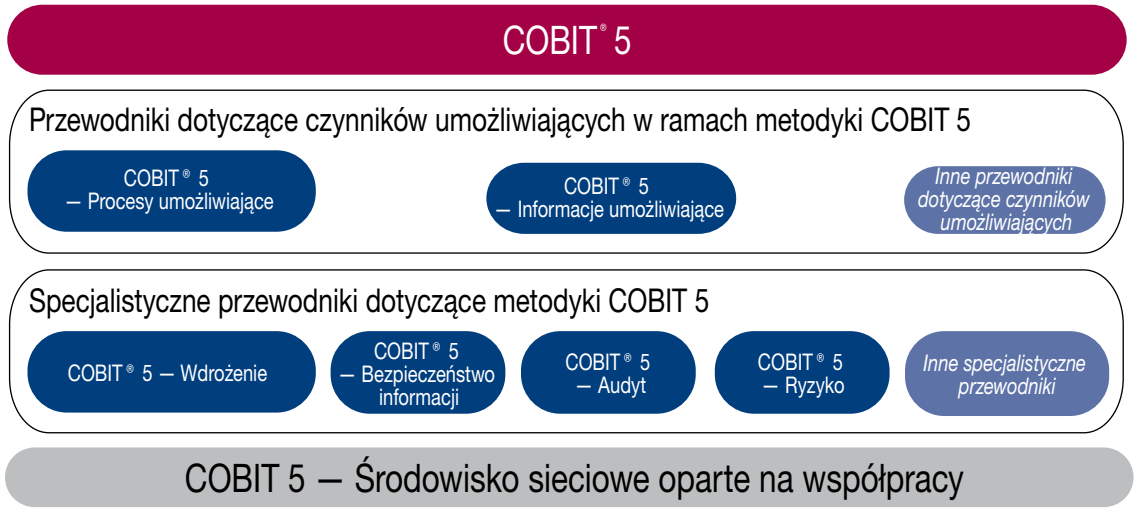
Spis ilustracji

Strona celowo pozostawiona pusta

COBIT 5: Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi

Publikacja COBIT 5 zawiera opis metodyki COBIT 5 w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi. Publikacja jest częścią rodziny produktów COBIT 5 przedstawionych na **ilustracji 1**.

Ilustracja 1 — Rodzina produktów COBIT 5



Metodyka COBIT 5 jest oparta na pięciu podstawowych, szczegółowo omówionych zasadach i obejmuje rozbudowane wytyczne dotyczące czynników umożliwiających w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi.

Rodzina produktów COBIT 5 obejmuje następujące elementy:
- COBIT 5 (metodyka);
- przewodniki dotyczące czynników umożliwiających COBIT 5, w których szczegółowo opisano czynniki związane z nadzorem i zarządzaniem. Należą do nich:
  - *COBIT 5: procesy umożliwiające*
  - *COBIT 5: informacje umożliwiające*
  - pozostałe przewodniki dotyczące czynników umożliwiających (*www.isaca.org/cobit*);
- specjalistyczne przewodniki COBIT 5, w tym:
  - *COBIT 5 — Wdrożenie*;
  - *COBIT 5 — Bezpieczeństwo informacji*;
  - *COBIT 5 — Audyt*;
  - *COBIT 5 — Ryzyko*;
  - inne specjalistyczne przewodniki (zob. *www.isaca.org/cobit*);
- środowisko współpracy sieciowej, które będzie wspierać korzystanie z metodyki COBIT 5.

Strona celowo pozostawiona pusta

Streszczenie dla kierownictwa

Informacje stanowią kluczowy zasób dla wszystkich przedsiębiorstw, a od chwili utworzenia informacji aż do momentu ich zniszczenia istotną rolę odgrywa technologia. Stopień zaawansowania technologii informatycznych powszechnie wykorzystywanych w przedsiębiorstwach, a także w otoczeniu społecznym, publicznym i biznesowym, stale rośnie.

W rezultacie obecnie w stopniu większym niż dotąd przedsiębiorstwa oraz ich zarządy dążą do:
- Utrzymania wysokiej jakości informacji w celu wspierania procesu podejmowania decyzji biznesowych.
- Generowania wartości biznesowej z inwestycji wspieranych przez IT, tj. osiągania celów strategicznych oraz realizacji korzyści biznesowych dzięki efektywnemu i innowacyjnemu wykorzystaniu technologii informatycznych.
- Osiągnięcia sprawności operacyjnej dzięki niezawodnemu i efektywnemu wykorzystaniu technologii.
- Utrzymania ryzyka związanego z IT na akceptowalnym poziomie.
- Optymalizacji kosztu usług oraz technologii IT.
- Zapewnienia zgodności z coraz bardziej złożonymi obowiązującymi przepisami, regulacjami, zobowiązaniami umownymi oraz politykami.

W ciągu ostatnich dziesięciu lat termin „nadzór” zaczął się cieszyć wielką popularnością wśród osób odpowiedzialnych za działalność biznesową w związku z przykładami potwierdzającymi istotną rolę dobrego nadzoru oraz przypadkami nieudanych przedsięwzięć w świecie biznesu.

Odnoszące sukcesy przedsiębiorstwa zdały sobie sprawę z faktu, że zarząd i kadra kierownicza muszą traktować IT jako jeden z istotnych elementów prowadzenia działalności. Członkowie zarządów i kadry kierowniczej (zarówno w ramach funkcji biznesowej, jak i funkcji IT) — muszą działać wspólnie, tak aby technologie informatyczne były częścią podejścia do zarządzania i nadzoru. Ponadto spełnieniu tych wymogów sprzyja tworzone obecnie prawodawstwo oraz wdrażane regulacje.

COBIT 5 stanowi kompleksową metodykę ułatwiającą przedsiębiorstwom osiągnięcie założonych celów w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi. Krótko mówiąc, metodyka COBIT 5 ułatwia przedsiębiorstwom uzyskanie optymalnej wartości z IT poprzez zachowanie równowagi między osiąganiem korzyści a optymalizacją poziomu ryzyka oraz wykorzystania zasobów. Metodyka COBIT 5 umożliwia nadzór nad technologiami informatycznymi i zarządzanie nimi w sposób całościowy, w odniesieniu do wszystkich aspektów działania przedsiębiorstwa, z uwzględnieniem pełnych, kompleksowych obszarów funkcjonalnych odpowiedzialności w zakresie działalności biznesowej oraz IT, a także związanych z IT interesów interesariuszy wewnętrznych i zewnętrznych. Metodyka COBIT 5 ma charakter ogólny i może zostać z powodzeniem wykorzystana w przedsiębiorstwach każdej wielkości, niezależnie od tego, czy mają charakter komercyjny, działają na zasadach not-for-profit, czy też należą do sektora publicznego.

Ilustracja 2 — Zasady metodyki COBIT 5

Metodyka COBIT 5 jest oparta na pięciu podstawowych zasadach (przedstawionych na **ilustracji 2**) dotyczących nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi:

- **Zasada 1: Spełnienie potrzeb interesariuszy** — istotą działania przedsiębiorstw jest tworzenie wartości dla interesariuszy poprzez zachowanie równowagi między realizacją korzyści, optymalizacją ryzyka i wykorzystaniem zasobów. Metodyka COBIT 5 uwzględnia wszystkie wymagane procesy oraz inne czynniki umożliwiające, które wspierają tworzenie wartości biznesowej dzięki wykorzystaniu IT. Ponieważ każde przedsiębiorstwo ma inne cele, istnieje możliwość dostosowania metodyki COBIT 5 tak, aby pasowała do kontekstu danej organizacji. Polega to na wykorzystaniu kaskady celów, tj. przełożeniu wysokiego poziomu celów przedsiębiorstwa na możliwe do zarządzania, konkretne cele związane z IT i odwzorowanie celów IT w ramach określonych celów czynników umożliwiających.
- **Zasada 2: Uwzględnienie wszystkich aspektów działania przedsiębiorstwa** — w metodyce COBIT 5 nadzór nad technologiami informatycznymi w przedsiębiorstwie jest częścią ładu korporacyjnego:
  - Obejmuje wszystkie funkcje i procesy realizowane w przedsiębiorstwie; metodyka COBIT 5 nie koncentruje się tylko na funkcji IT, ale traktuje informacje i związane z nimi technologie jako aktywa wymagające uwzględnienia — podobnie jak wszelkie inne zasoby — przez wszystkich pracowników przedsiębiorstwa.
  - Przyjęto założenie, że wszystkie czynniki umożliwiające dotyczące nadzoru nad systemami informatycznymi i zarządzania nimi są ogólnofirmowe i mają charakter kompleksowy, tj. obejmują wszystkich i wszystko — wewnątrz przedsiębiorstwa i poza nim — co jest istotne dla nadzoru nad zasobami informacyjnymi w przedsiębiorstwie i powiązanymi systemami IT oraz zarządzania nimi.
- **Zasada 3: Stosowanie jednej zintegrowanej metodyki** — istnieje wiele standardów i dobrych praktyk związanych z IT, obejmujących wytyczne dotyczące poszczególnych zbiorów działań IT. Na poziomie ogólnym metodyka COBIT 5 jest spójna z innymi stosownymi standardami i metodykami. W związku z tym może ona stanowić nadrzędną strukturę nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi.
- **Zasada 4: Wdrożenie podejścia całościowego** — skuteczny nadzór nad technologiami informatycznymi oraz wydajne zarządzanie nimi w przedsiębiorstwie wymagają przyjęcia całościowego podejścia uwzględniającego wiele wzajemnie oddziałujących na siebie komponentów. Metodyka COBIT 5 definiuje zbiór czynników umożliwiających, które wspierają wdrożenie kompleksowego systemu nadzoru i zarządzania dla technologii informatycznych w przedsiębiorstwie. Czynnik umożliwiający to pojęcie bardzo szerokie — obejmuje wszystko, co może ułatwić osiągnięcie celów przedsiębiorstwa: W metodyce COBIT 5 zdefiniowano siedem kategorii czynników umożliwiających:
  - Zasady, polityki i metodyki;
  - Procesy;
  - Struktury organizacyjne;
  - Kultura, etyka i zachowanie;
  - Informacja;
  - Usługi, infrastruktura i aplikacje;
  - Ludzie, umiejętności i kompetencje.
- **Zasada 5: Oddzielenie nadzoru od zarządzania** — w metodyce COBIT 5 wyraźnie rozróżnia się nadzór i zarządzanie. Każda z tych dziedzin obejmuje działania o odmiennym charakterze, wymaga różnych struktur organizacyjnych i służy innym celom. To kluczowe rozróżnienie nadzoru i zarządzania ujęto w metodyce COBIT 5 w następujący sposób:
  - Nadzór

    Dzięki nadzorowi zyskuje się pewność, że oceniono potrzeby, warunki i opcje interesariuszy w celu ustalenia zrównoważonych, uzgodnionych celów przedsiębiorstwa, które mają zostać osiągnięte. Nadzór polega również na ukierunkowaniu działań poprzez nadanie priorytetów i podejmowanie decyzji, a także na monitorowaniu sprawności i zgodności w odniesieniu do uzgodnionego kierunku i szczegółowych celów.

    W większości przedsiębiorstw za nadzór odpowiada zarząd pod przywództwem prezesa. Poszczególne obowiązki w zakresie nadzoru mogą zostać przekazane specjalnym strukturom organizacyjnym na właściwym poziomie, szczególnie w większych, złożonych przedsiębiorstwach.

  - Zarządzanie

    Zarządzanie polega na planowaniu, budowaniu, realizacji i monitorowaniu działań w sposób spójny z kierunkiem wskazanym przez organ nadzorujący, aby osiągnąć cele przedsiębiorstwa.

    W większości przedsiębiorstw za zarządzanie odpowiada kadra zarządzająca pod przywództwem dyrektora generalnego (CEO).

Owe pięć zasad łącznie umożliwia przedsiębiorstwu stworzenie skutecznej metodyki nadzoru i zarządzania, która zapewnia optymalizację inwestycji w informacje i technologię oraz ich wykorzystanie z korzyścią dla interesariuszy.

Rozdział 1
Przegląd metodyki COBIT 5

Metodyka COBIT 5 zawiera najnowsze wytyczne ISACA dotyczące nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi. Wykorzystano w niej ponad 15 lat doświadczeń wielu przedsiębiorstw i użytkowników korzystających z metodyki COBIT, reprezentujących społeczności zajmujące się działalnością biznesową, technologiami informatycznymi, ryzykiem, bezpieczeństwem oraz audytem. Najważniejsze wyznaczniki rozwoju metodyki COBIT 5 obejmują konieczność:

- Zapewnienia większej liczbie interesariuszy wpływu na określenie ich oczekiwań w stosunku do informacji i powiązanej technologii (jakie korzyści przy jakim akceptowalnym poziomie ryzyka i jakim kosztem) oraz ich priorytetów w odniesieniu do rzeczywistego osiągnięcia oczekiwanej wartości. Niektórzy są zainteresowani uzyskaniem szybkiego zwrotu z inwestycji, inni zaś większy nacisk kładą na zrównoważony rozwój w perspektywie długoterminowej. Niektórzy są skłonni do podejmowania wysokiego ryzyka, inni nie. Te rozbieżne — a niekiedy sprzeczne — oczekiwania muszą zostać uwzględnione w sposób efektywny. Co więcej, interesariusze nie tylko chcą uzyskać większy wpływ, lecz także oczekują większej przejrzystości w odniesieniu do sposobu realizacji działań oraz osiągniętych efektów.
- Uwzględnienia coraz większego uzależnienia sukcesu przedsiębiorstwa od stron zewnętrznych (zajmujących się zarówno działalnością biznesową, jak i IT), takich jak podmioty świadczące usługi w ramach outsourcingu, dostawcy, konsultanci, klienci, podmioty świadczące usługi w chmurze oraz inni dostawcy usług, a także od wielu różnych wewnętrznych środków i mechanizmów umożliwiających uzyskanie spodziewanej wartości.
- Obsługi znacznie większej ilości informacji. W jaki sposób przedsiębiorstwa dokonują wyboru istotnych i wiarygodnych informacji, które zapewnią skuteczność i wydajność procesu podejmowania decyzji biznesowych? Konieczne jest również wydajne zarządzanie informacjami. Może w tym pomóc efektywny model informacji.
- Korzystania z dużo powszechniej dostępnych technologii informatycznych, w coraz większym stopniu stanowiących integralny element działalności biznesowej. Oddzielenie IT od działalności biznesowej (nawet jeśli zadbano o odpowiednie dopasowanie) nie jest już optymalnym rozwiązaniem. Technologie informatyczne muszą być integralną częścią projektów biznesowych, struktur organizacyjnych, zarządzania ryzykiem, polityk, umiejętności, procesów itd. Role dyrektora ds. informatyki (CIO) oraz funkcji IT ewoluują. Coraz większa liczba osób pełniących funkcje biznesowe posiada umiejętności w zakresie IT i jest (lub będzie) zaangażowana w podejmowanie decyzji związanych z IT oraz realizację operacji IT. Konieczna jest lepsza integracja funkcji biznesowej oraz IT.
- Zapewnienia dodatkowych wytycznych w obszarze innowacji oraz nowo powstających technologii; dotyczą one kreatywności, pomysłowości, rozwoju nowych produktów oraz zwiększenia atrakcyjności obecnych produktów w oczach klientów, a także dotarcia do nowych typów klientów. Innowacyjność oznacza również usprawnienie rozwoju produktów, procesu produkcji oraz łańcucha dostaw z myślą o szybszym i bardziej efektywnym dostarczaniu na rynek produktów o wyższej jakości.
- Uwzględnienia pełnego zakresu odpowiedzialności funkcji biznesowej oraz IT, a także wszystkich aspektów umożliwiających efektywny nadzór nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi, takich jak struktury organizacyjne, polityki i kultura, a także procesy.
- Uzyskania większej kontroli nad coraz powszechniej wykorzystywanymi rozwiązaniami IT inicjowanymi i kontrolowanymi przez użytkowników.
- Zapewnienia (w ramach przedsiębiorstwa):
  - Tworzenia wartości dzięki efektywnemu i innowacyjnemu wykorzystaniu technologii informatycznych w przedsiębiorstwie;
  - Zadowolenia użytkowników biznesowych z zaangażowania IT i świadczonych przez ten dział usług;
  - Zgodności z obowiązującymi przepisami, regulacjami, zobowiązaniami umownymi oraz politykami wewnętrznymi;
  - Lepszych relacji między potrzebami biznesowymi oraz celami IT.
- Powiązania z innymi najważniejszymi metodykami i standardami na rynku oraz — w odpowiednich wypadkach — dopasowania do nich. Dotyczy to między innymi takich standardów i metodyk jak Information Technology Infrastructure Library (ITIL®), The Open Group Architecture Forum (TOGAF®), Project Management Body of Knowledge (PMBOK®), PRojects IN Controlled Environments 2 (PRINCE2®), metodyka opracowana przez Komitet Organizacji Sponsorujących Komisję Treadwaya (COSO) oraz normy ISO (Międzynarodowa Organizacja Normalizacyjna). To ułatwi interesariuszom zrozumienie wzajemnych powiązań między różnymi metodykami, dobrymi praktykami i normami oraz sposobu, w jaki można je wykorzystać.
- Połączenia wszystkich najważniejszych metodyk i wytycznych ISACA, w szczególności COBIT, Val IT oraz Risk IT, lecz także z uwzględnieniem Business Model for Information Security (BMIS — model biznesowy dotyczący bezpieczeństwa informacji), IT Assurance Framework (ITAF), publikacji zatytułowanej *Board Briefing on IT Governance* oraz zasobu Taking Governance Forward (TGF), tak aby metodyka COBIT 5 obejmowała całe przedsiębiorstwo i stanowiła podstawę umożliwiającą integrację innych metodyk, standardów i praktyk w ramach jednej struktury.

Różne produkty oraz inne wytyczne dotyczące odmiennych potrzeb różnych interesariuszy zostaną opracowane na podstawie głównej bazy wiedzy COBIT 5. W wyniku tego procesu z czasem architektura produktów COBIT 5 stanie się żywym dokumentem. Najnowszą architekturę produktów COBIT 5 można znaleźć na stronach COBIT witryny internetowej ISACA (*www.isaca.org/cobit*).

Przeglądowe informacje na temat niniejszej publikacji

Metodyka COBIT 5 zawiera jeszcze siedem rozdziałów:

- W rozdziale 2 omówiono zasadę 1, **Spełnienie potrzeb interesariuszy.** Wprowadzono w nim kaskadę celów COBIT 5. Cele przedsiębiorstwa dotyczące IT są wykorzystywane do sformalizowania i ustrukturyzowania potrzeb interesariuszy. Cele przedsiębiorstwa mogą zostać powiązane z celami związanymi z IT, a te ostatnie można zrealizować dzięki optymalnemu wykorzystaniu i realizacji wszystkich czynników umożliwiających (w tym procesów). Ten zbiór powiązanych celów jest nazywany kaskadą celów COBIT 5. W rozdziale przedstawiono również przykłady typowych pytań zadawanych przez interesariuszy, dotyczących nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi.
- W rozdziale 3 omówiono zasadę 2, **Uwzględnienie wszystkich aspektów działania przedsiębiorstwa.** Wyjaśniono sposób włączenia nadzoru nad technologiami informatycznymi w przedsiębiorstwie do ładu korporacyjnego w ramach metodyki COBIT 5 dzięki uwzględnieniu wszystkich funkcji i procesów realizowanych w przedsiębiorstwie.
- W rozdziale 4 omówiono zasadę 3, **Stosowanie jednej zintegrowanej metodyki**, i zwięźle opisano architekturę COBIT 5 umożliwiającą integrację.
- W rozdziale 5 omówiono zasadę 4, **Wdrożenie podejścia całościowego.** Nadzór nad technologiami informatycznymi w organizacji ma charakter systemowy i jest wspierany przez zbiór czynników umożliwiających. W tym rozdziale wprowadzono czynniki umożliwiające i standardowy sposób ich postrzegania: typowy model czynnika umożliwiającego.
- W rozdziale 6 omówiono zasadę 5, **Oddzielenie nadzoru od zarządzania**, i przedstawiono różnicę między nadzorem i zarządzaniem, a także ich wzajemne powiązania. Ogólny model referencyjny procesu COBIT 5 podano dla przykładu.
- Rozdział 7 zawiera wprowadzenie do **Wytycznych dotyczących wdrożenia**. Opisano w nim sposób, w jaki można utworzyć odpowiednie środowisko, wymagane czynniki umożliwiające, typowe punkty zapalne oraz zdarzenia inicjujące wdrożenie, a także cykl życia wdrożenia oraz ciągłego doskonalenia. Ten rozdział oparto na publikacji zatytułowanej *COBIT® 5 — Wdrożenie*, w której można znaleźć wszystkie szczegóły dotyczące sposobu wdrażania nadzoru nad technologiami informatycznymi w przedsiębiorstwie na podstawie metodyki COBIT 5.
- W rozdziale 8 omówiono **Model potencjału procesu COBIT 5** w ramach programu COBIT Assessment Programme (*www.isaca.org/cobit-assessment-programme*), różnice w stosunku do oceny dojrzałości procesu w ramach metodyki COBIT 4.1 oraz sposób, w jaki można migrować do najnowszej wersji metodyki.

W załącznikach zawarto informacje referencyjne, przyporządkowania oraz bardziej szczegółowe informacje dotyczące poszczególnych zagadnień:

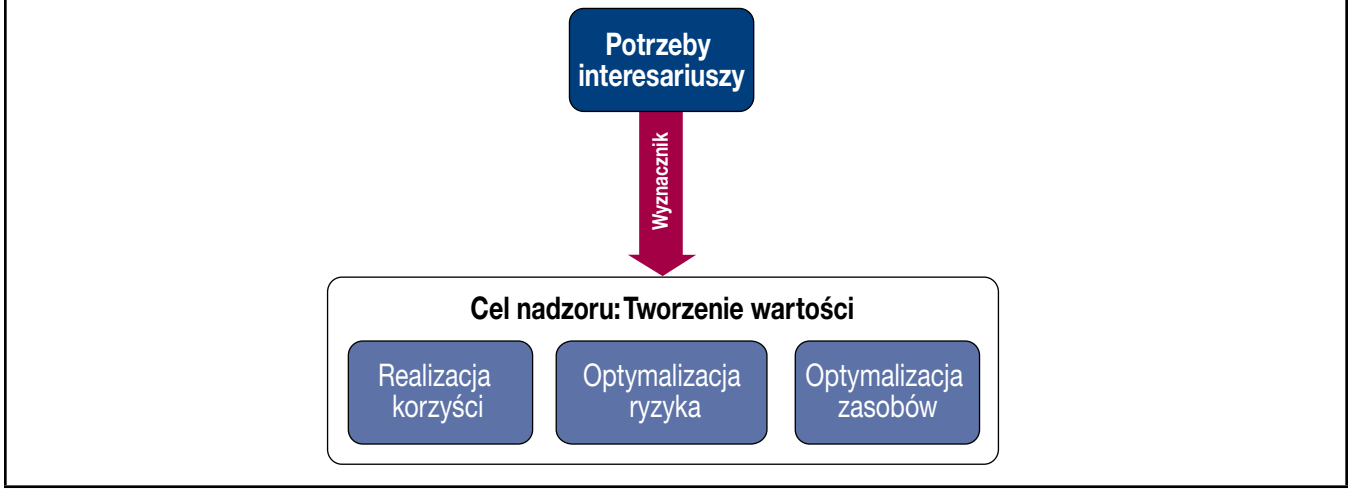
- W załączniku A. wymieniono **Materiały źródłowe** wykorzystane w trakcie prac nad metodyką COBIT 5.
- W załączniku B. **Szczegółowe mapowanie celów przedsiębiorstwa na cele związane z IT** opisano sposób, w jaki jeden lub kilka celów związanych z IT zazwyczaj wspiera realizację celów przedsiębiorstwa.
- W załączniku C. **Szczegółowe mapowanie celów związanych z IT na procesy związane z IT** opisano sposób, w jaki procesy COBIT ułatwiają osiągnięcie celów związanych z IT.
- W załączniku D. **Potrzeby interesariuszy oraz cele przedsiębiorstwa** opisano sposób, w jaki typowe potrzeby interesariuszy wiążą się z celami przedsiębiorstwa w ramach metodyki COBIT 5.
- Załącznik E. **Zestawienie metodyki COBIT 5 ze stosownymi powiązanymi standardami i metodykami**
- Załącznik F. **Porównanie modelu informacji według COBIT 5 z kryteriami informacji według COBIT 4.1**
- Załącznik G. **Szczegółowy opis czynników umożliwiających COBIT 5** jest oparty na rozdziale 5 i zawiera więcej szczegółowych informacji o różnych czynnikach umożliwiających, z uwzględnieniem szczegółowego modelu czynników umożliwiających opisującego poszczególne komponenty; opis poparto szeregiem przykładów.
- Załącznik H. **Terminologia**

Rozdział 2
Zasada 1: Spełnienie potrzeb interesariuszy

Wprowadzenie

Istotą funkcjonowania przedsiębiorstw jest tworzenie wartości dla interesariuszy. Oznacza to, że dla każdego przedsiębiorstwa — niezależnie od tego, czy prowadzi ono działalność komercyjną — jednym z celów w zakresie nadzoru jest tworzenie wartości. Tworzenie wartości oznacza osiąganie korzyści w sposób maksymalnie oszczędny pod względem wykorzystania zasobów i umożliwiający optymalizację ryzyka. (Zob. **ilustracja 3**.) Korzyści mogą przybierać wiele różnych postaci, np. w przypadku przedsiębiorstw komercyjnych mają charakter finansowy, zaś dla podmiotów rządowych są nimi usługi publiczne.

Ilustracja 3 — Cel nadzoru: Tworzenie Wartości



Przedsiębiorstwa mają wielu interesariuszy i dla każdego z nich „tworzenie wartości" oznacza różne — niekiedy wykluczające się — rzeczy. Nadzór polega na negocjowaniu i podejmowaniu decyzji dotyczących wartości istotnych dla różnych interesariuszy. Oznacza to, że przed podjęciem decyzji w zakresie oszacowania korzyści, ryzyka i zasobów system nadzoru powinien uwzględnić oczekiwania wszystkich interesariuszy. W przypadku każdej decyzji można i należy zadać następujące pytania: Kto odnosi korzyści? Kto ponosi ryzyko? Jakie zasoby są wymagane?

Kaskada celów COBIT 5

Każde przedsiębiorstwo działa w innym kontekście, zależnym od czynników zewnętrznych (rynek, branża, sytuacja geopolityczna itd.) oraz czynników wewnętrznych (kultura, organizacja, apetyt na ryzyko itd.) i wymagającym odpowiedniego dostosowania systemu nadzoru i zarządzania.

Potrzeby interesariuszy muszą zostać przekształcone w składającą się z konkretnych działań strategię przedsiębiorstwa. Kaskada celów COBIT 5 to mechanizm umożliwiający przełożenie potrzeb interesariuszy na określone, składające się z konkretnych działań i dostosowane cele przedsiębiorstwa, cele związane z IT oraz cele czynników umożliwiających. Tego rodzaju przełożenie umożliwia określenie konkretnych celów na każdym poziomie i w każdej dziedzinie przedsiębiorstwa z myślą o wspieraniu realizacji ogólnych celów i wymogów interesariuszy, co pozwala na skuteczne wspieranie dopasowania potrzeb przedsiębiorstwa oraz rozwiązań i usług IT.

Kaskadę celów COBIT 5 przedstawiono na **ilustracji 4**.

Krok 1. Wyznaczniki dotyczące interesariuszy wpływają na potrzeby interesariuszy

Na potrzeby interesariuszy wpływa wiele czynników, takich jak zmiany w strategii, zmiany w otoczeniu biznesowym i regulacyjnym oraz nowe technologie.

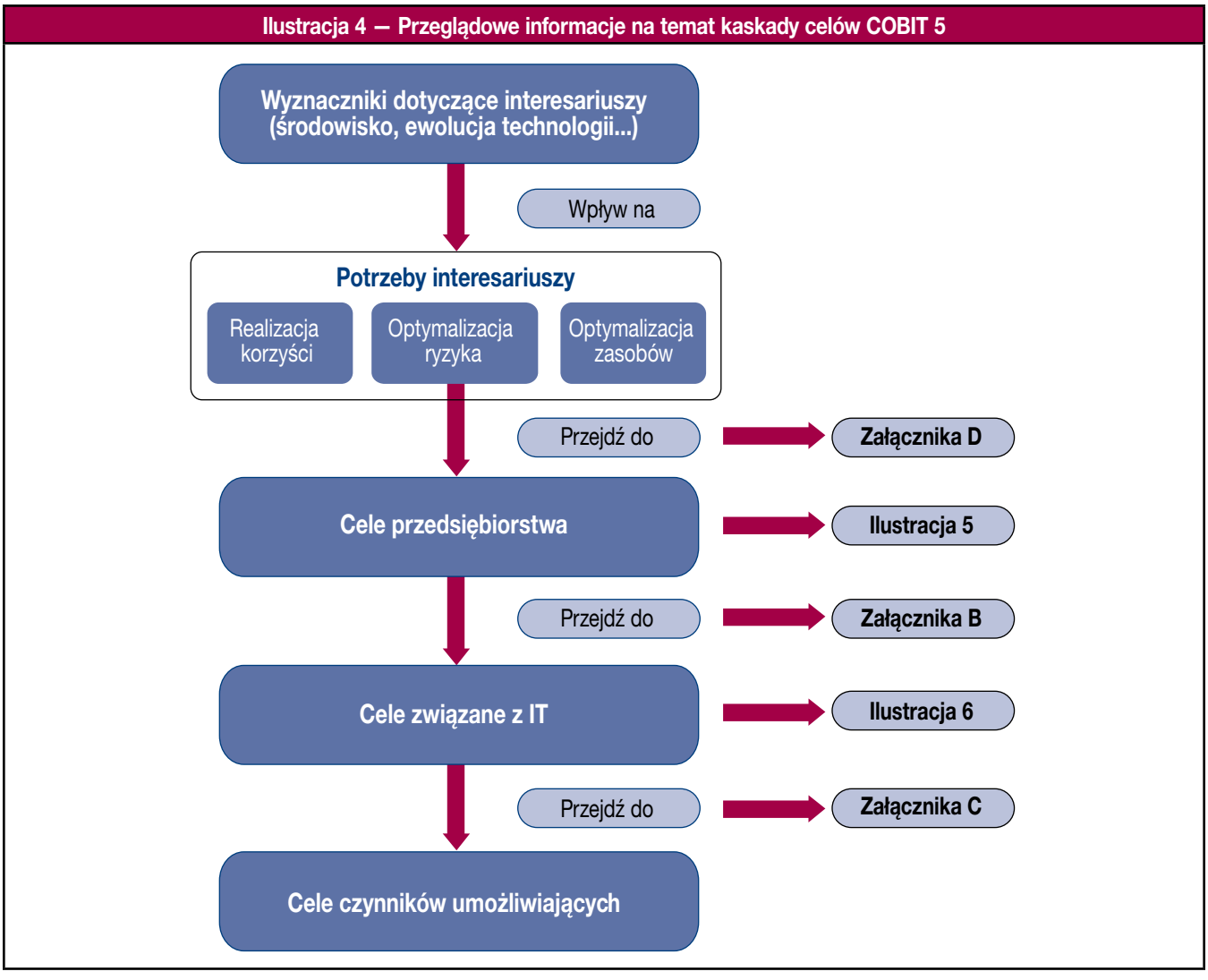
Krok 2. Kaskada potrzeb interesariuszy a cele przedsiębiorstwa

Potrzeby interesariuszy mogą być powiązane ze zbiorem typowych celów przedsiębiorstwa. Cele te zostały opracowane przy wykorzystaniu wymiarów zrównoważonej karty wyników (BSC)[1]. Stanowią one listę typowych celów definiowanych przez przedsiębiorstwo w odniesieniu do swojej działalności. Choć lista ta nie jest wyczerpująca,

[1] Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard: Translating Strategy Into Action*, Harvard University Press, USA, 1996

większość celów dotyczących konkretnego przedsiębiorstwa można łatwo przyporządkować do jednego lub kilku typowych celów przedsiębiorstwa. Tabela potrzeb interesariuszy oraz celów przedsiębiorstwa została przedstawiona w załączniku D.

Ilustracja 4 — Przeglądowe informacje na temat kaskady celów COBIT 5



W metodyce COBIT 5 zdefiniowano 17 typowych celów widocznych na **ilustracji 5**, na której przedstawiono następujące informacje:
- wymiar BSC, w którym mieści się dany cel przedsiębiorstwa;
- cele przedsiębiorstwa;
- związek z trzema głównymi celami w zakresie nadzoru — realizacją korzyści, optymalizacją ryzyka i optymalizacją zasobów (P oznacza relację podstawową, natomiast S — wspierającą, tj. słabszą).

Krok 3. Kaskada celów przedsiębiorstwa a cele związane z IT

Realizacja celów przedsiębiorstwa wymaga osiągnięcia pewnych rezultatów związanych z IT[2], reprezentowanych przez cele związane z IT. Związane z IT oznacza informacje i powiązaną technologię, natomiast cele związane z IT są ustrukturyzowane zgodnie z wymiarami zrównoważonej karty wyników IT (IT BSC). W metodyce COBIT 5 zdefiniowano 17 celów związanych z IT, przedstawionych na **ilustracji 6**.

Tabelę dotyczącą mapowania celów związanych z IT na cele przedsiębiorstwa przedstawiono w załączniku B. Zilustrowano w niej sposób, w jaki każdy z celów przedsiębiorstwa jest wspierany przez szereg celów związanych z IT.

Krok 4. Kaskada celów związanych z IT a cele czynników umożliwiających

Osiągnięcie celów związanych z IT wymaga skutecznego stosowania i wykorzystania kilku czynników umożliwiających. Koncepcja czynnika umożliwiającego została szczegółowo opisana w rozdziale 5. Czynniki umożliwiające obejmują procesy, struktury organizacyjne oraz informacje, a dla każdego czynnika umożliwiającego można zdefiniować zbiór konkretnych istotnych celów wspierających realizację celów związanych z IT.

[2] Wyniki związane z IT nie są oczywiście jedynymi pośrednimi korzyściami wymaganymi do osiągnięcia celów przedsiębiorstwa. Wszystkie inne obszary funkcjonalne w organizacji, np. finanse i marketing, również mają wpływ na osiągnięcie celów przedsiębiorstwa, ale w kontekście metodyki COBIT 5 uwzględniane są tylko działania i cele związane z IT.

Jednym z czynników umożliwiających są procesy, a w załączniku C zawarto mapowanie celów związanych z IT na istotne procesy COBIT 5, które zawierają powiązane cele procesów.

Ilustracja 5 — Cele przedsiębiorstwa COBIT 5

Wymiar zrównoważonej karty wyników (BSC)	Cel przedsiębiorstwa	Związek z celami w zakresie nadzoru		
		Realizacja korzyści	Optymalizacja ryzyka	Optymalizacja zasobów
Finanse	1. Wartość inwestycji biznesowych dla interesariuszy	P		S
	2. Portfel konkurencyjnych produktów i usług	P	P	S
	3. Zarządzane ryzyko biznesowe (ochrona zasobów)		P	S
	4. Zgodność z przepisami prawa i regulacjami		P	
	5. Przejrzystość finansowa	P	S	S
Klient	6. Kultura usług zorientowanych na klienta	P		S
	7. Ciągłość i dostępność usług biznesowych		P	
	8. Zwinność w reagowaniu na zmieniające się otoczenie biznesowe	P		S
	9. Świadome podejmowanie decyzji strategicznych na podstawie informacji	P	P	P
	10. Optymalizacja kosztów świadczenia usług	P		P
Obszar wewnętrzny	11. Optymalizacja funkcjonalności procesów biznesowych	P		P
	12. Optymalizacja kosztów procesów biznesowych	P		P
	13. Zarządzanie programami biznesowymi — zmiany biznesowe	P	P	S
	14. Wydajność pracowników i działań operacyjnych	P		P
	15. Zgodność z politykami wewnętrznymi		P	
Szkolenie i rozwój	16. Wykwalifikowany i zmotywowany personel	S	P	P
	17. Kultura innowacji produktów i biznesu	P		

Ilustracja 6 — Cele związane z IT

Wymiar zrównoważonej karty wyników IT (IT BSC)	Informacje i powiązany cel dotyczący technologii	
Finanse	01	Zgodność IT z biznesowymi celami strategicznymi
	02	Zgodność IT oraz wsparcie w zakresie zgodności działalności z przepisami prawa i regulacjami
	03	Zaangażowanie kadry zarządzającej w podejmowanie decyzji związanych z IT
	04	Zarządzanie ryzykiem biznesowym związanym z IT
	05	Uzyskanie korzyści z inwestycji i portfela usług związanych z IT
	06	W obszarze IT: przejrzystość kosztów, korzyści i ryzyka
Klient	07	Dostarczanie usług IT zgodnie z wymogami biznesowymi
	08	Adekwatne wykorzystanie aplikacji, informacji i rozwiązań w zakresie technologii
Obszar wewnętrzny	09	Zwinność IT (ang. agility)
	10	Bezpieczeństwo informacji, infrastruktury przetwarzania i aplikacji
	11	Optymalizacja aktywów, zasobów i potencjału związanych z IT
	12	Umożliwianie i wsparcie realizacji procesów biznesowych poprzez integrację aplikacji i rozwiązań technologicznych z procesami biznesowymi
	13	Realizacja programów przynoszących korzyści — w sposób terminowy, w ramach budżetu i zgodnie z wymogami i standardami jakościowymi
	14	Dostępność wiarygodnych i przydatnych informacji wspierających proces decyzyjny
	15	Zgodność IT z politykami wewnętrznymi
Szkolenie i rozwój	16	Kompetentny i zmotywowany personel działu biznesowego i działu IT
	17	Wiedza, kompetencje oraz inicjatywy w zakresie innowacji biznesowych

Wykorzystanie kaskady celów COBIT 5

Korzyści związane z kaskadą celów COBIT 5

Kaskada celów[3] jest istotna, ponieważ umożliwia zdefiniowanie priorytetów dotyczących wdrożenia, udoskonalenia oraz audytu nadzoru nad technologiami informatycznymi w przedsiębiorstwie na podstawie (strategicznych) celów przedsiębiorstwa oraz związanego z nimi ryzyka. W praktyce kaskada celów:

- definiuje istotne i wymierne cele i zadania na różnych poziomach odpowiedzialności;
- filtruje bazę wiedzy COBIT 5 (na podstawie celów przedsiębiorstwa) w celu wyszukania stosownych wytycznych, które zostaną uwzględnione w konkretnych projektach związanych z wdrożeniem, doskonaleniem i audytem;
- wyraźnie identyfikuje i komunikuje sposób (niekiedy z wyszczególnieniem operacji), w jaki czynniki umożliwiające ułatwiają osiągnięcie celów przedsiębiorstwa.

Właściwe korzystanie z kaskady celów COBIT 5

Kaskada celów — z tabelami dotyczącymi mapowania między celami przedsiębiorstwa oraz celami związanymi z IT, a także między celami związanymi z IT i czynnikami umożliwiającymi COBIT 5 (w tym procesami) — nie zawiera uniwersalnej prawdy, a użytkownicy nie powinni podejmować prób korzystania z niej w sposób mechaniczny, lecz raczej powinni potraktować ją jako wytyczną. Takie podejście jest konieczne z wielu powodów:

- Każde przedsiębiorstwo w inny sposób przypisuje priorytety swoim celom, a priorytety te mogą zmieniać się w czasie.
- Tabele dotyczące mapowania nie uwzględniają wielkości przedsiębiorstwa i/lub branży, w której działa. Reprezentują swego rodzaju wspólny mianownik dotyczący ogólnego sposobu wzajemnego powiązania różnych poziomów celów.
- Wskaźniki wykorzystane w mapowaniu są oparte na dwóch poziomach ważności lub istotności, co sugeruje, że istnieją łatwe do wskazania osobne poziomy istotności, podczas gdy w rzeczywistości mapowanie bardziej przypomina pewne continuum różnych stopni powiązania.

Praktyczne wykorzystanie kaskady celów COBIT 5

Z powyższego zastrzeżenia wynika jasno, że pierwszą czynnością, którą przedsiębiorstwo powinno zawsze wykonać, gdy korzysta z kaskady celów, jest dostosowanie ich mapowania w taki sposób, aby odpowiadało konkretnej sytuacji przedsiębiorstwa. Innymi słowy, każde przedsiębiorstwo powinno opracować własną kaskadę celów, porównać ją z metodyką COBIT, a następnie dopracować szczegóły.

Przedsiębiorstwo może na przykład zdecydować się na:

- Przełożenie strategicznych priorytetów na konkretną „wagę” lub istotność dla każdego z celów przedsiębiorstwa.
- Weryfikację mapowania kaskady celów z uwzględnieniem specyfiki środowiska, branży itd.

[3] Kaskada celów została oparta na wynikach badań przeprowadzonych przez Antwerp Management School, IT Alignment and Governance Institute w Belgii.

PRZYKŁAD 1 — KASKADA CELÓW

Przedsiębiorstwo zdefiniowało szereg celów strategicznych, z których najważniejszym jest zwiększenie zadowolenia klientów. W związku z tym chce się dowiedzieć, które aspekty związane z technologiami informatycznymi wymagają poprawy.

Przedsiębiorstwo uznaje, że przypisanie najwyższego priorytetu zadowoleniu klientów oznacza podwyższenie priorytetu następujących celów przedsiębiorstwa (zob. **ilustracja 5**):

- 6. Kultura usług zorientowanych na klienta
- 7. Ciągłość i dostępność usług biznesowych
- 8. Zwinność w reagowaniu na zmieniające się otoczenie biznesowe

Przedsiębiorstwo wykonuje kolejny krok w ramach kaskady celów: analizuje, które cele związane z IT odpowiadają celom przedsiębiorstwa. Sugerowane mapowanie między nimi przedstawiono w załączniku B.

Na tej podstawie sugerowane są poniższe cele związane z IT, uznane za najważniejsze (wszystkie relacje oznaczone literą P):

- 01 zgodność IT z biznesowymi celami strategicznymi
- 04 Zarządzanie ryzykiem biznesowym związanym z IT
- 07 Dostarczanie usług IT zgodnie z wymogami biznesowymi
- 09 Zwinność IT (ang. agility)
- 10 Bezpieczeństwo informacji, infrastruktury przetwarzania i aplikacji
- 14 Dostępność wiarygodnych i przydatnych informacji wspierających proces decyzyjny
- 17 Wiedza, kompetencje oraz inicjatywy w zakresie innowacji biznesowych

Przedsiębiorstwo weryfikuje tę listę i postanawia uznać za priorytetowe pierwsze cztery cele.

W kolejnym etapie w ramach kaskady celów, zgodnie z koncepcją czynnika umożliwiającego (zob. rozdział 5), cele związane z IT ułatwiają realizację szeregu celów czynników umożliwiających, w tym celów procesu. W załączniku C zasugerowano mapowanie między celami związanymi z IT i procesami w ramach metodyki COBIT 5. Tabela umożliwia identyfikację najistotniejszych procesów związanych z IT, które wspierają realizację celów związanych z IT. Same procesy jednak nie wystarczą. Pozostałe czynniki umożliwiające, takie jak kultura, etyka i zachowanie, struktury organizacyjne oraz umiejętności i kompetencje są równie ważne i wymagają zbioru jasnych celów.

Po zakończeniu tych działań przedsiębiorstwo posiada zbiór spójnych celów dla wszystkich czynników umożliwiających, które ułatwią realizację wskazanych celów strategicznych, oraz komplet powiązanych mierników pozwalających na pomiar sprawności.

PRZYKŁAD 2 — POTRZEBY INTERESARIUSZY: ZRÓWNOWAŻONY ROZWÓJ

Po przeprowadzeniu analizy potrzeb interesariuszy przedsiębiorstwo uznaje, że strategicznym priorytetem jest zrównoważony rozwój. Zrównoważony rozwój obejmuje nie tylko aspekty środowiskowe, lecz także wszystkie elementy składające się na długoterminowy sukces przedsiębiorstwa.

Na podstawie wyników analizy potrzeb interesariuszy przedsiębiorstwo postanawia skupić się na realizacji pięciu poniższych celów, które zostaną w pewnym stopniu uszczegółowione:

1. Wartość inwestycji biznesowych dla interesariuszy, szczególnie dla społeczności interesariuszy
4. Zgodność z przepisami prawa i regulacjami, ze szczególnym uwzględnieniem przepisów środowiskowych oraz wynikających z regulacji dotyczących warunków zatrudnienia w uzgodnieniach dotyczących outsourcingu
8. Zwinność w reagowaniu na zmieniające się otoczenie biznesowe
16. Wykwalifikowany i zmotywowany zespół rozumiejący, że sukces przedsiębiorstwa zależy od jego pracowników
17. Kultura innowacji produktów i biznesu, koncentrująca się na długofalowym rozwoju innowacji

Na podstawie tych priorytetów można stosować kaskadę celów w sposób opisany w tekście.

Pytania dotyczące nadzoru nad technologiami informatycznymi i zarządzania nimi

Spełnienie potrzeb interesariuszy w każdym przedsiębiorstwie — biorąc pod uwagę duże uzależnienie od IT — wymaga udzielenia odpowiedzi na szereg pytań dotyczących nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi (**ilustracja 7**).

Ilustracja 7 — Pytania dotyczące nadzoru nad technologiami informatycznymi i zarządzania nimi	
Interesariusze wewnętrzni	**Pytania interesariuszy wewnętrznych**
• Zarząd • Dyrektor generalny (CEO) • Dyrektor ds. finansowych (CFO) • Dyrektor ds. informatyki (CIO) • Dyrektor ds. ryzyka (CRO) • Naczelne kierownictwo • Właściciele procesów biznesowych • Kierownicy obszaru biznesowego • Kierownicy ds. ryzyka • Kierownicy ds. bezpieczeństwa • Kierownicy ds. usług • Kierownicy ds. zarządzania zasobami ludzkimi (HR) • Audyt wewnętrzny • Dyrektorzy ds. prywatności • Użytkownicy IT • Kierownicy ds. IT • Itd.	• W jaki sposób uzyskuje się wartość z korzystania z IT? Czy użytkownicy końcowi są zadowoleni z jakości usług IT? • W jaki sposób zarządza się sprawnością technologii informatycznych? • Jaki jest najlepszy sposób wykorzystania nowych technologii w kontekście nowych strategicznych szans dla przedsiębiorstwa? • Jaki jest optymalny sposób utworzenia i struktura działu IT? • W jakim stopniu jestem uzależniony od zewnętrznych dostawców? Jak wypada ocena sprawności zarządzania umowami o outsourcing IT? Jak można zapewnić audyt dotyczący zewnętrznych dostawców? • Jakie są wymogi (kontrolne) w odniesieniu do informacji? • Czy uwzględniłem całe zidentyfikowane ryzyko związane z IT? • Czy realizowane przeze mnie operacje IT są efektywne i elastyczne? • Jak kontrolować koszty IT? Jaki jest najbardziej skuteczny i wydajny sposób wykorzystania zasobów IT? Jakie są najbardziej skuteczne i wydajne opcje zaopatrzenia? • Czy liczba pracowników odpowiedzialnych za IT jest wystarczająca? W jaki sposób można rozwijać i utrzymywać ich umiejętności oraz jak zarządza się ich sprawnością? • W jaki sposób zapewnić audyt IT? • Czy informacje, które przetwarzam, są dobrze zabezpieczone? • Jak można poprawić zwinność biznesu dzięki bardziej elastycznemu środowisku IT? • Czy projekty IT nie przynoszą spodziewanych rezultatów — a jeśli tak, to dlaczego? Czy IT stanowi przeszkodę w realizacji strategii biznesowej? • Jak dużą rolę odgrywa IT w utrzymaniu funkcjonowania przedsiębiorstwa? Jak postępować w przypadku braku dostępności IT? • Jakie kluczowe procesy biznesowe zależą od technologii informatycznych i jakie są wymogi dotyczące procesów biznesowych? • Ile wynosiła średnia wartość przekroczenia budżetów operacyjnych IT? Jak często i w jakim stopniu projekty IT przekraczają wyznaczony budżet? • Jaka część działań w ramach IT dotyczy reaktywnego rozwiązywania nagłych problemów, nie zaś proaktywnego wspierania działalności biznesowej? • Czy dostępne zasoby oraz infrastruktura IT są wystarczające do realizacji strategicznych celów przedsiębiorstwa? • Jak długo trwa proces podejmowania najważniejszych decyzji dotyczących IT? • Czy wszystkie działania i inwestycje związane z IT są transparentne? • Czy technologie informatyczne ułatwiają przedsiębiorstwu zachowanie zgodności z regulacjami oraz poziomami usług? Jak mogę sprawdzić, czy przestrzegam wszystkich obowiązujących regulacji?
Interesariusze zewnętrzni	**Pytania interesariuszy zewnętrznych**
• Partnerzy biznesowi • Dostawcy • Udziałowcy • Organy nadzorcze/rządowe • Użytkownicy zewnętrzni • Klienci • Organizacje normalizacyjne • Audytorzy zewnętrzni • Konsultanci • Itd.	• Jak mogę się przekonać, czy działalność operacyjna mojego partnera biznesowego jest chroniona i wiarygodna? • Skąd wiadomo, że przedsiębiorstwo przestrzega obowiązujących przepisów i regulacji? • Jak mogę się przekonać, czy przedsiębiorstwo utrzymuje efektywny system kontroli wewnętrznej? • Czy partnerzy biznesowi kontrolują istniejący między nimi łańcuch informacji?

Jak można znaleźć odpowiedzi na te pytania?

Wszystkie kwestie wskazane na **ilustracji 7** mogą zostać powiązane z celami przedsiębiorstwa i stanowią dane wejściowe dla kaskady celów, która umożliwia ich skuteczne uwzględnienie. Załącznik D zawiera przykład mapowania między pytaniami interesariuszy wskazanymi na **ilustracji 7** i celami przedsiębiorstwa.

Rozdział 3
Zasada 2: Uwzględnienie wszystkich aspektów działania przedsiębiorstwa

W metodyce COBIT 5 w sposób kompleksowy i z perspektywy całego przedsiębiorstwa uwzględniono nadzór nad informacjami oraz powiązaną technologią i zarządzanie nimi. Oznacza to, że w metodyce COBIT 5:
- Nadzór nad technologiami informatycznymi w organizacji jest częścią ładu korporacyjnego. Zaproponowany w metodyce COBIT 5 system nadzoru dla technologii informatycznych w przedsiębiorstwie można w płynny sposób zintegrować z każdym systemem nadzoru. Metodyka COBIT 5 jest spójna z najnowszymi poglądami dotyczącymi nadzoru.
- Uwzględniono wszystkie funkcje i procesy wymagane do zapewnienia nadzoru nad informacjami oraz powiązanymi technologiami w przedsiębiorstwie i zarządzania nimi we wszystkich miejscach, w których informacje mogą być przetwarzane. Biorąc pod uwagę rozszerzony zakres przedsiębiorstwa, metodyka COBIT 5 uwzględnia wszystkie istotne wewnętrzne i zewnętrzne usługi IT, a także wewnętrzne i zewnętrzne procesy biznesowe.

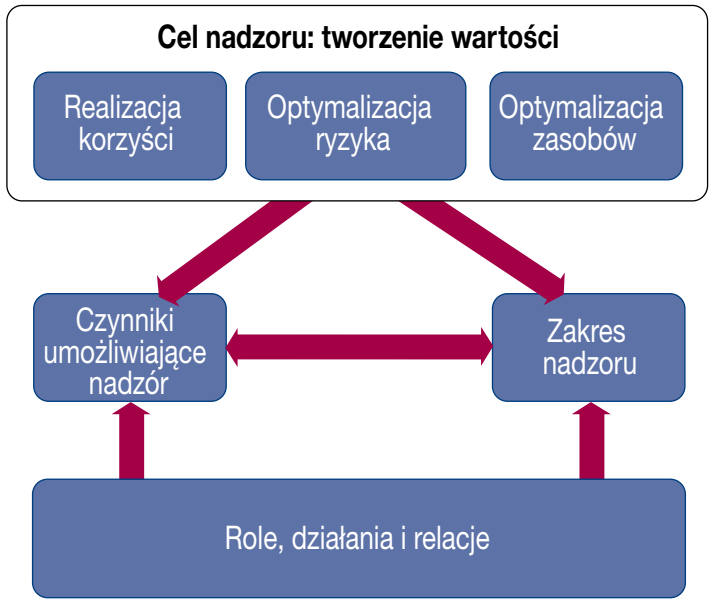
COBIT 5 zapewnia całościowy i systemowy wgląd w nadzór nad technologiami informatycznymi w przedsiębiorstwie i zarządzanie nimi (zob. zasada 4) na podstawie szeregu czynników umożliwiających. Czynniki umożliwiające dotyczące nadzoru nad systemami informatycznymi i zarządzania nimi są ogólnofirmowe i mają charakter kompleksowy, tj. obejmują wszystkich i wszystko — wewnątrz przedsiębiorstwa i poza nim — co jest istotne dla nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi, z uwzględnieniem działań i zakresów odpowiedzialności zarówno funkcji IT, jak i funkcji biznesowych niezwiązanych z IT.

Informacja jest jedną z kategorii czynników umożliwiających COBIT. Model, na podstawie którego zdefiniowano czynniki umożliwiające w ramach metodyki COBIT 5, pozwala każdemu interesariuszowi na zdefiniowanie rozbudowanych i kompletnych wymogów dotyczących informacji oraz cyklu życia przetwarzania informacji. Umożliwia on w ten sposób powiązanie funkcji biznesowej i jej potrzeby uzyskania odpowiednich informacji z funkcją IT, wspierając skoncentrowanie się na działalności biznesowej i kontekście funkcjonowania przedsiębiorstwa.

Podejście do nadzoru

Kompleksowe podejście do nadzoru leżące u podstaw metodyki COBIT 5 przedstawiono na **ilustracji 8**, na której wskazano kluczowe komponenty systemu nadzoru[4].

Ilustracja 8 — Nadzór i zarządzanie w ramach metodyki COBIT 5



[4] Pojęcia związane z nadzorem przedstawione we wcześniejszej inicjatywie ISACA, Taking Governance Forward (TGF), zostały włączone do metodyki COBIT 5. Ponieważ nie ma już potrzeby korzystania z TGF jako osobnego zasobu, został on wycofany.

Oprócz celu dotyczącego nadzoru — pozostałe główne elementy podejścia do nadzoru obejmują czynniki umożliwiające, zakres i role, a także działania i relacje.

Czynniki umożliwiające nadzór

Czynniki umożliwiające nadzór to zasoby organizacyjne związane z nadzorem, takie jak metodyki, zasady, struktury, procesy oraz praktyki, na które ukierunkowane jest działanie i które umożliwiają osiągnięcie celów. Czynniki umożliwiające uwzględniają również zasoby przedsiębiorstwa — np. zdolność do świadczenia usług (infrastruktura IT, aplikacje itd.), osoby i informacje. Brak zasobów lub czynników umożliwiających może wpłynąć na zdolność przedsiębiorstwa do tworzenia wartości.

Biorąc pod uwagę istotną rolę czynników umożliwiających nadzór, metodyka COBIT 5 uwzględnia jednolity sposób postrzegania czynników umożliwiających i postępowania z nimi (zob. rozdział 5).

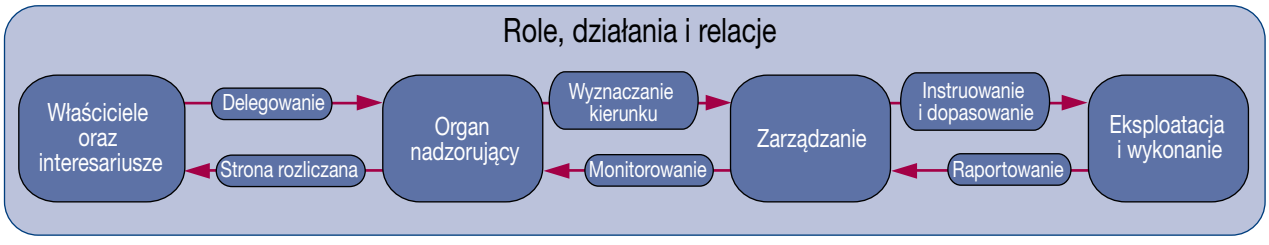
Zakres nadzoru

Nadzór może być stosowany w odniesieniu do całego przedsiębiorstwa, jednostki, środków trwałych oraz wartości niematerialnych itd. Istnieje możliwość zdefiniowania różnych sposobów postrzegania przedsiębiorstwa, którego dotyczy nadzór; konieczne jest również zdefiniowanie zakresu systemu nadzoru. Zakres metodyki COBIT 5 obejmuje przedsiębiorstwo — ale zasadniczo metodyka COBIT 5 może korzystać z każdego z tych różnych sposobów postrzegania.

Role, działania i relacje

Ostatnim elementem są role, działania i relacje w zakresie nadzoru. Definiuje on osoby zajmujące się nadzorem, sposób, w jaki są zaangażowane, charakter ich działań oraz sposób interakcji w zakresie określonego systemu zarządzania. W metodyce COBIT 5 istnieje wyraźne rozróżnienie działań związanych z nadzorem i zarządzaniem w domenie nadzoru i zarządzania; wskazano również wspólne płaszczyzny oraz osoby pełniących określone role. **Ilustracja 9** stanowi rozwinięcie dolnej części **ilustracji 8** i przedstawia interakcje między poszczególnymi rolami.

Ilustracja 9 — Kluczowe role, działania i relacje



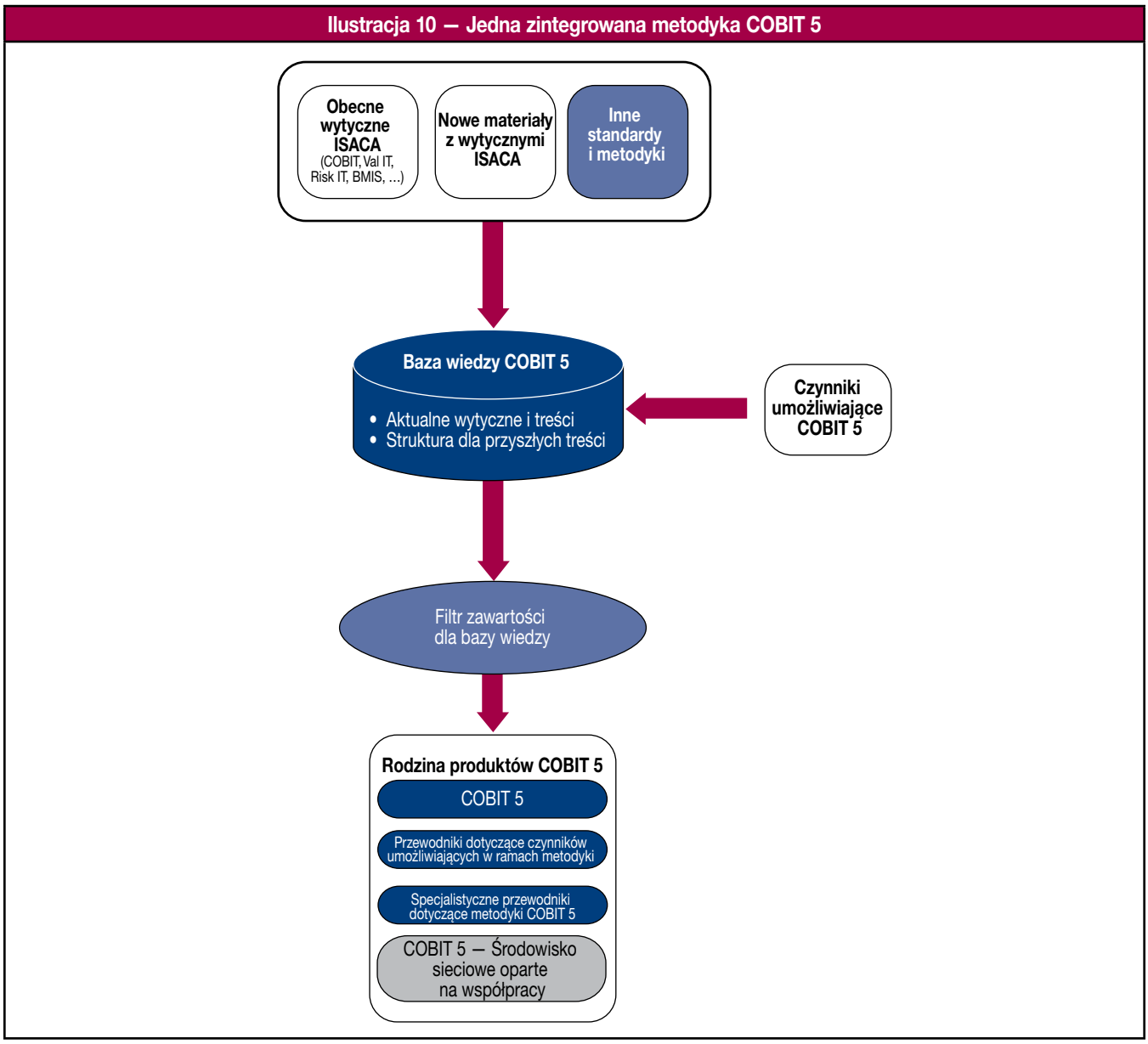
Rozdział 4
Zasada 3: Stosowanie jednej zintegrowanej metodyki

Metodyka COBIT 5 stanowi jedną zintegrowaną strukturę, ponieważ:
- Jest spójna z innymi najnowszymi stosownymi normami i metodykami, co sprawia, że przedsiębiorstwo może wykorzystać metodykę COBIT 5 jako nadrzędną strukturę nadzoru nad technologiami informatycznymi i zarządzania nimi, umożliwiającą integrację innych metodyk.
- Obejmuje swoim zakresem całe przedsiębiorstwo, stanowiąc podstawę umożliwiającą efektywną integrację innych wykorzystywanych metodyk, norm i praktyk. Jedna nadrzędna metodyka stanowi spójne i zintegrowane źródło wytycznych napisanych przystępnym językiem zrozumiałym dla osób nieposiadających specjalistycznej wiedzy technicznej.
- Zapewnia prostą architekturę umożliwiającą ustrukturyzowanie materiałów pomocniczych i uzyskanie spójnego zbioru produktów.
- Łączy całą wiedzę wcześniej rozproszoną w różnych metodykach ISACA. ISACA od wielu lat prowadzi badania dotyczące kluczowego obszaru ładu korporacyjnego i opracowała metodyki, takie jak COBIT, Val IT, Risk IT, BMIS, publikację *Board Briefing on IT Governance* oraz ITAF, z myślą o zapewnieniu wytycznych oraz wsparcia dla przedsiębiorstw. Metodyka COBIT 5 zawiera całą tę wiedzę.

Integracja różnych metodyk w ramach COBIT 5

Na **ilustracji 10** w sposób graficzny przedstawiono sposób, w jaki metodyka COBIT 5 w spójny sposób łączy w sobie różne elementy.

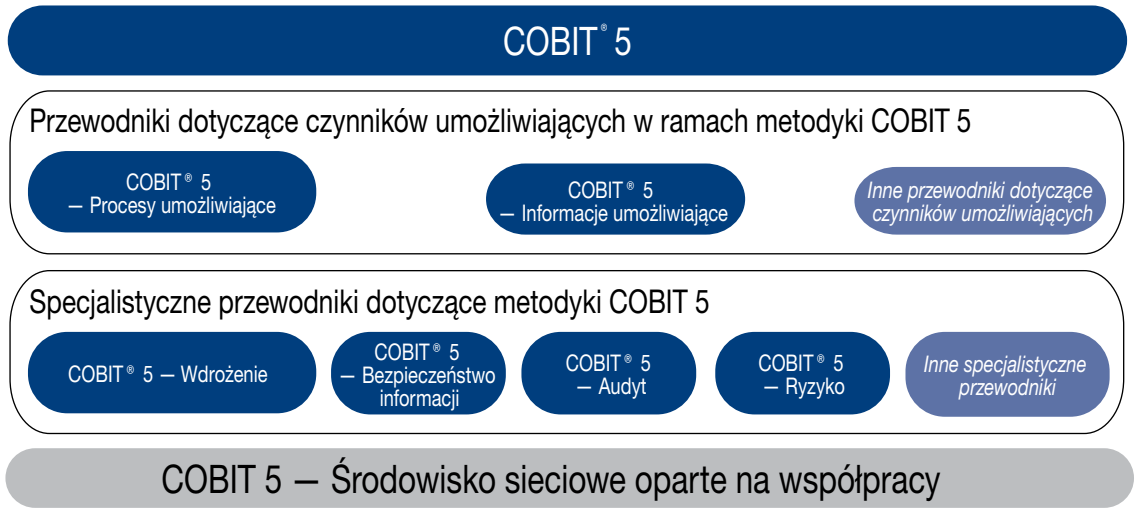
Ilustracja 10 — Jedna zintegrowana metodyka COBIT 5



Metodyka COBIT 5 zapewnia interesariuszom najbardziej kompletne i aktualne wytyczne (zob. **ilustracja 11**) dotyczące nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi poprzez:

- Badanie i wykorzystywanie zbioru materiałów źródłowych, na podstawie których opracowano nowe treści, np.:
  – łączenie istniejących wytycznych ISACA (COBIT 4.1, Val IT 2.0, Risk IT, BMIS) w ramach jednej metodyki;
  – uzupełnienie tych treści o obszary wymagające dalszego opracowania i aktualizacji;
  – dopasowanie do innych standardów i metodyk, takich jak ITIL, TOGAF oraz normy ISO. Pełną listę materiałów źródłowych można znaleźć w załączniku A.
- Zdefiniowanie zbioru czynników umożliwiających nadzór i zarządzanie, zapewniających strukturę dla wszystkich materiałów pomocniczych.
- Uzupełnienie bazy wiedzy COBIT 5 zawierającej wszystkie wytyczne i treści utworzone do tej pory i stanowiącej strukturę dla dodatkowych przyszłych treści.
- Zapewnienie rzetelnej i kompleksowej podstawy dla dobrych praktyk.

Ilustracja 11 — Rodzina produktów COBIT 5



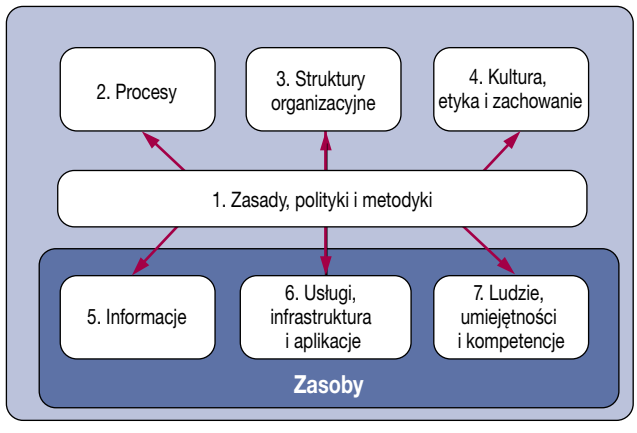
Rozdział 5
Zasada 4: Wdrożenie podejścia całościowego

Czynniki umożliwiające COBIT 5

Czynniki umożliwiające indywidualnie i kolektywnie decydują o tym, czy dany aspekt (w tym przypadku nadzór nad technologiami informatycznymi w przedsiębiorstwie i zarządzanie nimi) będzie działał właściwie. Czynniki umożliwiające są oparte na kaskadzie celów, tj. cele wyższego rzędu związane z IT określają, co powinny zrealizować poszczególne czynniki umożliwiające.

W metodyce COBIT 5 opisano siedem kategorii czynników umożliwiających (**ilustracja 12**).
- **Zasady, polityki i metodyki** stanowią środek umożliwiający przełożenie pożądanych wzorców zachowań na praktyczne wytyczne dotyczące codziennego zarządzania.
- **Procesy** opisują uporządkowany zbiór praktyk i działań umożliwiających osiągnięcie określonych celów i uzyskanie zbioru wyników ułatwiających realizację ogólnych celów związanych z IT.
- **Struktury organizacyjne** to kluczowe jednostki odpowiedzialne za podejmowanie decyzji w przedsiębiorstwie.
- **Kultura, etyka i zachowanie** odnoszą się do osób oraz przedsiębiorstwa i są często niedocenianym czynnikiem sukcesu działań związanych z nadzorem i zarządzaniem.
- **Informacja** dotyczy całego przedsiębiorstwa i obejmuje wszystkie informacje wytwarzane i wykorzystywane przez przedsiębiorstwo. Informacje są wymagane do zapewnienia właściwego funkcjonowania organizacji oraz nadzoru nad jej działalnością, ale na poziomie operacyjnym informacje są bardzo często kluczowym produktem przedsiębiorstwa.
- **Usługi, infrastruktura i aplikacje** obejmują infrastrukturę, technologię i aplikacje zapewniające przedsiębiorstwu możliwości przetwarzania oraz usługi IT.
- **Ludzie, umiejętności i kompetencje** to czynnik dotyczący osób i jest wymagany do skutecznej realizacji wszystkich działań oraz podejmowania właściwych decyzji i przeprowadzania działań naprawczych.

Ilustracja 12 — Czynniki umożliwiające funkcjonowanie przedsiębiorstwa w metodyce COBIT 5



Niektóre zdefiniowane wcześniej czynniki umożliwiające stanowią również zasoby przedsiębiorstwa, które również wymagają zarządzania i nadzoru. Odnosi się to do następujących czynników:
- Informacje, którymi należy zarządzać jako zasobem. Niektóre informacje, takie jak raporty dotyczące zarządzania oraz informacje uzyskane podczas analizy biznesowej, są ważnymi czynnikami umożliwiającymi nadzór oraz zarządzanie w przedsiębiorstwie.
- Usługi, infrastruktura i aplikacje.
- Ludzie, umiejętności i kompetencje.

Systemowy nadzór i zarządzanie za pomocą wzajemnie powiązanych czynników umożliwiających

Na ilustracji 12 wskazano również nastawienie wymagane dla zapewnienia ładu korporacyjnego, w tym nadzoru nad technologiami informatycznymi, który ułatwi realizację głównych celów przedsiębiorstwa. Każde przedsiębiorstwo musi zawsze uwzględniać wzajemnie powiązany zbiór czynników umożliwiających. Oznacza to, że każdy czynnik umożliwiający:

- będzie w pełni efektywny tylko wtedy, jeśli zapewnione zostaną dane wejściowe innych czynników umożliwiających, np. procesy wymagają informacji, struktury organizacyjne wymagają umiejętności i zachowania;
- zapewnia wynik, z którego korzystają inne czynniki umożliwiające, np. procesy zapewniają informacje, a umiejętności i zachowanie zwiększają efektywność realizacji procesów.

Dobre decyzje związane z nadzorem nad technologiami informatycznymi w przedsiębiorstwie i zarządzaniem nimi można podjąć tylko wtedy, gdy uwzględni się ten systemowy charakter ustaleń dotyczących nadzoru i zarządzania. Oznacza to, że spełnienie potrzeb interesariuszy wymaga analizy wszystkich wzajemnie powiązanych czynników umożliwiających w celu dokonania oceny ich odpowiedniości i uwzględnienia (w razie potrzeby). To nastawienie wymaga wsparcia kierownictwa najwyższego szczebla w przedsiębiorstwie, co przedstawiono na poniższych przykładach.

PRZYKŁAD 3 — NADZÓR NAD TECHNOLOGIAMI INFORMATYCZNYMI W PRZEDSIĘBIORSTWIE I ZARZĄDZANIE NIMI

Zapewnienie operacyjnych usług IT wszystkim użytkownikom wymaga zdolności do świadczenia usług (infrastruktura, aplikacje), dla których potrzebne są osoby posiadające odpowiedni zbiór umiejętności (w tym umiejętności behawioralnych). Należy również wdrożyć szereg procesów realizacji usług, wspieranych przez właściwe struktury organizacyjne, z przedstawieniem sposobu, w jaki wszystkie czynniki umożliwiające są wymagane do skutecznej realizacji usług.

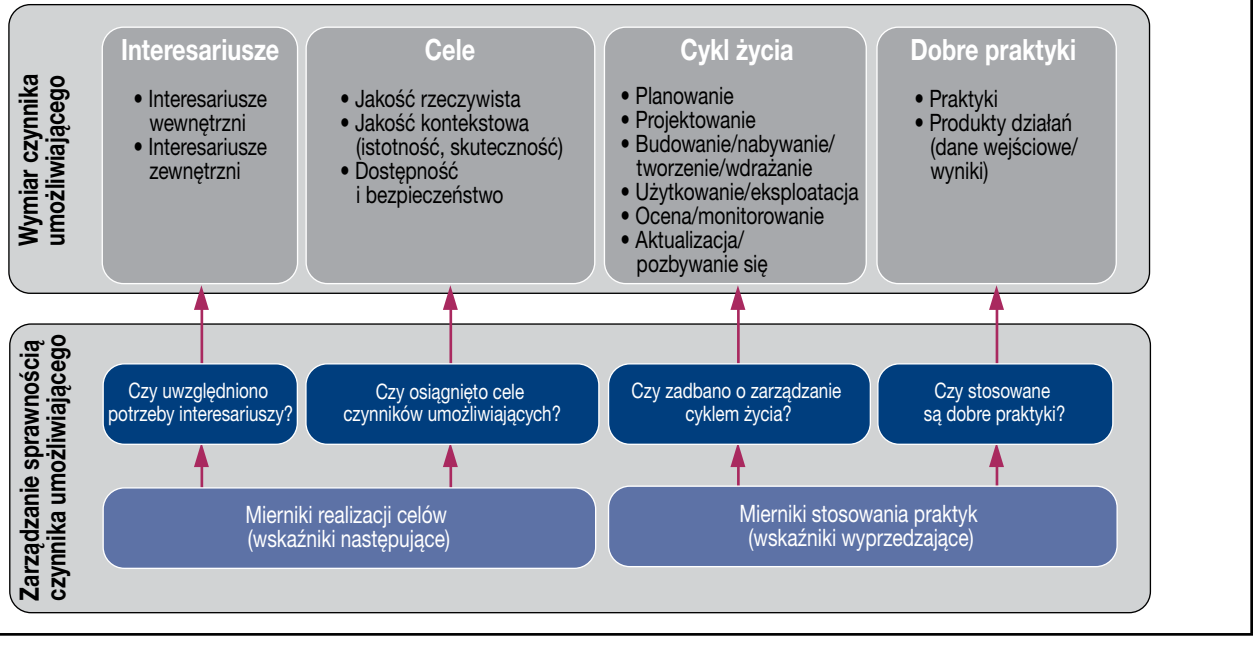
PRZYKŁAD 4 — NADZÓR NAD TECHNOLOGIAMI INFORMATYCZNYMI W PRZEDSIĘBIORSTWIE I ZARZĄDZANIE NIMI

Zapewnienie bezpieczeństwa informacji wymaga opracowania i wdrożenia szeregu polityk i procedur. Polityki te z kolei wymagają wdrożenia praktyk związanych z bezpieczeństwem. Jeśli jednak kultura i etyka przedsiębiorstwa oraz personelu nie są odpowiednie, procesy i procedury dotyczące bezpieczeństwa informacji nie będą skuteczne.

Wymiary czynników umożliwiających COBIT 5

Wszystkie czynniki umożliwiające mają zbiór wspólnych wymiarów. Zbiór wspólnych wymiarów (**ilustracja 13**):
- pozwala na wykorzystanie czynników umożliwiających w sposób typowy, prosty i ustrukturyzowany;
- umożliwia przedsiębiorstwu zarządzanie jego złożonymi interakcjami;
- ułatwia wykorzystanie czynników umożliwiających z pomyślnym wynikiem.

Ilustracja 13 — Czynniki umożliwiające COBIT 5: typowe



Wymiary czynnika umożliwiającego

Cztery wspólne wymiary dla czynników umożliwiających to:
- **Interesariusze** — dla każdego czynnika umożliwiającego można wskazać interesariuszy (strony, które odgrywają aktywną rolę i/lub są zainteresowane czynnikiem umożliwiającym). Na przykład: w procesach uczestniczą różne strony, które realizują czynności w ramach procesów i/lub są zainteresowane rezultatami procesów; struktury organizacyjne mają interesariuszy — z ich własnymi rolami i zainteresowaniami — stanowiących część struktur.

Interesariusze przedsiębiorstwa mogą być wewnętrzni lub zewnętrzni i wszyscy mają własne — niekiedy wykluczające się — zainteresowania i potrzeby. Potrzeby interesariuszy przekładają się na cele przedsiębiorstwa, które z kolei przekładają się na cele przedsiębiorstwa związane z IT. Listę interesariuszy przedstawiono na **ilustracji 7**.

- **Cele** — Dla każdego czynnika umożliwiającego istnieje określona liczba celów, a czynniki umożliwiające zapewniają wartość poprzez osiągnięcie tych celów. Cele można definiować na podstawie następujących kryteriów:
  – oczekiwane wyniki wykorzystania czynników umożliwiających;
  – zastosowanie lub wykorzystanie samego czynnika umożliwiającego.

Cele czynników umożliwiających to ostateczny etap w kaskadzie celów COBIT 5. Cele można dodatkowo podzielić na różne kategorie:

- **Jakość rzeczywista** — stopień, w jakim czynniki umożliwiające działają w sposób dokładny i obiektywny oraz zapewniają dokładne, obiektywne i uznane wyniki.
- **Jakość kontekstowa** — stopień, w jakim czynniki umożliwiające oraz ich rezultaty odpowiadają danemu celowi, biorąc pod uwagę kontekst, w którym funkcjonują. Na przykład: wyniki powinny być istotne, kompletne, aktualne, odpowiednie, spójne, zrozumiałe i łatwe do wykorzystania.
- **Dostęp i bezpieczeństwo** — stopień, w jakim czynniki umożliwiające oraz ich rezultaty są dostępne i zabezpieczone, np.:
  - czynniki umożliwiające są dostępne w razie potrzeby;
  - wyniki są zabezpieczone, tj. dostępne jedynie dla osób uprawnionych i potrzebujących takiego dostępu.

- **Cykl życia** — każdy czynnik umożliwiający ma cykl życia, od rozpoczęcia, przez okres funkcjonowania/żywotności, aż po jego wycofanie. Odnosi się to do informacji, struktur, procesów, polityk itd. Fazy cyklu życia:
  – Planowanie (obejmuje opracowanie oraz wybór koncepcji);
  – Projektowanie;
  – Budowanie/nabywanie/tworzenie/wdrażanie;
  – Użytkowanie/obsługa;
  – Ocena/monitorowanie;
  – Aktualizacja/pozbywanie się.
- **Dobre praktyki** — dla każdego czynnika umożliwiającego można zdefiniować dobre praktyki. Dobre praktyki ułatwiają osiągnięcie celów czynników umożliwiających. Dobre praktyki obejmują przykłady lub sugestie dotyczące optymalnego sposobu wdrożenia czynnika umożliwiającego i określają wymagane produkty działań bądź dane wejściowe i wyniki. W ramach metodyki COBIT 5 zapewniono przykłady dobrych praktyk w odniesieniu do niektórych czynników umożliwiających COBIT 5 (np. procesów). W przypadku innych czynników umożliwiających można wykorzystać wytyczne z innych standardów, metodyk itd.

Zarządzanie sprawnością czynnika umożliwiającego

Przedsiębiorstwa oczekują, że zastosowanie czynników umożliwiających przyniesie pozytywne wyniki. Zarządzanie sprawnością czynników umożliwiających wymaga regularnego monitorowania i udzielania odpowiedzi na poniższe pytania — na podstawie mierników:

- Czy uwzględniono potrzeby interesariuszy?
- Czy osiągnięto cele czynników umożliwiających?
- Czy zadbano o zarządzanie cyklem życia czynników umożliwiających?
- Czy stosowane są dobre praktyki?

Pierwsze dwa punkty dotyczą rzeczywistego wyniku zastosowania czynnika umożliwiającego. Mierniki pozwalające na określenie stopnia, w jakim osiągnięto cele, można nazwać „wskaźnikami następującymi”.

Ostatnie dwa punkty dotyczą rzeczywistego funkcjonowania samego czynnika umożliwiającego, a mierniki stosowane w tym celu można nazwać „wskaźnikami wyprzedzającymi”.

Przykład czynników umożliwiających w praktyce

Przykład 5 przedstawia czynniki umożliwiające, ich wzajemne powiązania oraz wymiary czynnika umożliwiającego, a także sposób ich wykorzystania w celu osiągnięcia praktycznych korzyści.

PRZYKŁAD 5 — CZYNNIKI UMOŻLIWIAJĄCE

Organizacja wyznaczyła „kierowników ds. procesów" dla procesów związanych z IT. Ich obowiązkiem jest definiowanie i realizacja skutecznych i wydajnych procesów związanych z IT w kontekście dobrego nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi.

Początkowo kierownicy ds. procesów skupią się na czynniku umożliwiającym Proces, rozważając jego następujące wymiary:

- **Interesariusze:** Interesariuszami procesów są wszystkie podmioty zaangażowane w realizację procesów, tj. wszystkie strony odpowiedzialne, rozliczane, konsultowane lub informowane (RACI) w związku z działaniami w ramach procesów. Można się tu posłużyć tabelą RACI opisaną w przewodniku *COBIT 5: Procesy umożliwiające*.
- **Cele:** Dla każdego procesu muszą zostać zdefiniowane odpowiednie cele i powiązane mierniki. Na przykład dla procesu *Zarządzanie relacjami* (proces APO08 w metodyce *COBIT 5: Procesy umożliwiające*) można znaleźć zbiór celów i mierników procesu, takich jak:
  - **Cel:** strategie biznesowe, plany i wymogi są dobrze zrozumiane, udokumentowane i zatwierdzone.
    - **Miernik:** odsetek programów spójny z wymogami/priorytetami biznesowymi przedsiębiorstwa.
  - **Cel:** istnieją dobre relacje między przedsiębiorstwem i działem IT.
    - **Miernik:** wskaźniki na podstawie badań dotyczących zadowolenia użytkowników i personelu IT.
- **Cykl życia**: Dla każdego procesu można wskazać cykl życia, tj. musi on zostać utworzony i zrealizowany oraz być monitorowany, a także (w stosownych wypadkach) dostosowywany. Ostatecznie procesy przestają istnieć. W tym przypadku kierownicy ds. procesów musieliby najpierw zaprojektować i zdefiniować proces. Mogą wykorzystać kilka elementów z przewodnika *COBIT 5: Procesy umożliwiające* w celu zaprojektowania procesów, tj. zdefiniowania zakresów odpowiedzialności oraz podziału procesów na praktyki i działania, a także zdefiniowania produktów działań w ramach procesów (dane wejściowe i wyniki). Na późniejszym etapie konieczne jest zwiększenie wydajności i solidności procesów. W tym celu kierownicy ds. procesów mogą podnieść poziom potencjału procesu. W tym celu można wykorzystać Model potencjału procesu COBIT 5 inspirowany normą ISO/IEC 15504 oraz atrybuty potencjału procesów.
- **Dobra praktyka:** W ramach metodyki COBIT 5 opisane są z dużą szczegółowością dobre praktyki wobec procesów w przewodniku *COBIT 5: Procesy umożliwiające*, wspomniane we wcześniejszym punkcie. W publikacji tej można znaleźć inspirację i przykładowe procesy, obejmujące pełne spektrum wymaganych działań dla celów nadzoru nad technologiami informatycznymi w przedsiębiorstwie oraz zarządzania nimi.

Oprócz wytycznych dotyczących czynnika umożliwiającego Proces kierownicy ds. procesów mogą przyjrzeć się kilku innym czynnikom umożliwiającym:

- tabele RACI, opisujące role i zakresy odpowiedzialności. Inne czynniki umożliwiające pozwalają na przejście do szczegółów tego wymiaru, np.:
  - w przypadku czynnika Umiejętności i kompetencje istnieje możliwość zdefiniowania umiejętności i kompetencji dla każdej roli, a także określenia właściwych celów (np. poziomy umiejętności technicznych i behawioralnych) oraz powiązanych mierników.
  - Tabela RACI zawiera również szereg struktur organizacyjnych. Struktury te mogą zostać dodatkowo omówione w związku z czynnikiem Struktury organizacyjne. Można wówczas przedstawić bardziej szczegółowy opis struktury oraz zdefiniować oczekiwane wyniki i powiązane mierniki (np. decyzje), a także określić dobre praktyki (np. zakres kontroli, zasady działania struktury, poziom uprawnień).
- Zasady i polityki sformalizują proces i określą, dlaczego istnieje, kogo dotyczy oraz w jaki sposób ma być wykorzystywany. To obszar, którego dotyczy czynnik umożliwiający Zasady i polityki.

W załączniku G w sposób bardziej szczegółowy omówiono siedem kategorii czynników umożliwiających. Zalecane jest zapoznanie się z tym załącznikiem w celu lepszego zrozumienia charakteru czynników umożliwiających oraz ich istotnej roli w organizowaniu nadzoru nad technologiami informatycznymi w przedsiębiorstwie oraz zarządzania nimi.

Rozdział 6
Zasada 5: Oddzielenie nadzoru od zarządzania

Nadzór i zarządzanie

W metodyce COBIT 5 wyraźnie rozróżnia się nadzór i zarządzanie. Każda z tych dziedzin obejmuje działania o odmiennym charakterze, wymaga różnych struktur organizacyjnych i służy innym celom. Kluczowe rozróżnienie nadzoru i zarządzania w metodyce COBIT 5:

- **Nadzór**

Dzięki nadzorowi zyskuje się pewność, że oceniono potrzeby, warunki i opcje interesariuszy w celu ustalenia zrównoważonych, uzgodnionych celów przedsiębiorstwa, które mają zostać osiągnięte. Nadzór polega również na ukierunkowaniu działań poprzez nadanie priorytetów i podejmowanie decyzji, a także na monitorowaniu sprawności i zgodności w odniesieniu do uzgodnionego kierunku i szczegółowych celów.

W większości przedsiębiorstw za nadzór odpowiada zarząd pod przywództwem prezesa.

- **Kierownictwo**

Zarządzanie polega na planowaniu, budowaniu, realizacji i monitorowaniu działań w sposób spójny z kierunkiem wskazanym przez organ nadzorujący, aby osiągnąć cele przedsiębiorstwa.

W większości przedsiębiorstw za zarządzanie odpowiada kadra zarządzająca pod przywództwem dyrektora generalnego (CEO).

Interakcje między nadzorem i zarządzaniem

Z definicji nadzoru i zarządzania wynika jasno, że wiążą się z nimi różne typy działań, odmienne zakresy odpowiedzialności, jednakże, biorąc pod uwagę rolę nadzoru (ocena, kierowanie i monitorowanie), wymagany jest zbiór interakcji między nadzorem i zarządzaniem w celu uzyskania skutecznego i wydajnego systemu nadzoru. Interakcje te, wykorzystujące strukturę czynnika umożliwiającego, przedstawiono w sposób ogólny na **ilustracji 14**.

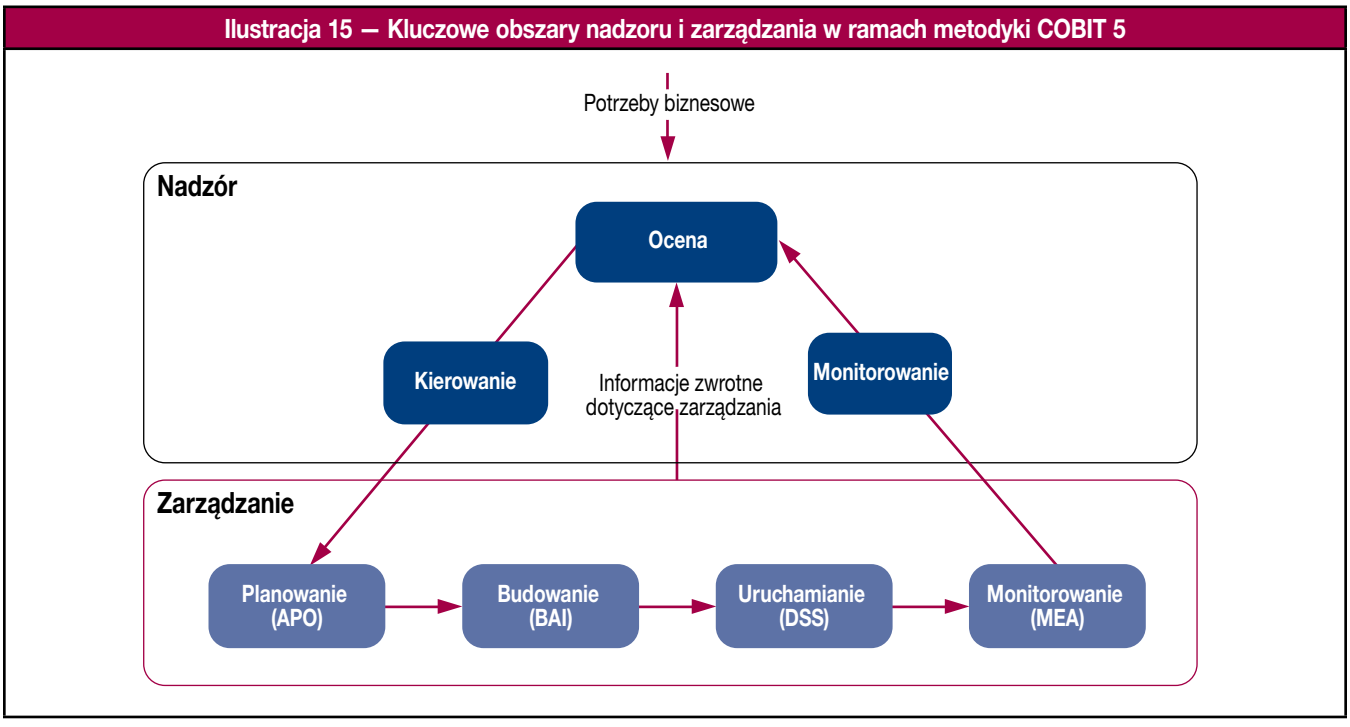
Ilustracja 14 — Interakcje między nadzorem i zarządzaniem w ramach metodyki COBIT 5

Czynnik umożliwiający	Interakcje między nadzorem i zarządzaniem
Procesy	W przykładowym modelu procesów COBIT 5 (*COBIT 5: Procesy umożliwiające*) rozróżnia się procesy nadzoru i zarządzania, z uwzględnieniem konkretnych zbiorów praktyk i działań. Model procesu uwzględnia również tabele RACI, opisujące zakresy odpowiedzialności różnych struktur organizacyjnych oraz ról w ramach przedsiębiorstwa.
Informacje	Model procesów opisuje dane wejściowe i wyniki różnych praktyk procesów w odniesieniu do innych procesów, z uwzględnieniem informacji wymienianych między procesami nadzoru i zarządzania. Informacje wykorzystywane do oceny, kierowania i monitorowania technologii informatycznych w przedsiębiorstwie są wymieniane między procesami zarządzania i nadzoru zgodnie z opisem danych wejściowych i wyników modelu procesów.
Struktury organizacyjne	W każdym przedsiębiorstwie zdefiniowano szereg struktur organizacyjnych; struktury mogą należeć do przestrzeni nadzoru lub przestrzeni zarządzania, w zależności od ich składu i zakresu decyzji. Ponieważ nadzór polega na określaniu kierunku, istnieje interakcja między decyzjami podejmowanymi przez struktury nadzoru — np. decyzjami dotyczącymi portfela inwestycyjnego oraz określania apetytu na ryzyko w przedsiębiorstwie — oraz decyzjami i operacjami, które dotyczą wdrożenia.
Zasady, polityki i metodyki	Zasady, polityki i metodyki stanowią środek umożliwiający zinstytucjonalizowanie decyzji dotyczących nadzoru w ramach przedsiębiorstwa i z tego powodu pozwalają na interakcję między decyzjami nadzoru (określanie kierunku) i zarządzania (realizacja decyzji).
Kultura, etyka i zachowanie	Zachowanie jest również kluczowym czynnikiem umożliwiającym właściwy nadzór nad przedsiębiorstwem i zarządzanie nim. Jest ustalane odgórnie (przywództwo przez dawanie przykładu) i w związku z tym stanowi istotną interakcję między nadzorem i zarządzaniem.
Ludzie, umiejętności i kompetencje	Działania w ramach nadzoru i zarządzania wymagają różnych zbiorów umiejętności, ale kluczową umiejętnością członków organu nadzorującego oraz osób odpowiedzialnych za zarządzanie jest znajomość charakteru obu zadań i świadomość dzielących je różnic.
Usługi, infrastruktura i aplikacje	Wymagane są usługi, wspierane przez aplikacje i infrastrukturę, zapewniające organowi nadzorującemu odpowiednie informacje i ułatwiające realizację działań w zakresie nadzoru, które polegają na ocenie, określaniu kierunku i monitorowaniu.

Model referencyjny procesu COBIT 5

Metodyka COBIT 5 nie ma charakteru normatywnego, ale zaleca wdrożenie procesów nadzoru i zarządzania w przedsiębiorstwie, tak aby obejmowały kluczowe obszary, zgodnie z **ilustracją 15**.

Ilustracja 15 — Kluczowe obszary nadzoru i zarządzania w ramach metodyki COBIT 5



Przedsiębiorstwo może organizować swoje procesy w sposób, który uznaje za odpowiedni, o ile obejmują one wszystkie konieczne cele w zakresie nadzoru i zarządzania. W mniejszych przedsiębiorstwach liczba procesów może być niższa; większe i bardziej złożone przedsiębiorstwa mogą mieć wiele procesów, z których wszystkie służą tym samym celom.

Metodyka COBIT 5 obejmuje model referencyjny procesu, który w sposób szczegółowy definiuje szereg procesów nadzoru i zarządzania. Obejmuje wszystkie procesy związane z działaniami w ramach IT, zwykle realizowane w przedsiębiorstwie, zapewniając wspólny model odniesienia, zrozumiały dla kierownictwa operacyjnego działu IT i firmy. Proponowany model procesów jest kompletny i kompleksowy, ale nie jest to jedyny możliwy model procesów. Każde przedsiębiorstwo musi zdefiniować własny zbiór procesów, uwzględniając specyfikę swojej działalności.

Wprowadzenie modelu operacyjnego i wspólnego języka komunikacji we wszystkich obszarach przedsiębiorstwa związanych z działaniami IT jest jednym z najważniejszych i kluczowych kroków w kierunku odpowiedniego nadzoru. Zapewnia to również metodykę pomiaru i monitorowania sprawności IT, zapewnienia audytu IT, komunikacji z dostawcami usług oraz wdrażania dobrych praktyk zarządzania.

W modelu referencyjnym procesu COBIT 5 podzielono procesy nadzoru i zarządzania technologiami informatycznymi w przedsiębiorstwie na dwie główne domeny:

- **Nadzór** — obejmuje pięć procesów nadzoru; w ramach każdego procesu zdefiniowano praktyki w zakresie oceny, kierowania i monitorowania (EDM)[5].
- **Zarządzanie** — obejmuje cztery domeny związane z obszarami odpowiedzialności w zakresie planowania, budowania, realizacji i monitorowania (PBRM), zapewniając całościowy wgląd w działalność IT. Te domeny stanowią rozwinięcie domeny i struktury procesów według COBIT 4.1. Nazwy domen są wybierane zgodnie z oznaczeniami głównych obszarów, ale zawierają dodatkowe określenia:
  - Dopasowanie, planowanie i organizacja (APO);
  - Budowanie, nabywanie i wdrażanie (BAI);
  - Dostarczanie, obsługa i wsparcie (DSS);
  - Monitorowanie, ocena i oszacowanie (MEA).

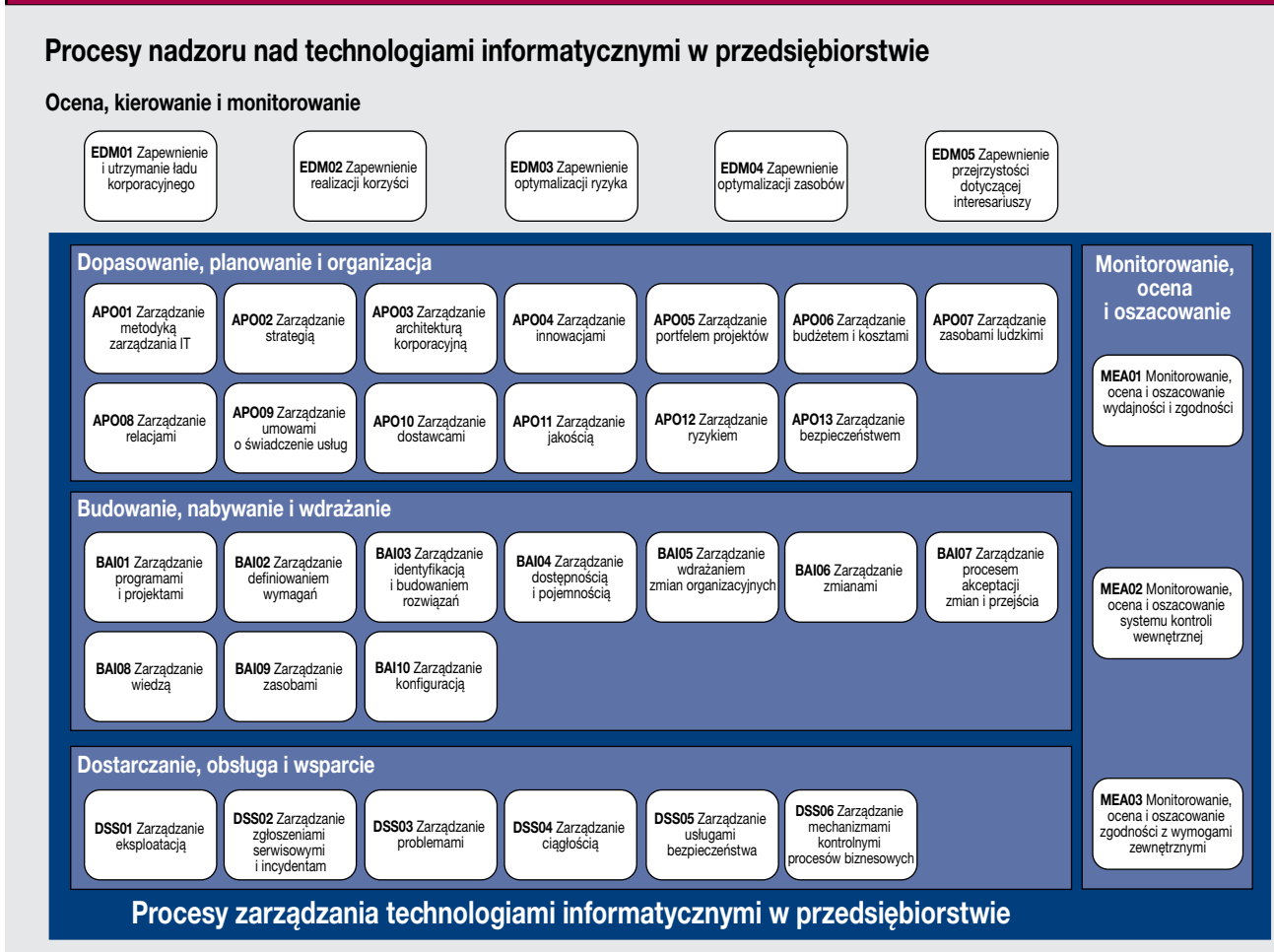
[5] W kontekście domeny nadzoru monitorowanie oznacza te działania, w ramach których organ nadzorujący sprawdza, w jakim stopniu określony kierunek wytyczony dla zarządzania został wcielony w życie.

Każda domena obejmuje szereg procesów. Choć, jak wcześniej opisano, większość procesów wymaga działań związanych z planowaniem, wdrożeniem, realizacją i monitorowaniem w ramach procesów lub w ramach konkretnego problemu (np. jakość, bezpieczeństwo), są one umieszczane w domenach odpowiadających zasadniczo najwłaściwszemu obszarowi działania, gdy ocenia się IT na poziomie przedsiębiorstwa.

Model referencyjny procesu COBIT 5 jest następcą modelu procesów COBIT 4.1, łączy w sobie również modele procesów Risk IT oraz Val IT.

Na **ilustracji 16** przedstawiono pełny zestaw 37 procesów nadzoru i zarządzania w ramach metodyki COBIT 5. Szczegóły wszystkich procesów, zgodnie z opisanym wcześniej modelem procesów, można znaleźć w przewodniku *COBIT 5: Procesy umożliwiające.*

Ilustracja 16 — Model referencyjny procesu COBIT 5



Strona celowo pozostawiona pusta

Rozdział 7
Wytyczne dotyczące wdrożenia

Wprowadzenie

Z wykorzystania metodyki COBIT można uzyskać optymalną wartość tylko wtedy, jeśli została ona skutecznie przyjęta i dostosowana, tak aby pasowała do unikalnego środowiska każdego przedsiębiorstwa. Każde podejście do wdrożenia musi również uwzględniać konkretne wyzwania, takie jak zarządzanie zmianami dotyczącymi kultury i zachowania.

ISACA zawarła praktyczne i rozbudowane wytyczne dotyczące wdrożenia w publikacji *COBIT® 5 — Wdrożenie*[6], opartej na cyklu życia ciągłego doskonalenia. Publikacja ta nie ma charakteru normatywnego ani nie stanowi kompletnego rozwiązania, lecz jest raczej zbiorem wskazówek ułatwiających uniknięcie często spotykanych problemów, wykorzystanie dobrych praktyk i uzyskanie pożądanych wyników. Do przewodnika dołączono również zestaw narzędzi wdrożeniowych zawierający różne zasoby, które wymagają ciągłego doskonalenia. Zawiera on:
- narzędzia do samooceny, pomiarów i diagnostyki;
- prezentacje przeznaczone dla różnych odbiorców;
- powiązane artykuły i dalsze wyjaśnienia.

Celem niniejszego rozdziału jest wstępne, ogólne omówienie cyklu życia wdrożenia i ciągłego doskonalenia oraz przedstawienie szeregu ważnych kwestii dotyczących metodyki *COBIT 5 — Wdrożenie*, takich jak:
- przygotowanie uzasadnienia biznesowego dotyczącego wdrożenia i udoskonalenia nadzoru nad technologiami informatycznymi oraz zarządzania nimi;
- rozpoznawanie typowych punktów zapalnych i zdarzeń inicjujących;
- stworzenie właściwego środowiska umożliwiającego wdrożenie;
- wykorzystanie metodyki COBIT do zidentyfikowania luk oraz ukierunkowania opracowania czynników umożliwiających, takich jak polityki, procesy, zasady, struktury organizacyjne oraz role i zakresy odpowiedzialności.

Uwzględnienie kontekstu przedsiębiorstwa

Nadzór nad technologiami informatycznymi w przedsiębiorstwie i zarządzanie nimi nie odbywa się w próżni.
Każde przedsiębiorstwo musi zaprojektować własny plan wdrożenia lub mapę działań, uwzględniając poniższe czynniki związane ze środowiskiem wewnętrznym i zewnętrznym przedsiębiorstwa, takie jak:
- etyka i kultura;
- obowiązujące przepisy, regulacje i polityki;
- misja, wizja i wartości;
- polityki i praktyki w zakresie nadzoru;
- plan biznesowy i strategiczne kierunki działania;
- model operacyjny oraz poziom dojrzałości;
- styl zarządzania;
- apetyt na ryzyko;
- potencjał oraz dostępne zasoby;
- praktyki stosowane w branży.

Równie ważne jest wykorzystanie i rozwinięcie istniejących czynników umożliwiających dotyczących ładu korporacyjnego.

Optymalne podejście do nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi będzie inne w każdym przedsiębiorstwie, a efektywne przyjęcie i dostosowanie metodyki COBIT w procesie wdrażania czynników umożliwiających nadzór nad technologiami informatycznymi i zarządzanie nimi wymaga zrozumienia i uwzględnienia kontekstu. COBIT często opiera się na innych metodykach, dobrych praktykach i normach, które również muszą zostać dostosowane, tak aby spełniały wymagania danego środowiska.

Kluczowe czynniki sukcesu umożliwiające skuteczne wdrożenie:
- kierownictwo najwyższego szczebla przedstawia wytyczne i przyznaje uprawnienia odnoszące się do inicjatywy; widoczne jest także jego ciągłe zaangażowanie i wsparcie;
- wszystkie strony wspierające realizację procesów nadzoru i zarządzania muszą zrozumieć cele biznesowe i cele IT;
- zapewnienie efektywnej komunikacji oraz umożliwienie wprowadzenia koniecznych zmian;

[6] *www.isaca.org/cobit*

- dostosowanie metodyki COBIT oraz innych pomocniczych dobrych praktyk i norm w taki sposób, aby pasowały do unikalnego kontekstu przedsiębiorstwa;
- skupienie się na szybkich korzyściach i określenie priorytetów najkorzystniejszych udoskonaleń, które będą najłatwiejsze do wprowadzenia.

Stworzenie właściwego środowiska

Ważny jest właściwy nadzór nad inicjatywami związanymi z wdrożeniem, wykorzystującymi metodykę COBIT, i odpowiednie zarządzanie nimi. Istotne inicjatywy związane z IT często kończą się niepowodzeniem z powodu braku odpowiedniego ukierunkowania działań, wsparcia i nadzoru ze strony różnych wymaganych interesariuszy; to samo dotyczy wdrożenia czynników umożliwiających dotyczących nadzoru nad technologiami informatycznymi i zarządzania nimi na podstawie metodyki COBIT. Wsparcie i wytyczne ze strony kluczowych interesariuszy mają krytyczne znaczenie dla wprowadzenia udoskonaleń i zapewnienia ich trwałości. W przypadku przedsiębiorstw działających w niekorzystnym środowisku (np. gdy ogólny model funkcjonowania przedsiębiorstwa jest niejasny lub brak czynników umożliwiających nadzór na poziomie przedsiębiorstwa) tego rodzaju wsparcie i uczestnictwo są jeszcze istotniejsze.

Czynniki umożliwiające oparte na metodyce COBIT powinny zapewnić rozwiązanie odnoszące się do realnych potrzeb i problemów biznesowych, nie mogą być celem samym w sobie. Wymagania oparte na analizie aktualnych punktów zapalnych oraz wyznaczników powinny zostać zidentyfikowane i zaakceptowane przez kierownictwo jako obszary wymagające podjęcia działań. Ogólne kontrole kondycji, diagnostyka lub oceny zdolności oparte na metodyce COBIT to doskonałe narzędzia umożliwiające podniesienie świadomości, uzgodnienie wspólnego stanowiska oraz uzyskanie zobowiązania do działania. O zaangażowanie i akceptację istotnych interesariuszy należy zabiegać od samego początku. W tym celu konieczne jest jasne przedstawienie celów i korzyści związanych z wdrożeniem (w kategoriach biznesowych) oraz podsumowanie ich w uzasadnieniu biznesowym.

Po uzyskaniu zaangażowania konieczne jest zapewnienie odpowiednich zasobów umożliwiających realizację programu. Należy zdefiniować i przydzielić kluczowe role oraz zakresy odpowiedzialności w programie. Powinno się zadbać o utrzymanie ciągłego zaangażowania wszystkich odpowiednich interesariuszy.

Należy wprowadzić i utrzymać właściwe struktury oraz procesy nadzoru i zarządzania. Te struktury i procesy powinny również zapewniać trwałe dopasowanie do ogólnofirmowych podejść w zakresie nadzoru oraz zarządzania ryzykiem.

Kluczowi interesariusze (np. zarząd i członkowie kierownictwa) muszą okazać widoczne wsparcie i zademonstrować zaangażowanie w celu określenia najważniejszych wytycznych i zapewnienia realizacji programu na wszystkich poziomach.

Rozpoznawanie punktów zapalnych i zdarzeń inicjujących

Istnieje kilka czynników, które mogą wskazywać na potrzebę udoskonalenia czynników umożliwiających dotyczących nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi.

Wykorzystanie punktów zapalnych lub zdarzeń inicjujących jako punktów, które stanowią bodziec do realizacji inicjatyw na rzecz wdrożenia umożliwia powiązanie uzasadnienia biznesowego dla udoskonaleń w odniesieniu do nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi z praktycznymi, codziennymi problemami. To zwiększy akceptację i stworzy w przedsiębiorstwie poczucie konieczności pilnego podjęcia działań, niezbędne do zainicjowania procesu wdrożenia. Ponadto istnieje możliwość zidentyfikowania szybkich korzyści i zademonstrowania wartości dodanej w obszarach, które są najbardziej widoczne lub rozpoznawalne w przedsiębiorstwie. Stanowi to platformę umożliwiającą wprowadzenie dalszych zmian i może ułatwić uzyskanie powszechnego zaangażowania członków kierownictwa wyższego szczebla oraz ich wsparcia dla wprowadzenia zmian o szerszym zakresie.

Poniżej przedstawiono przykłady typowych punktów zapalnych, dla których rozwiązaniem (lub częścią rozwiązania) mogą być nowe lub zmienione czynniki umożliwiające dotyczące nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi, wskazane w przewodniku *COBIT 5 — Wdrożenie*:
- frustracja pracowników działu biznesowego wynikająca z nieudanych inicjatyw, wzrostu kosztów IT oraz przekonania o niskiej wartości działalności;
- istotne incydenty związane z ryzykiem informatycznym, takie jak utrata danych lub niepowodzenie projektu;
- problemy z realizacją usług w ramach outsourcingu, takie jak ciągły brak zapewnienia uzgodnionego poziomu usług;
- niespełnienie wymagań regulacyjnych lub wymogów wynikających z umów;

- IT ogranicza potencjał przedsiębiorstwa w zakresie innowacji oraz zwinność biznesową;
- wyniki audytu regularnie wskazują na niedostateczną sprawność IT lub problemy z jakością usług IT;
- ukryte i nieuczciwe wydatki na IT;
- inicjatywy powielają się lub nakładają bądź dochodzi do marnotrawstwa zasobów, np. w przypadku przedwczesnego zakończenia projektu;
- niewystarczające zasoby IT, brak odpowiednich umiejętności zespołu lub wypalenie/niezadowolenie zespołu;
- zmiany wprowadzone dzięki IT nie spełniają potrzeb biznesowych i zostały wprowadzone z opóźnieniem lub przekroczyły budżet;
- niechęć członków zarządu, kadry kierowniczej i kierownictwa wyższego szczebla do współpracy z działem IT lub brak zaangażowanych i zadowolonych sponsorów biznesowych dla IT;
- złożone modele operacyjne IT.

Oprócz tych punktów zapalnych sygnałem lub czynnikiem skłaniającym do większego skupienia się na nadzorze nad technologiami informatycznymi i zarządzaniu nimi mogą być inne zdarzenia w wewnętrznym lub zewnętrznym środowisku przedsiębiorstwa. Przykłady z rozdziału 3 w publikacji *COBIT 5 — Wdrożenie*:
- fuzje, przejęcia lub inne zbycie;
- zmiana pozycji na rynku, pozycji ekonomicznej lub konkurencyjnej;
- zmiana modelu funkcjonowania przedsiębiorstwa lub uzgodnień dotyczących zaopatrzenia;
- nowe wymagania regulacyjne lub dotyczące zgodności z przepisami;
- istotna zmiana dotycząca technologii lub przesunięcie paradygmatu;
- ogólnofirmowa inicjatywa lub ogólnofirmowy projekt w zakresie nadzoru;
- nowy dyrektor generalny (CEO), dyrektor ds. finansowych (CFO), dyrektor ds. informatyki (CIO) itd.;
- audyt zewnętrzny lub oceny dokonane przez konsultantów;
- nowa strategia biznesowa lub nowy priorytet.

Umożliwienie zmian

Skuteczne wdrożenie zależy od wprowadzenia właściwej zmiany (właściwe czynniki umożliwiające dotyczące nadzoru lub zarządzania) we właściwy sposób. W wielu przedsiębiorstwach duży nacisk kładzie się na pierwszy aspekt — podstawowy nadzór nad technologiami informatycznymi w przedsiębiorstwie lub zarządzanie nimi — ale zbyt małą wagę przywiązuje się do zarządzania tymi aspektami zmiany, które dotyczą osób, zachowania i kultury, a także do motywowania interesariuszy do zaakceptowania zmiany.

Nie należy zakładać, że różni interesariusze, których dotyczą nowe lub zmienione czynniki umożliwiające, chętnie zaakceptują i przyjmą zmianę. Konieczne jest uwzględnienie możliwości braku świadomości zmian lub oporu, jakie wywołają, poprzez przyjęcie ustrukturyzowanego i proaktywnego podejścia. Należy również zadbać o jak największą świadomość realizacji programu wdrożeniowego poprzez opracowanie planu komunikacji, w którym dla każdej z faz programu zdefiniowana zostanie treść komunikatu, sposób, w jaki zostanie przekazany, oraz adresaci.

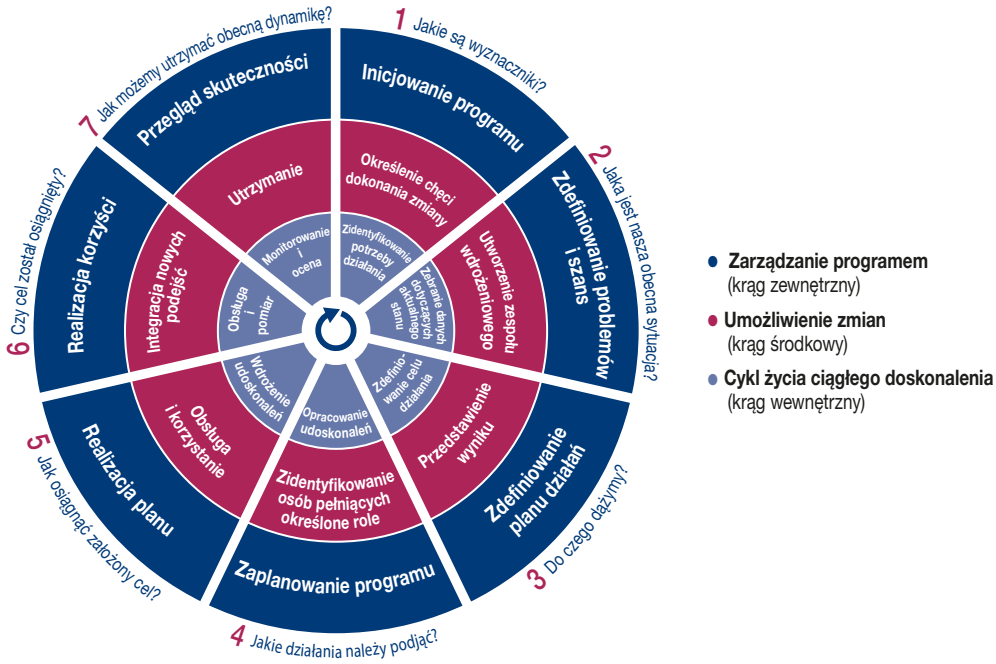
Trwałą poprawę można osiągnąć poprzez zyskanie zaangażowania interesariuszy (inwestycja w budowanie zaufania, zaangażowanie liderów oraz komunikowanie się z pracownikami i reagowanie na ich potrzeby) lub, w przypadkach, w których jest to wymagane, poprzez egzekwowanie zgodności z przepisami (inwestycja w procesy związane z administrowaniem, monitorowaniem i egzekwowaniem). Innymi słowy, konieczne jest przezwyciężenie barier związanych z czynnikiem ludzkim i zachowaniem oraz barier kulturowych, tak aby właściwe przyjęcie zmian, stworzenie atmosfery sprzyjającej zmianie i zapewnienie możliwości przyjęcia zmiany leżało we wspólnym interesie.

Podejście do cyklu życia

Cykl życia wdrożenia to sposób, w jaki przedsiębiorstwa mogą wykorzystać metodykę COBIT do uwzględnienia złożoności wdrożenia oraz sprostania typowym dla niego wyzwaniom w celu zapewnienia bezpieczeństwa informacji. Trzy wzajemnie powiązane komponenty cyklu życia:
1. Podstawowy cykl życia ciągłego doskonalenia — nie jest to projekt jednorazowy.
2. Wdrożenie zmiany — uwzględnienie aspektów związanych z zachowaniem i kulturą.
3. Zarządzanie programem.

Jak wspomniano, konieczne jest stworzenie właściwego środowiska w celu zapewnienia powodzenia realizacji inicjatywy związanej z wdrożeniem lub doskonaleniem. Cykl życia oraz jego siedem faz przedstawiono na **ilustracji 17**.

Ilustracja 17 — Siedem faz cyklu życia wdrożenia



Faza 1 rozpoczyna się od stwierdzenia i uzgodnienia potrzeby realizacji inicjatywy związanej z wdrożeniem lub doskonaleniem. Identyfikuje się w niej aktualne punkty zapalne oraz czynniki inicjujące, a także określa się potrzebę wprowadzenia zmian na poziomie zarządczym przedsiębiorstwa.

W **fazie 2** definiuje się zakres inicjatywy związanej z wdrożeniem lub doskonaleniem z wykorzystaniem mapowania celów przedsiębiorstwa na cele związane z IT oraz powiązane procesy IT (w ramach metodyki COBIT) i rozważa sposób, w jaki scenariusze ryzyka mogłyby również pomóc w ustaleniu kluczowych procesów, na których należy się skupić. Ogólna diagnostyka może również ułatwić określenie zakresu i wskazanie obszarów o wysokim priorytecie, na których należy się skoncentrować. Następnie przeprowadza się ocenę aktualnego stanu oraz szacowanie potencjału procesu, które umożliwia identyfikację problemów lub niedoskonałości. Inicjatywy o dużej skali powinny mieć strukturę opartą na wielu iteracjach cyklu życia — w przypadku każdej inicjatywy związanej z wdrożeniem, której realizacja trwa dłużej niż sześć miesięcy, istnieje ryzyko utraty dynamiki, koncentracji i akceptacji interesariuszy.

W trakcie **fazy 3** określa się cel procesu doskonalenia, a następnie przeprowadza się bardziej szczegółową analizę opartą na wytycznych COBIT w celu zidentyfikowania luk oraz możliwych rozwiązań. Niektóre rozwiązania mogą umożliwiać uzyskanie szybkich korzyści, inne zaś są bardziej wymagające, a ich realizacja trwa dłużej. Priorytet powinny mieć inicjatywy, których realizacja jest prostsza, oraz te, które mogą przynieść największe korzyści.

W **fazie 4** planuje się praktyczne rozwiązania, definiując projekty wspierane przez uzasadnienia biznesowe. Opracowuje się również plan zmian w odniesieniu do wdrożenia. Dobrze opracowane uzasadnienie biznesowe daje pewność, że korzyści płynące z projektu zostały zidentyfikowane i są monitorowane.

W **fazie 5** proponowane rozwiązania są przekształcane w praktyczne działania. Istnieje możliwość zdefiniowania miar i wprowadzenia procesu monitorowania na podstawie celów i mierników COBIT w celu osiągnięcia i utrzymania dopasowania działalności biznesowej oraz możliwości pomiaru sprawności. Powodzenie tych działań wymaga wyraźnego zaangażowania i udziału kierownictwa najwyższego szczebla, a także przejęcia własności przez odpowiednich interesariuszy w odniesieniu do funkcji biznesowej oraz IT.

Działania w **fazie 6** koncentrują się na zrównoważonym wykorzystaniu nowych lub udoskonalonych czynników umożliwiających i monitorowaniu uzyskania spodziewanych korzyści.

W trakcie **fazy 7** weryfikuje się ogólny sukces inicjatywy, identyfikuje dalsze wymagania dotyczące nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi oraz wzmacnia potrzebę ciągłego doskonalenia.

Z czasem cykl życia powinien być realizowany w sposób iteracyjny w trakcie budowania zrównoważonego podejścia do nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi.

Rozpoczęcie: przygotowanie uzasadnienia biznesowego

W celu zapewnienia skutecznej realizacji inicjatyw na rzecz wdrożenia z wykorzystaniem metodyki COBIT konieczne jest powszechne uznanie i zakomunikowanie potrzeby działania w ramach przedsiębiorstwa. Może ono mieć formę „dzwonka alarmowego" (odnoszącego się do określonych punktów zapalnych omówionych wcześniej) bądź komunikatu dotyczącego szansy udoskonalenia, która ma zostać wykorzystana, oraz, co bardzo ważne, korzyści, które zostaną osiągnięte. Należy określić właściwy stopień pilności, a kluczowi interesariusze powinni być świadomi ryzyka związanego z niepodjęciem odpowiednich działań oraz korzyści płynących z realizacji programu.

Za realizację inicjatywy powinien odpowiadać sponsor; musi ona również obejmować wszystkich kluczowych interesariuszy i opierać się na uzasadnieniu biznesowym. Początkowo może ona mieć charakter ogólny, strategiczny (odgórny). Pierwszym krokiem powinno być jasne określenie pożądanych wyników biznesowych, kolejnym zaś — szczegółowy opis kluczowych zadań oraz etapów (kamieni milowych), a także kluczowych ról i zakresów odpowiedzialności. Uzasadnienie biznesowe to cenne narzędzie, za pomocą którego kierownictwo może ukierunkować sposób tworzenia wartości biznesowej. Uzasadnienie biznesowe musi uwzględniać co najmniej następujące elementy:

- docelowe korzyści biznesowe, ich zgodność ze strategią biznesową oraz powiązani beneficjenci (kto w przedsiębiorstwie będzie odpowiadać za ich zapewnienie). Podstawą mogą być punkty zapalne i zdarzenia inicjujące.
- Zmiany biznesowe wymagane do uzyskania przewidzianej wartości. Podstawą mogą być kontrole kondycji oraz analizy luk potencjału; należy również określić elementy mieszczące się w zakresie oraz te, które się w nim nie mieszczą.
- Inwestycje wymagane do wprowadzenia zmian dotyczących nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi (na podstawie szacunków dotyczących wymaganych projektów).
- Bieżące koszty IT i koszty biznesowe.
- Oczekiwane korzyści z funkcjonowania po dokonaniu zmian.
- Ryzyko związane z wcześniejszymi punktami, w tym wszelkie ograniczenia i zależności (na podstawie wyzwań i czynników sukcesu).
- Role, zakresy odpowiedzialności i rozliczalności związane z inicjatywą.
- Sposób monitorowania inwestycji i tworzenia wartości w ramach pełnego cyklu życia ekonomicznego oraz mierniki, które zostaną wykorzystane (na podstawie celów i mierników).

Uzasadnienie biznesowe nie jest jednorazowym statycznym dokumentem, ale dynamicznym narzędziem operacyjnym, które musi być stale aktualizowane w celu odzwierciedlenia aktualnego obrazu przyszłej sytuacji, tak aby można było zachować wgląd w opłacalność programu.

Kwantyfikacja korzyści płynących z realizacji inicjatyw związanych z wdrożeniem lub doskonaleniem może być trudne, i należy zadbać o to, aby skupiono się tylko na korzyściach, które są realistyczne i możliwe do osiągnięcia. Badania przeprowadzone w wielu przedsiębiorstwach mogą dostarczyć przydatnych informacji o korzyściach, które zostały osiągnięte.

PRZYKŁAD 6 — NADZÓR NAD STATYSTYKAMI IT

ITGI zleciła firmie PwC realizację projektu badania rynku dotyczącego nadzoru nad technologiami informatycznymi[7]. W badaniu wzięło udział ponad 800 respondentów odpowiedzialnych za działalność biznesową oraz IT w 21 krajach. 38% respondentów wskazało niższe koszty IT jako wynik praktyk w zakresie nadzoru nad technologiami informatycznymi, 28,1% wskazało większą konkurencyjność biznesową, natomiast 27,1% wskazało wyższy zwrot z inwestycji w IT. Ponadto wskazano szereg mniej wymiernych korzyści, takich jak lepsze zarządzanie ryzykiem związanym z IT (42,2% respondentów), skuteczniejsza komunikacja oraz relacje między działalnością biznesową i IT (39,6% respondentów) oraz usprawniona realizacja celów biznesowych dzięki wykorzystaniu IT (37,3% respondentów).

ISACA przeprowadziła również badania[8] w celu określenia i wykazania wartości biznesowej metodyki COBIT. Zbiór danych uzyskanych podczas badań stwarza możliwość przeprowadzania wielu analiz i pozwala na jasne określenie relacji między nadzorem nad technologiami informatycznymi w przedsiębiorstwie i wynikami działalności biznesowej.

W kolejnym badaniu przeprowadzonym w 250 przedsiębiorstwach na całym świecie ustalono, że rentowność przedsiębiorstw, w których zadbano o doskonały nadzór nad technologiami informatycznymi, była o co najmniej 20% wyższa niż w przypadku firm, w których nadzór był niewystarczający, przy założeniu, że realizowane cele były takie same[9]. Wyniki badania wskazują, że wartość biznesowa IT jest bezpośrednio związana ze skutecznością nadzoru nad IT.

Wyniki innego badania, przeprowadzonego wśród przedstawicieli branży lotniczej, wskazują, że wdrożenie nadzoru nad technologiami informatycznymi w przedsiębiorstwie oraz ciągły audyt przywróciły zaufanie między funkcją biznesową i funkcją IT oraz zapewniły lepsze dopasowanie inwestycji do celów strategicznych. Wskazano również bardziej wymierne korzyści, takie jak niższy koszt zapewnienia ciągłości IT na biznesową jednostkę produkcji oraz zwolnienie środków na wprowadzanie innowacji. Wyniki innych badań w sektorze finansowym wykazały, że organizacje, w których wprowadzono lepsze podejście do nadzoru nad technologiami informatycznymi, uzyskały wyższe wyniki w zakresie dojrzałości dopasowania działalności biznesowej/IT[10].

[7] ITGI, *Global Status Report on the Governance of Enterprise IT (GEIT)* — 2011, USA, 2011, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Global-Status-Report-on-the-Governance-of-Enterprise-IT-GEIT-2011.aspx*

[8] ISACA, *Building the Business Case for COBIT® and Val IT™ Executive Briefing*, USA, 2009, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Building-the-Business-Case-for-COBIT-and-Val-IT-Executive-Briefing.aspx*

[9] Weill, Peter; Jeanne W. Ross; *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, USA, 2004

[10] De Haes, Steven; Dirk Gemke; John Thorp; Wim Van Grembergen; 'Analyzing IT Value Management @ KLM Through the Lens of Val IT', *ISACA Journal*, 2011, vol 4. Van Grembergen, Wim; Steven De Haes; *Enterprise Governance of IT: Achieving Alignment and Value*, Springer, USA, 2009

Strona celowo pozostawiona pusta

Rozdział 8
Model potencjału procesu COBIT 5

Wprowadzenie

Użytkownicy metodyki COBIT 4.1, Risk IT oraz Val IT znają modele dojrzałości procesów zawarte w tych strukturach. Modele te wykorzystuje się do pomiaru aktualnej dojrzałości („tak jest") związanych z IT procesów realizowanych w przedsiębiorstwie, definiowania wymaganego stanu dojrzałości („tak ma być") oraz określania luki między nimi, a także sposobu udoskonalenia procesu w celu uzyskania pożądanego poziomu dojrzałości.

Do produktów COBIT 5 należy również model potencjału procesu oparty na uznanej międzynarodowej normie ISO/IEC 15504 Software Engineering — Process Assessment (Inżynieria oprogramowania — ocena procesów). Ten model umożliwia realizację tych samych ogólnych celów związanych z oceną procesu oraz wsparcia w doskonaleniu procesów, tj. zapewnia środki pomiaru sprawności każdego z procesów nadzoru (opartych na domenie EDM) lub procesów zarządzania (opartych na domenie PBRM) oraz umożliwia identyfikację obszarów wymagających usprawnień.

Ten nowy model różni się jednak od modelu dojrzałości COBIT 4.1 projektem i sposobem korzystania, i z tego powodu omówiono następujące tematy:
- różnice między modelem COBIT 5 i modelem COBIT 4.1;
- korzyści związane z wykorzystaniem metodyki COBIT 5;
- podsumowanie różnic, które użytkownicy metodyki COBIT 5 napotkają w praktyce;
- dokonywanie oszacowania potencjału w ramach metodyki COBIT 5.

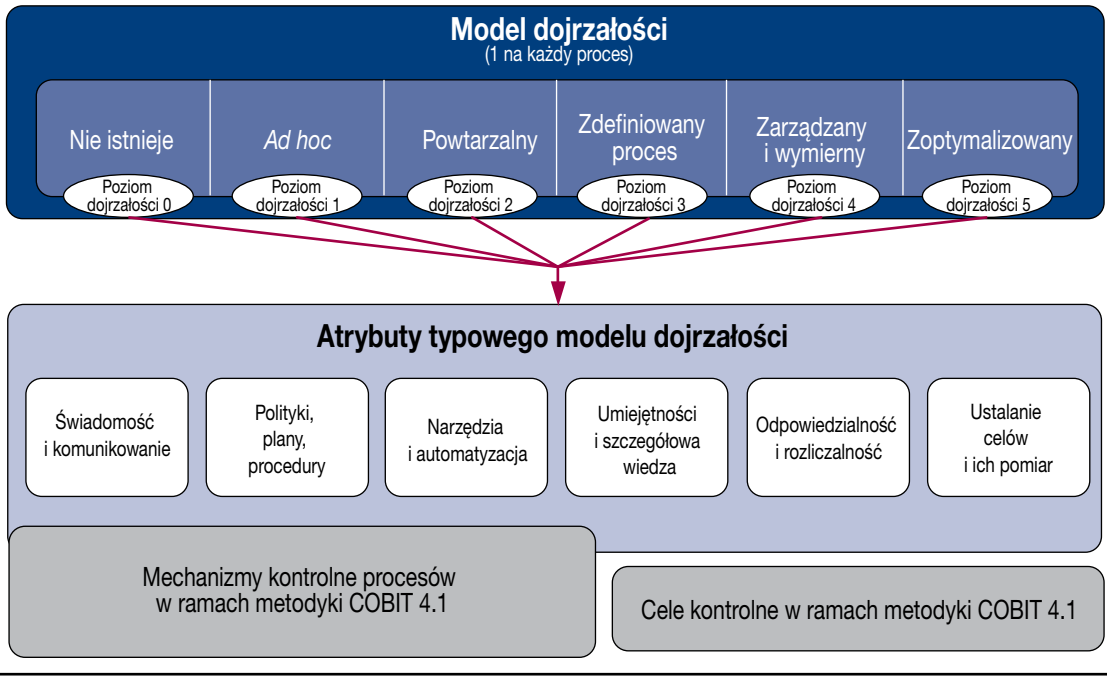
Szczegóły podejścia do oszacowania potencjału w ramach metodyki COBIT 5 są zawarte w publikacji ISACA *COBIT® Model oceny procesu (ang. Process Assessment Model – PAM): Using COBIT® 4.1*[11].

Choć to podejście zapewni cenne informacje dotyczące stanu procesów, procesy są tylko jednym z siedmiu czynników umożliwiających dotyczących nadzoru nad ryzykiem i zarządzania nim. W związku z tym oszacowanie procesów nie zapewni pełnego obrazu stanu nadzoru w danym przedsiębiorstwie. Z tego powodu należy również ocenić pozostałe czynniki umożliwiające.

Różnice między modelem dojrzałości COBIT 4.1 i modelem potencjału procesu COBIT 5

Elementy podejścia opartego na modelu dojrzałości COBIT 4.1 przedstawiono na **ilustracji 18**.

Ilustracja 18 — Podsumowanie modelu dojrzałości COBIT 4.1



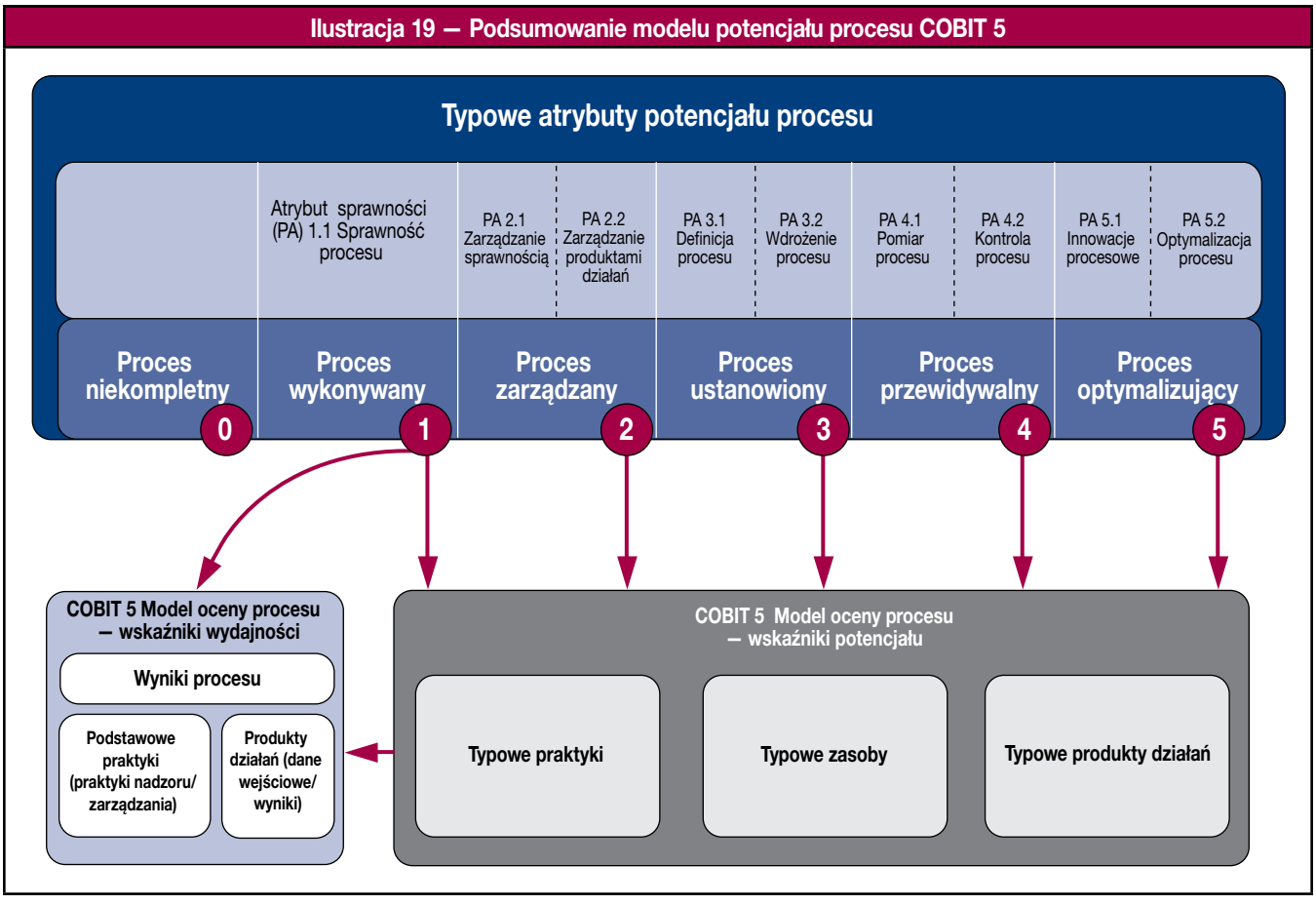
Wykorzystanie modelu dojrzałości COBIT 4.1 dla celów koniecznego doskonalenia procesów (oszacowanie dojrzałości procesu, definiowanie docelowego poziomu dojrzałości oraz zidentyfikowanie luk) z wykorzystaniem następujących komponentów metodyki COBIT 4.1:

[11] *www.isaca.org/cobit-pam*

- po pierwsze konieczne było dokonanie oszacowania w celu stwierdzenia, czy zrealizowano cele kontrolne dla procesów.
- Następnie można było wykorzystać model dojrzałości zawarty w wytycznych kierownictwa dla każdego procesu w celu uzyskania profilu dojrzałości procesu.
- Ponadto typowy model dojrzałości w metodyce COBIT 4.1 zawierał sześć osobnych atrybutów możliwych do zastosowania w odniesieniu do poszczególnych procesów i ułatwiających uzyskanie bardziej szczegółowego wglądu w poziom dojrzałości procesów.
- Mechanizmy kontrolne procesów stanowią typowe cele kontrolne — muszą również być weryfikowane podczas dokonywania oceny procesów. Mechanizmy kontrolne procesów częściowo pokrywają się z atrybutami typowego modelu dojrzałości.

Podejście do potencjału procesu w ramach metodyki COBIT 5 można podsumować w sposób przedstawiony na **ilustracji 19**.

Ilustracja 19 — Podsumowanie modelu potencjału procesu COBIT 5



Istnieje sześć poziomów potencjału, które może osiągnąć proces. Jednym z nich jest oznaczenie „proces niekompletny” — w przypadku, gdy praktyki w ramach procesu nie umożliwiają osiągnięcia zamierzonego celu procesu:

- **0 Proces niekompletny** — proces nie został wdrożony lub jego cel nie został osiągnięty. Na tym poziomie nie istnieją dowody systematycznej realizacji celu procesu lub ich liczba jest znikoma.
- **1 Proces wykonywany** (jeden atrybut) — cel wdrożonego procesu został osiągnięty.
- **2 Proces zarządzany** (dwa atrybuty) — opisany wyżej proces wykonywany został wdrożony w sposób zarządzany (zapewniono planowanie, monitorowanie i dostosowanie), a jego produkty działań są właściwie określone, kontrolowane i utrzymywane.
- **3 Proces ustanowiony** (dwa atrybuty) — opisany wcześniej proces zarządzany jest wdrażany za pomocą zdefiniowanego procesu umożliwiającego osiągnięcie wyniku procesu.
- **4 Proces przewidywalny** (dwa atrybuty) — opisany wcześniej proces ustanowiony działa teraz w ramach zdefiniowanych limitów w celu osiągnięcia wyników procesu.
- **5 Proces optymalizujący** (dwa atrybuty) — opisany wcześniej proces przewidywalny jest nieustannie doskonalony w celu realizacji istotnych aktualnych i projektowanych celów biznesowych.

Każdy z poziomów potencjału może zostać osiągnięty tylko wtedy, gdy w pełni uzyskano niższy poziom. Na przykład: poziom 3 potencjału procesu (proces ustanowiony) wymaga zdefiniowania procesu oraz osiągnięcia (w znacznym stopniu) atrybutów wdrożenia — oprócz pełnego osiągnięcia wszystkich atrybutów poziomu 2 potencjału procesu (proces zarządzany).

Poziom 1 potencjału procesu w sposób istotny różni się od wyższych poziomów potencjału. Osiągnięcie poziomu 1 potencjału procesu wymaga osiągnięcia (w znacznym stopniu) atrybutu sprawności procesu, co oznacza, że proces jest skutecznie realizowany, a przedsiębiorstwo uzyskuje wymagane wyniki. Na kolejnych poziomach potencjału dodawane są kolejne atrybuty. W tym schemacie szacowania osiągnięcie poziomu 1 potencjału (nawet jeśli poziomów jest pięć) już stanowi ważne osiągnięcie dla przedsiębiorstwa. Warto zauważyć, że każde przedsiębiorstwo powinno wybrać

(na podstawie rachunku kosztów i korzyści oraz analizy wykonalności) poziom docelowy lub pożądany, który bardzo rzadko będzie jednym z najwyższych poziomów.

Najważniejsze różnice między oszacowaniem potencjału procesu na podstawie normy ISO/IEC 15504 i aktualnym modelem dojrzałości COBIT 4.1 (oraz podobnymi modelami dojrzałości opartymi na domenie Val IT i Risk IT) można streścić w następujący sposób:
- nazewnictwo i znaczenie poziomów potencjału zdefiniowanych w normie ISO/IEC 15504 jest zupełnie inne niż w przypadku aktualnych poziomów dojrzałości procesów w ramach metodyki COBIT 4.1.
- W przypadku normy ISO/IEC 15504 poziomy potencjału definiuje się za pomocą zbioru dziewięciu atrybutów procesów. Atrybuty te częściowo dotyczą tych samych kwestii, do których odnoszą się aktualne atrybuty dojrzałości i/lub mechanizmy kontrolne procesów w ramach metodyki COBIT 4.1 — ale jedynie w ograniczonym stopniu i w inny sposób.

Zgodnie z wymogami dotyczącymi modelu referencyjnego procesu opartego na normie ISO/IEC 15504:2 opis każdego procesu, który będzie podlegał oszacowaniu, tj. każdego procesu zarządzania i/lub nadzoru w ramach metodyki COBIT 5, musi spełniać następujące kryteria:
- opis procesu zawiera jego cel i wyniki.
- Opis procesu nie może zawierać żadnych aspektów struktury pomiarów wykraczających poza poziom 1, co oznacza, że w opisie procesu nie może pojawić się żadna cecha atrybutu procesu wykraczająca poza poziom 1. Niezależnie od tego, czy proces podlega pomiarowi i monitorowaniu, czy też został formalnie opisany itd., nie może on stać się częścią opisu procesu ani żadnej z praktyk/ żadnego z działań w ramach zarządzania, leżących u jego podstaw. Oznacza to, że opisy procesów — przedstawione w przewodniku *COBIT 5: Procesy umożliwiające* — zawierają wyłącznie kroki konieczne do osiągnięcia rzeczywistych zamiarów i celów procesu.
- Na podstawie powyższych punktów wspólne atrybuty możliwe do zastosowania w odniesieniu do wszystkich procesów przedsiębiorstwa, powodujące powielenie celów kontrolnych w publikacji *COBIT® 3rd Edition* i zgrupowane w ramach celów procesów kontrolnych (PC) w metodyce COBIT 4.1, zdefiniowano obecnie na poziomach 2–5 modelu oszacowania.

Różnice w praktyce[12]

Z wcześniejszych opisów wynika jasno, że istnieją pewne praktyczne różnice związane ze zmianą w modelach oceny procesów. Użytkownicy muszą być świadomi tych zmian i przygotować się do uwzględnienia ich w planach działania.

Podstawowe zmiany wymagające rozważenia:
- choć ze względu na pozorne podobieństwa skal numerycznych oraz słów użytych do ich opisania kuszące wydaje się porównanie wyników oszacowania dojrzałości organizacji oraz potencjału procesów uzyskanych w oparciu o metodyki COBIT 4.1 i COBIT 5, porównanie takie jest jednak trudne ze względu na różnice w zakresie, ukierunkowaniu i intencjach — co jest zobrazowane na **ilustracji 20**.
- Zasadniczo w przypadku modelu potencjału procesu w ramach metodyki COBIT 5 wyniki będą niższe, co pokazano na **ilustracji 20**. W przypadku modelu dojrzałości COBIT 4.1 proces mógł osiągnąć poziom 1 lub 2 bez pełnego osiągnięcia wszystkich celów procesu; w odniesieniu do poziomu potencjału procesu w ramach metodyki COBIT 5 można w ten sposób uzyskać niższy wynik (0 lub 1).

Można uznać, że skala COBIT 4.1 jest w przybliżony sposób odwzorowana w skali potencjału COBIT 5, co przedstawiono na **ilustracji 20.**
- W metodyce COBIT 5 zrezygnowano z osobnego modelu dojrzałości dla każdego procesu wraz ze szczegółami dotyczącymi treści procesu, ponieważ sposób oszacowania potencjału procesu oparty na normie ISO/IEC 15504 nie tylko nie wymaga takiego podejścia, ale wręcz je uniemożliwia. Zamiast tego podejście definiuje informacje wymagane w „modelu referencyjnym procesu” (model procesu, który zostanie wykorzystany dla celów oceny):
  – opis procesu ze wskazanym celem;
  – podstawowe praktyki, stanowiące odpowiednik praktyk nadzoru nad procesami lub zarządzania nimi w kategoriach stosowanych w metodyce COBIT 5;
  – produkty działań, stanowiące odpowiednik danych wejściowych i wyników w kategoriach stosowanych w metodyce COBIT 5.
- Model dojrzałości COBIT 4.1 pozwalał uzyskać profil dojrzałości przedsiębiorstwa. Głównym celem tego profilu było ustalenie, w których wymiarach lub dla których atrybutów istniały niedociągnięcia wymagające usprawnienia. Podejście to zostało wykorzystane przez przedsiębiorstwa, gdy większy nacisk kładziono na udoskonalenie niż potrzebę uzyskania konkretnego poziomu dojrzałości dla celów raportowania. W modelu oszacowania potencjału COBIT 5 wskazano skalę pomiarową dla każdego atrybutu potencjału oraz wytyczne dotyczące jego stosowania, w efekcie czego w przypadku każdego procesu można dokonać oszacowania dla każdego z dziewięciu atrybutów potencjału.
- Atrybuty dojrzałości COBIT 4.1 oraz atrybuty potencjału procesów COBIT 5 nie są identyczne. Atrybuty te w pewnym stopniu pokrywają się, co przedstawiono na **ilustracji 21**. Przedsiębiorstwa, które wcześniej korzystały z podejścia opartego na atrybutach modelu dojrzałości w metodyce COBIT 4.1, mogą ponownie wykorzystać istniejącą ocenę i dokonać jej ponownej klasyfikacji zgodnie z atrybutami COBIT 5, biorąc pod uwagę **ilustrację 21**.

[12] Więcej informacji na temat nowego programu COBIT Assessment Programme opartego na normie ISO/IEC 15504 można znaleźć na stronie *www.isaca.org/cobit-assessment-programme.*

Ilustracja 20 — Tabela porównawcza poziomów dojrzałości (COBIT 4.1) oraz poziomów potencjału procesu (COBIT 5)

Poziom modelu dojrzałości COBIT 4.1	Potencjał procesu na podstawie ISO/IEC 15504	Kontekst
5 Zoptymalizowane — procesy zostały dopracowane do poziomu dobrej praktyki w oparciu o rezultaty ciągłego doskonalenia i modelowania dojrzałości w innych przedsiębiorstwach. Technologia informatyczna jest wykorzystywana w zintegrowany sposób do automatyzacji przepływu pracy, zapewniając narzędzia w celu poprawy jakości i skuteczności, sprawiając, że przedsiębiorstwo szybko adaptuje się do zmieniających się warunków.	**Poziom 5: Proces optymalizujący** — proces przewidywalny na poziomie 4 jest nieustannie doskonalony w celu realizacji istotnych aktualnych i projektowanych celów biznesowych.	**Punkt widzenia przedsiębiorstwa — wiedza korporacyjna**
4 Zarządzane i mierzalne — kierownictwo monitoruje i ocenia zgodność z procedurami, a także podejmuje odpowiednie czynności, gdy procesy nie działają efektywnie. Procesy są stale doskonalone i stanowią źródło dobrych praktyk. W ograniczony lub fragmentaryczny sposób wykorzystywane są zautomatyzowane rozwiązania oraz narzędzia.	**Poziom 4: Proces przewidywalny** — proces ustanowiony na poziomie 3 działa teraz w ramach zdefiniowanych ograniczeń w celu osiągnięcia wyników procesu.	
3 Zdefiniowany proces — istnieją ustandaryzowane i udokumentowane procedury, które zostały zakomunikowane poprzez szkolenie. Pracownicy są zobowiązani do ich stosowania. Jest jednak mało prawdopodobne, że odstępstwa od stosowania procedur zostaną wykryte. Procedury nie są zaawansowane, a są raczej formalizacją istniejących praktyk.	**Poziom 3: Proces ustanowiony** — proces zarządzany na poziomie 2 został wdrożony w taki sposób, że jest on zdefiniowanym procesem umożliwiającym osiągnięcie celów procesu.	
	Poziom 2: Proces zarządzany — proces wykonywany na poziomie 1 został wdrożony w taki sposób, że jest on zarządzany (zapewniono planowanie, monitorowanie i dostosowanie), a jego produkty działań są właściwie określone, kontrolowane i utrzymywane.	**Punkt widzenia jednostki — wiedza indywidualna**
2 Powtarzalne lecz intuicyjne — procesy zostały rozwinięte do poziomu, na którym różne osoby wykonujące to samo zadanie postępują zgodnie z podobnymi procedurami. Nie ma formalnych szkoleń, standardowe procedury nie zostały zakomunikowane, a podjęcie odpowiedzialności pozostawiono jednostkom. Występuje wysoki poziom zależności od wiedzy poszczególnych osób, dlatego prawdopodobne jest występowanie błędów.	**Poziom 1: Proces wykonywany** — wdrożony proces osiąga swoje cele. **Uwaga: Istnieje możliwość, że niektóre procesy sklasyfikowane w ramach Modelu dojrzałości jako 1 zostaną sklasyfikowane w 15504 jako 0 — jeśli nie osiągnięto wyników procesu.**	
1 Wstępne/*Ad hoc* — istnieje potwierdzenie tego, że przedsiębiorstwo dostrzegło problemy wraz z koniecznością ich rozwiązania. Nie są to jednak ustandaryzowane procesy. Zamiast nich do rozwiązywania poszczególnych problemów stosuje się podejście *ad hoc*. Ogólne podejście do zarządzania nie jest podejściem zorganizowanym.		
0 Nieistniejące — całkowity brak rozpoznawalnych procesów. Przedsiębiorstwo nie dostrzegło nawet istnienia problemu, który wymaga rozwiązania.	**Poziom 0: Proces niekompletny** — proces nie został wdrożony lub jego cel nie jest osiągany.	

Ilustracja 21 — Tabela porównawcza atrybutów dojrzałości (COBIT 4.1) oraz atrybutów procesów (COBIT 5)

Atrybut dojrzałości COBIT 4.1	Atrybut potencjału procesu COBIT 5								
	Sprawność procesu	Zarządzanie sprawnością	Zarządzanie produktami działań	Definiowanie procesu	Wdrażanie procesu	Pomiar procesu	Kontrola procesu	Innowacja procesowa	Optymalizacja procesu
Świadomość i komunikowanie				■	■	■			
Polityki, plany i procedury							■		
Narzędzia i automatyzacja				■					
Umiejętności i szczegółowa wiedza				■	■				
Odpowiedzialność i rozliczalność				■					
Ustalanie celów i pomiar		■				■			

Korzyści płynące z wprowadzenia zmian

Korzyści związane z wykorzystaniem modelu potencjału procesów COBIT 5 (w porównaniu z modelami dojrzałości COBIT 4.1):

- większe skupienie się na realizowanym procesie w celu potwierdzenia, że jego cel został osiągnięty i umożliwia uzyskanie wymaganych wyników;
- uproszczenie zawartości dzięki wyeliminowaniu przypadków powielania się treści. Ocena w modelu dojrzałości COBIT 4.1 w celu wspierania oceny procesów wymagała użycia szeregu komponentów, w tym typowego modelu dojrzałości, modeli dojrzałości procesu, celów kontrolnych oraz mechanizmów kontrolnych procesów;
- większa niezawodność i powtarzalność działań szacowania i oceny potencjału procesu, ograniczająca dyskusje i nieporozumienia między interesariuszami dotyczące rezultatów oszacowania;
- większa użyteczność rezultatów szacowania potencjału procesów, ponieważ nowy model stanowi podstawę

dokonania bardziej formalnej, rygorystycznej oceny — zarówno dla celów wewnętrznych, jak i potencjalnych celów zewnętrznych;
- zgodność z ogólnie akceptowanym standardem oceny procesów, a co za tym idzie — silne wsparcie podejścia do oceny procesu na rynku.

Dokonywanie oszacowania potencjału procesów w ramach metodyki COBIT 5

Zgodnie z normą ISO/IEC 15504 oszacowane potencjału procesu może zostać dokonane w różnych celach z różnym stopniem rygoryzmu. Cele mogą mieć charakter wewnętrzny i dotyczyć porównania między obszarami przedsiębiorstwa i/lub dotyczyć udoskonalenia procesów z myślą o korzyściach wewnętrznych albo też mogą mieć charakter zewnętrzny i dotyczyć formalnego oszacowania, raportowania i certyfikacji.

Podejście do oszacowania według COBIT 5 oparte na normie ISO/IEC 15504 ułatwia realizację następujących celów stanowiących kluczowe podejście COBIT od roku 2000:
- umożliwienie organowi nadzorującemu i kierownictwu porównanie potencjału procesów;
- umożliwienie wysokopoziomowego określenia przybliżonego stanu aktualnego („jak jest") oraz stanu wymaganego („jak ma być") w celu ułatwienia organowi nadzorującemu i kierownictwu podejmowania decyzji inwestycyjnych w odniesieniu do usprawnienia procesu;
- zapewnienie analizy luk oraz informacji dotyczących planowania udoskonaleń w celu ułatwienia procesu definiowania możliwych do uzasadnienia projektów związanych z doskonaleniem;
- zapewnienie organowi nadzorującemu oraz kierownictwu klasyfikacji ocen, które umożliwią pomiar i monitorowanie aktualnego potencjału.

W tej części opisano sposób dokonywania ogólnej oceny z wykorzystaniem modelu potencjału procesów w ramach metodyki COBIT 5 z myślą o osiągnięciu tych celów.

W ramach oceny rozróżnia się poziom 1 potencjału oraz wyższe poziomy. Jak wspomniano wcześniej, na poziomie 1 potencjału procesu ustala się, czy zamierzony cel procesu został osiągnięty, co oznacza, że osiągnięcie tego poziomu jest bardzo ważne. Stanowi to ponadto fundament umożliwiający osiągnięcie wyższych poziomów potencjału.

Oszacowanie, czy cel procesu został osiągnięty (lub, inaczej mówiąc, czy potencjał procesu osiągnął poziom 1), może zostać dokonane w następujący sposób:
1. Weryfikacja wyników procesu na podstawie ich charakterystyki zawartej w szczegółowych opisach procesów i wykorzystanie skali ocen ISO/IEC 15504 do przypisania ratingu określającego stopień, w jakim osiągnięto cel. Skala składa się z następujących ocen:
   - **N** (nie osiągnięto) — na tym poziomie nie istnieją dowody osiągania zdefiniowanego atrybutu w ocenianym procesie lub ich liczba jest znikoma. (uzyskanie 0–15%)
   - **P** (częściowo osiągnięto) — istnieją pewne dowody na zbliżanie się do zdefiniowanego atrybutu w ocenianym procesie i częściowe osiąganie go. Niektóre aspekty osiągnięcia atrybutu mogą być niemożliwe do przewidzenia. (uzyskanie 15–50%)
   - **L** (w znacznym stopniu osiągnięto) — istnieją dowody systematycznego zbliżania się do zdefiniowanego atrybutu w ocenianym procesie i znacznego osiągania go. W ocenianym procesie mogą istnieć pewne słabości związane z tym atrybutem. (uzyskanie 50–85%)
   - **F** (w pełni osiągnięto) — istnieją dowody kompletnego i systematycznego zbliżania się do zdefiniowanego atrybutu w ocenianym procesie i pełnego osiągania go. W ocenianym procesie nie stwierdzono istotnych słabości związanych z tym atrybutem. (uzyskanie 85–100%)
2. Ponadto praktyki w ramach procesu (nadzoru lub zarządzania) mogą zostać oszacowane za pomocą tej samej skali ocen, wyrażającej stopień, w jakim zastosowano podstawowe praktyki.
3. Z myślą o dalszym dopracowaniu oceny można również uwzględnić produkty działań w celu ustalenia stopnia, w jakim osiągnięto dany atrybut oceny.

Choć zdefiniowanie docelowych poziomów potencjału zależy od decyzji poszczególnych przedsiębiorstw, ambicją wielu z nich będzie zapewnienie poziomu 1 potencjału w przypadku wszystkich procesów. (W innym wypadku jak byłby sens realizowania tych procesów?) Jeśli nie osiągnięto tego poziomu, powody są od razu znane dzięki wyjaśnionemu powyżej podejściu i można zdefiniować plan doskonalenia:
1. Jeśli wymagany wynik procesu nie jest konsekwentnie uzyskiwany, proces nie osiąga swojego celu i musi zostać udoskonalony.
2. Oszacowanie praktyk procesów pozwoli na ustalenie, których praktyk brakuje, a które nie spełniają swojego zadania, co pozwala na wdrożenie i/lub udoskonalenie tych praktyk z myślą o osiągnięciu wszystkich wyników procesów.

W przypadku wyższych poziomów potencjału procesów wykorzystuje się typowe praktyki oparte na normie ISO/IEC 15504:2. Zawierają one ogólne opisy dla każdego z poziomów potencjału.

Strona celowo pozostawiona pusta

Załącznik A
Materiały źródłowe

Poniższe metodyki, normy oraz inne wytyczne zostały wykorzystane jako materiały referencyjne oraz dane wejściowe podczas prac nad metodyką COBIT 5.

Association for Project Management (APM); *APM Introduction to Programme Management*, Latimer, Trend and Co., Wielka Brytania, 2007

British Standards Institute (BSI), BS25999:2007 Business Continuity Management Standard, Wielka Brytania, 2007

CIO Council, *Federal Enterprise Architecture* (FEA), wer. 1.0, Stany Zjednoczone, 2005

Komisja Europejska, *The Commission Enterprise IT Architecture Framework (CEAF)*, Belgia, 2006

Kotter, John; *Leading Change*, Harvard Business School Press, Stany Zjednoczone, 1996

HM Government, Best Management Practice Portfolio, *Managing Successful Programmes (MSP)*, Wielka Brytania, 2009

HM Government, Best Management Practice Portfolio, *PRINCE2®*, Wielka Brytania, 2009

HM Government, Best Management Practice Portfolio, *Information Technology Infrastructure Library* (*ITIL®),* 2011

Międzynarodowa Organizacja Normalizacyjna (ISO), 9001:2008 Quality Management Standard, Szwajcaria, 2008

ISO/Międzynarodowa Komisja Elektrotechniczna (IEC), 20000:2006 IT Service Management Standard, Szwajcaria, 2006

ISO/IEC, 27005:2008, Information Security Risk Management Standard, Szwajcaria, 2008

ISO/IEC, 38500:2008, Corporate Governance of Information Technology Standard, Szwajcaria, 2008

King Code of Governance Principles (King III), Republika Południowej Afryki, 2009

Organizacja Współpracy Gospodarczej i Rozwoju (OECD), *OECD Principles of Corporate Governance*, Francja, 2004

The Open Group, TOGAF® 9, Wielka Brytania, 2009

Project Management Institute, Project Management Body of Knowledge (PMBOK2®), Stany Zjednoczone, 2008

UK Financial Reporting Council, 'Combined Code on Corporate Governance', Wielka Brytania, 2009

Strona celowo pozostawiona pusta

Załącznik B
Szczegółowe mapowanie celów przedsiębiorstwa na cele związane z IT

Kaskadę celów COBIT 5 wyjaśniono w rozdziale 2.

Celem tabeli dotyczącej mapowania przedstawionej na **ilustracji 22** jest wskazanie sposobu, w jaki cele przedsiębiorstwa mogą być wspierane przez (lub przekładane na) cele związane z IT. Z tego powodu tabela zawiera następujące informacje:
- w kolumnach przedstawiono 17 typowych celów przedsiębiorstwa zdefiniowanych w metodyce COBIT 5, podzielonych na grupy zgodnie z wymiarem BSC (ang. Business Score Card — Zrównoważona Karta Wyników);
- w wierszach przedstawiono 17 celów związanych z IT, również pogrupowanych zgodnie z wymiarami IT BSC;
- mapowanie sposobu, w jaki każdy z celów przedsiębiorstwa jest wspierany przez cele związane z IT. Mapowanie wyrażono za pomocą następującej skali:
  - P (ang. Primary) oznacza relację podstawową, a więc istotną, tj. cel związany z IT ma podstawowe znaczenie dla realizacji celu przedsiębiorstwa;
  - S (ang. Secondary) oznacza relację wspierającą, wciąż silną, ale mniej istotną, tj. cel związany z IT ma drugorzędne znaczenie dla realizacji celu przedsiębiorstwa.

PRZYKŁAD 7 — TABELA DOTYCZĄCA MAPOWANIA

Tabela dotycząca mapowania sugeruje, iż zwykle należy się spodziewać, że:
- cel przedsiębiorstwa 7. Ciągłość i dostępność usług biznesowych:
  - zależy przede wszystkim od osiągnięcia celów związanych z IT:
    - 04 Zarządzanie ryzykiem biznesowym związanym z IT
    - 10 Bezpieczeństwo informacji, infrastruktury przetwarzania i aplikacji
    - 14 Dostępność wiarygodnych i przydatnych informacji wspierających proces decyzyjny
  - zależy również, choć w mniejszym stopniu, od osiągnięcia celów związanych z IT:
    - 01 Zgodność IT z biznesowymi celami strategicznymi
    - 07 Dostarczanie usług IT zgodnie z wymogami biznesowymi
    - 08 Adekwatne wykorzystanie aplikacji, informacji i rozwiązań w zakresie technologii
- Korzystanie z tabeli w przeciwnym kierunku z osiągnięciem celu związanego z IT 09. Zwinność IT ułatwi osiągnięcie kilku celów przedsiębiorstwa:
  - przede wszystkim następujących celów przedsiębiorstwa:
    - 2. Portfel konkurencyjnych produktów i usług
    - 8. Zwinność w reagowaniu na zmieniające się otoczenie biznesowe
    - 11. Optymalizacja funkcjonalności procesów biznesowych
    - 17. Kultura innowacji produktów i biznesu
  - w mniejszym stopniu następujących celów przedsiębiorstwa:
    - 1. Wartość inwestycji biznesowych dla interesariuszy
    - 3. Zarządzane ryzyko biznesowe (ochrona zasobów)
    - 6. Kultura usług zorientowanych na klienta
    - 13. Zarządzanie programami biznesowymi — zmiany biznesowe
    - 14. Wydajność pracowników i działań operacyjnych
    - 16. Wykwalifikowany i zmotywowany personel

Tabelę opracowano na podstawie następujących danych wejściowych:
- wyniki badań przeprowadzonych przez Antwerp Management School, IT Alignment and Governance Research Institute;
- dodatkowe recenzje oraz opinie ekspertów uzyskane w procesie rozwoju i weryfikacji metodyki COBIT 5.

Gdy korzysta się z tabeli przedstawionej na ilustracji 22, należy uwzględnić zawarte w rozdziale 2 uwagi dotyczące sposobu korzystania z kaskady celów COBIT 5.

Ilustracja 22 — Mapowanie celów przedsiębiorstwa w ramach metodyki COBIT 5 na cele związane z IT

			Cel przedsiębiorstwa																
			Wartość inwestycji biznesowych dla interesariuszy	Portfel konkurencyjnych produktów i usług	Zarządzane ryzyko biznesowe (ochrona zasobów)	Zgodność z przepisami prawa i regulacjami	Przejrzystość finansowa	Kultura usług zorientowanych na klienta	Ciągłość i dostępność usług biznesowych	Zwinność w reagowaniu na zmieniające się otoczenie biznesowe	Świadome podejmowanie decyzji strategicznych na podstawie informacji	Optymalizacja kosztów świadczenia usług	Optymalizacja funkcjonalności procesów biznesowych	Optymalizacja kosztów procesów biznesowych	Zarządzanie programami biznesowymi — zmiany biznesowe	Wydajność pracowników i działań operacyjnych	Zgodność z politykami wewnętrznymi	Wykwalifikowany i zmotywowany personel	Kultura innowacji produktów i biznesu
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
		Cel związany z IT	Finanse					Klient					Obszar wewnętrzny					Szkolenie i rozwój	
Finanse	01	Zgodność IT z biznesowymi celami strategicznymi	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	Zgodność IT oraz wsparcie w zakresie zgodności działalności z przepisami prawa i regulacjami			S	P											P		
	03	Zaangażowanie kadry zarządzającej w podejmowanie decyzji związanych z IT	P	S	S					S	S		S		P			S	S
	04	Zarządzanie ryzykiem biznesowym związanym z IT			P	S			P	S		P			S		S	S	
	05	Uzyskane korzyści z inwestycji i portfela usług związanych z IT	P	P				S		S		S	S	P		S			S
	06	W obszarze IT: przejrzystość kosztów, korzyści i ryzyka	S		S		P				S	P		P					
Klient	07	Dostarczanie usług IT zgodnie z wymogami biznesowymi	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Adekwatne wykorzystanie aplikacji, informacji i rozwiązań w zakresie technologii	S	S	S			S	S		S	S	P	S		P		S	S
Obszar wewnętrzny	09	Zwinność IT (ang. agility)	S	P	S			S		P			P		S	S		S	P
	10	Bezpieczeństwo informacji, infrastruktury przetwarzania i aplikacji			P	P			P								P		
	11	Optymalizacja aktywów, zasobów i potencjału związanych z IT	P	S						S		P	S	P	S	S			S
	12	Umożliwianie i wsparcie realizacji procesów biznesowych poprzez integrację aplikacji i rozwiązań technologicznych z procesami biznesowymi	S	P	S			S		S		S	P	S	S	S			S
	13	Realizacja programów przynoszących korzyści — w sposób terminowy, w ramach budżetu i zgodnie z wymogami i standardami jakościowymi	P	S	S			S				S		S	P				
	14	Dostępność wiarygodnych i przydatnych informacji wspierających proces decyzyjny	S	S	S	S			P		P		S						
	15	Zgodność IT z politykami wewnętrznymi			S	S											P		
Szkolenie i rozwój	16	Kompetentny i zmotywowany personel działu biznesowego i działu IT	S	S	P			S		S						P		P	S
	17	Wiedza, kompetencje oraz inicjatywy w zakresie innowacji biznesowych	S	P				S		P	S		S		S			S	P

Załącznik C
Szczegółowe mapowanie celów związanych z IT na procesy związane z IT

Ten załącznik zawiera tabelę dotyczącą mapowania między celami związanymi z IT i sposobem, w jaki są one wspierane przez procesy związane z IT w ramach kaskady celów wyjaśnionej w rozdziale 2.

Ilustracja 23 zawiera następujące elementy:
- w kolumnach przedstawiono 17 typowych celów związanych z IT zdefiniowanych w rozdziale 2, podzielonych na grupy zgodnie z wymiarem IT BSC;
- w wierszach przedstawiono wszystkie 37 procesów COBIT 5 pogrupowanych zgodnie z domenami;
- mapowanie sposobu, w jaki każdy z celów związanych z IT jest wspierany przez proces COBIT 5 związany z IT. Mapowanie wyrażono za pomocą następującej skali:
  – P (ang. Primary) oznacza relację podstawową, a więc istotną, tj. odpowiedni proces COBIT 5 ma podstawowe znaczenie dla realizacji celu związanego z IT.
  – S (ang. Secondary) oznacza relację wspierającą, wciąż silną, ale mniej istotną, tj. odpowiedni proces COBIT 5 ma drugorzędne znaczenie dla realizacji celu związanego z IT.

PRZYKŁAD 8 – APO13 ZARZĄDZANIE BEZPIECZEŃSTWEM

Proces APO13 *Zarządzanie bezpieczeństwem* :
- przede wszystkim ułatwia osiągnięcie następujących celów związanych z IT:
  – 02 Zgodność IT oraz wsparcie w zakresie zgodności działalności z przepisami prawa i regulacjami
  – 04 Zarządzanie ryzykiem biznesowym związanym z IT
  – 06 Przejrzystość kosztów, korzyści i ryzyka związanych z IT
  – 10 Bezpieczeństwo informacji, infrastruktury przetwarzania i aplikacji
  – 14 Dostępność wiarygodnych i przydatnych informacji wspierających proces decyzyjny
- w mniejszym stopniu ułatwia osiągnięcie następujących celów związanych z IT:
  – 07 Dostarczanie usług IT zgodnie z wymogami biznesowymi
  – 08 Adekwatne wykorzystanie aplikacji, informacji i rozwiązań w zakresie technologii

Tabelę opracowano na podstawie następujących danych wejściowych:
- wyniki badań przeprowadzonych przez Antwerp Management School, IT Alignment and Governance Research Institute;
- dodatkowe recenzje oraz opinie ekspertów uzyskane w procesie rozwoju i weryfikacji metodyki COBIT 5.

Gdy korzysta się z tabeli przedstawionej na ilustracji 23, należy uwzględnić zawarte w rozdziale 2 uwagi dotyczące sposobu korzystania z kaskady celów COBIT 5.

Ilustracja 23 — Mapowanie celów związanych z IT w ramach metodyki COBIT 5 na procesy

			Cel związany z IT																
			01 Zgodność IT z biznesowymi celami strategicznymi	02 Zgodność IT oraz wsparcie w zakresie zgodności działalności z przepisami prawa i regulacjami	03 Zaangażowanie kadry zarządzającej w podejmowanie decyzji związanych z IT	04 Zarządzanie ryzykiem biznesowym związanym z IT	05 Uzyskanie korzyści z inwestycji i portfela usług związanych z IT	06 W obszarze IT: przejrzystość kosztów, korzyści i ryzyka	07 Dostarczanie usług IT zgodnie z wymogami biznesowymi	08 Adekwatne wykorzystanie aplikacji, informacji i rozwiązań w zakresie technologii	09 Zwinność IT (ang. agility)	10 Bezpieczeństwo informacji, infrastruktury przetwarzania i aplikacji	11 Optymalizacja aktywów, zasobów i potencjału związanych z IT	12 Umożliwianie i wsparcie realizacji procesów biznesowych poprzez integrację aplikacji i rozwiązań technologicznych z procesami biznesowymi	13 Realizacja programów przynoszących korzyści — w sposób terminowy, w ramach budżetu i zgodnie z wymogami i standardami jakościowymi	14 Dostępność wiarygodnych i przydatnych informacji wspierających proces decyzyjny	15 Zgodność IT z politykami wewnętrznymi	16 Kompetentny i zmotywowany personel działu biznesowego i działu IT	17 Wiedza, kompetencje oraz inicjatywy w zakresie innowacji biznesowych
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
		Proces COBIT 5	Finanse						Klient		Obszar wewnętrzny							Szkolenie i rozwój	
Ocena, kierowanie i monitorowanie	EDM01	Zapewnienie i utrzymanie ładu korporacyjnego	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Zapewnienie realizacji korzyści	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Zapewnienie optymalizacji ryzyka	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Zapewnienie optymalizacji zasobów	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Zapewnienie przejrzystości dotyczącej interesariuszy	S	S	P			P	P						S	S	S		S
Dopasowanie, planowanie i organizacja	APO01	Zarządzanie metodyką zarządzania IT	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Zarządzanie strategią	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Zarządzanie architekturą korporacyjną	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Zarządzanie innowacjami	S			S	P			P	P		P	S		S			P
	APO05	Zarządzanie portfelem projektów	P		S	S	P	S	S	S	S		S		P				S
	APO06	Zarządzanie budżetem i kosztami	S		S	S	P	P	S	S			S		S				
	APO07	Zarządzanie zasobami ludzkimi	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Zarządzanie relacjami	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Zarządzanie umowami o świadczenie usług	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Zarządzanie dostawcami		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Zarządzanie jakością	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Zarządzanie ryzykiem		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Zarządzanie bezpieczeństwem		P		P		P	S	S		P				P			

Ilustracja 23 — Mapowanie celów związanych z IT w ramach metodyki COBIT 5 na procesy *(ciąg dalszy)*

			Cel związany z IT																
			Zgodność IT z biznesowymi celami strategicznymi	Zgodność IT oraz wsparcie w zakresie zgodności działalności z przepisami prawa i regulacjami	Zaangażowanie kadry zarządzającej w podejmowanie decyzji związanych z IT	Zarządzanie ryzykiem biznesowym związanym z IT	Uzyskanie korzyści z inwestycji i portfela usług związanych z IT	W obszarze IT: przejrzystość kosztów, korzyści i ryzyka	Dostarczanie usług IT zgodnie z wymogami biznesowymi	Adekwatne wykorzystanie aplikacji, informacji i rozwiązań w zakresie technologii	Zwinność IT (ang. agility)	Bezpieczeństwo informacji, infrastruktury przetwarzania i aplikacji	Optymalizacja aktywów, zasobów i potencjału związanych z IT	Umożliwianie i wsparcie realizacji procesów biznesowych poprzez integrację aplikacji i rozwiązań technologicznych z procesami biznesowymi	Realizacja programów przynoszących korzyści — w sposób terminowy, w ramach budżetu i zgodnie z wymogami i standardami jakościowymi	Dostępność wiarygodnych i przydatnych informacji wspierających proces decyzyjny	Zgodność IT z politykami wewnętrznymi	Kompetentny i zmotywowany personel działu biznesowego i działu IT	Wiedza, kompetencje oraz inicjatywy w zakresie innowacji biznesowych
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
		Proces COBIT 5	**Finanse**						**Klient**		**Obszar wewnętrzny**							**Szkolenie i rozwój**	
Budowanie, nabywanie i wdrażanie	BAI01	Zarządzanie programami i projektami	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Zarządzanie definiowaniem wymagań	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Zarządzanie identyfikacją i budowaniem rozwiązań	S			S	S		P	S			S	S	S	S			S
	BAI04	Zarządzanie dostępnością i pojemnością				S	S		P	S	S		P		S	P			S
	BAI05	Zarządzanie wdrażaniem zmian organizacyjnych	S		S		S		S	P	S		S	S	P				P
	BAI06	Zarządzanie zmianami			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Zarządzanie procesem akceptacji zmian i przejścia				S	S		S	P	S			P	S	S	S		S
	BAI08	Zarządzanie wiedzą	S				S		S	S	P	S	S			S		S	P
	BAI09	Zarządzanie zasobami		S		S		P	S		S	S	P			S	S		
	BAI10	Zarządzanie konfiguracją		P		S		S		S	S	S	P			P	S		
Dostarczanie, obsługa i wsparcie	DSS01	Zarządzanie eksploatacją		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Zarządzanie zgłoszeniami serwisowymi i incydentami				P			P	S		S				S	S		S
	DSS03	Zarządzanie problemami		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Zarządzanie ciągłością	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Zarządzanie usługami bezpieczeństwa	S	P		P			S	S		P	S	S		S	S		
	DSS06	Zarządzanie mechanizmami kontrolnymi procesów biznesowych		S		P			P	S		S	S	S		S	S	S	S
Monitorowanie, ocena i oszacowanie	MEA01	Monitorowanie, ocena i oszacowanie wydajności i zgodności	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Monitorowanie, ocena i oszacowanie systemu kontroli wewnętrznej		P		P		S	S	S		S				S	P		S
	MEA03	Monitorowanie, ocena i oszacowanie zgodności z wymogami zewnętrznymi		P		P	S		S			S					S		S

Strona celowo pozostawiona pusta

Załącznik D
Potrzeby interesariuszy oraz cele przedsiębiorstwa

W rozdziale 4 przedstawiono poszczególne etapy kaskady celów, od potrzeb interesariuszy po cele czynników umożliwiających. W rozdziale 2 przedstawiono tabelę zawierającą typowe pytania dotyczące nadzoru nad technologiami informatycznymi i zarządzania nimi. Z punktu widzenia interesariuszy ciekawa jest kwestia powiązania tych pytań z celami przedsiębiorstwa. W związku z tym do publikacji włączono **ilustrację 24**, na której przedstawiono sposób, w jaki można powiązać listę potrzeb wewnętrznych interesariuszy z celami przedsiębiorstwa.

Tabelę tę można wykorzystać do wyznaczenia szczegółowych celów przedsiębiorstwa lub celów związanych z IT oraz określenia ich priorytetów na podstawie określonych potrzeb interesariuszy. Gdy korzysta się z tych tabel, należy zachować takie same środki ostrożności jak w przypadku innych tabel z kaskadami celów. Sytuacja każdego przedsiębiorstwa jest inna i dlatego tabele te nie powinny być wykorzystywane w sposób mechaniczny, lecz stanowią jedynie sugerowany typowy zbiór relacji. Na **ilustracji 24** punkt przecięcia potrzeby interesariusza oraz celu przedsiębiorstwa jest wypełniony, jeśli dana potrzeba powinna zostać uwzględniona w odniesieniu do tego celu.

Ilustracja 24 — Mapowanie celów przedsiębiorstwa w ramach metodyki COBIT 5 na pytania dotyczące nadzoru i zarządzania

POTRZEBY INTERESARIUSZY	1. Wartość inwestycji biznesowych dla interesariuszy	2. Portfel konkurencyjnych produktów i usług	3. Zarządzane ryzyko biznesowe (ochrona zasobów)	4. Zgodność z przepisami prawa i regulacjami	5. Przejrzystość finansowa	6. Kultura usług zorientowanych na klienta	7. Ciągłość i dostępność usług biznesowych	8. Zwinność w reagowaniu na zmieniające się otoczenie biznesowe	9. Świadome podejmowanie decyzji strategicznych na podstawie informacji	10. Optymalizacja kosztów świadczenia usług	11. Optymalizacja funkcjonalności procesów biznesowych	12. Optymalizacja kosztów procesów biznesowych	13. Zarządzanie programami biznesowymi – zmiany biznesowe	14. Wydajność pracowników i działań operacyjnych	15. Zgodność z politykami wewnętrznymi	16. Wykwalifikowany i zmotywowany personel	17. Kultura innowacji produktów i biznesu
W jaki sposób uzyskuje się wartość z inwestycji w IT? Czy użytkownicy końcowi są zadowoleni z jakości usług IT?	■	■				■	■						■			■	■
W jaki sposób zarządza się sprawnością technologii informatycznych?		■			■				■	■	■	■		■			
Jaki jest najlepszy sposób wykorzystania nowych technologii w kontekście nowych strategicznych szans dla przedsiębiorstwa?	■	■						■					■			■	■
Jaki jest optymalny sposób utworzenia i ustrukturyzowania działu IT?								■		■	■	■		■	■	■	
W jakim stopniu jestem uzależniony od zewnętrznych dostawców? Jak wypada ocena sprawności zarządzania umowami o outsourcing IT? Jak można zapewnić audyt dotyczący zewnętrznych dostawców?			■	■						■							
Jakie są wymogi (kontrolne) w odniesieniu do informacji?				■					■						■		
Czy uwzględniłem całe ryzyko związane z IT?			■				■		■						■		
Czy realizowane przeze mnie operacje IT są efektywne i elastyczne?					■		■										
Jak kontroluje się koszt IT? Jaki jest najbardziej skuteczny i wydajny sposób wykorzystania zasobów IT? Jakie są najbardziej skuteczne i wydajne opcje zaopatrzenia?										■		■		■			

Ilustracja 24 — Mapowanie celów przedsiębiorstwa w ramach metodyki COBIT 5 na pytania dotyczące nadzoru i zarządzania *(ciąg dalszy)*

POTRZEBY INTERESARIUSZY	Wartość inwestycji biznesowych dla interesariuszy 1.	Portfel konkurencyjnych produktów i usług 2.	Zarządzane ryzyko biznesowe (ochrona zasobów) 3.	Zgodność z przepisami prawa i regulacjami 4.	Przejrzystość finansowa 5.	Kultura usług zorientowanych na klienta 6.	Ciągłość i dostępność usług biznesowych 7.	Zwinność w reagowaniu na zmieniające się otoczenie biznesowe 8.	Świadome podejmowanie decyzji strategicznych na podstawie informacji 9.	Optymalizacja kosztów świadczenia usług 10.	Optymalizacja funkcjonalności procesów biznesowych 11.	Optymalizacja kosztów procesów biznesowych 12.	Zarządzanie programami biznesowymi — zmiany biznesowe 13.	Wydajność pracowników i działań operacyjnych 14.	Zgodność z politykami wewnętrznymi 15.	Wykwalifikowany i zmotywowany personel 16.	Kultura innowacji produktów i biznesu 17.
Czy liczba pracowników odpowiedzialnych za IT jest wystarczająca? W jaki sposób można rozwijać i utrzymywać ich umiejętności oraz jak zarządza się ich sprawnością?										■		■		■			
W jaki sposób zapewnia się audyt IT?				■											■		
Czy informacje, które przetwarzam, są dobrze zabezpieczone?			■	■			■								■		
Jak można poprawić zwinność biznesową dzięki bardziej elastycznemu środowisku IT?	■							■								■	■
Czy projekty IT nie przynoszą spodziewanych rezultatów — a jeśli tak, dlaczego? Czy IT stanowi przeszkodę w realizacji strategii biznesowej?	■	■	■					■			■	■	■				
Jak dużą rolę odgrywa IT w utrzymaniu funkcjonowania przedsiębiorstwa? Jak postępować w przypadku braku dostępności IT?	■	■					■										
Jakie konkretne najważniejsze procesy biznesowe zależą od technologii informatycznych i jakie są wymogi dotyczące procesów biznesowych?	■	■									■	■					
Ile wynosiła średnia wartość przekroczenia budżetów operacyjnych IT? Jak często i w jakim stopniu projekty IT przekraczają wyznaczony budżet?					■					■		■		■			
Jaka część działań w ramach IT dotyczy rozwiązywania pilnych problemów, nie zaś wspierania udoskonaleń działalności biznesowej?		■	■									■					
Czy dostępne zasoby oraz infrastruktura IT są wystarczające do realizacji strategicznych celów przedsiębiorstwa?		■			■					■		■					
Jak długo trwa proces podejmowania najważniejszych decyzji dotyczących IT?	■	■			■			■									
Czy wszystkie działania i inwestycje związane z IT są transparentne?		■		■	■										■		
Czy technologie informatyczne ułatwiają przedsiębiorstwu zachowanie zgodności z regulacjami oraz poziomami usług? Jak mogę sprawdzić, czy przestrzegam wszystkich obowiązujących regulacji?				■											■		

Załącznik E
Zestawienie metodyki COBIT 5 ze stosownymi powiązanymi standardami i metodykami

Wprowadzenie

W tym załączniku porównano metodykę COBIT 5 z najistotniejszymi wykorzystywanymi standardami i metodykami w obszarze nadzoru. W przypadku normy ISO/IEC 38500 porównanie oparto na zasadach normy ISO/IEC 38500; w przypadku innych porównań wykorzystany został format tabeli, w której procesy COBIT 5 zostały zestawione z równoważnymi treściami w przywoływanym standardzie lub metodyce.

COBIT 5 oraz ISO/IEC 38500

Poniżej podsumowano sposób, w jaki metodyka COBIT 5 wspiera przyjęcie opisanych w normie zasad oraz podejścia do wdrożenia. Norma *ISO/IEC 38500:2008–Corporate governance of information technology* opiera się na sześciu kluczowych zasadach. Wyjaśniono praktyczne implikacje każdej z zasad, a także sposób, w jaki wytyczne COBIT 5 umożliwiają przyjęcie dobrych praktyk.

Zasady ISO/IEC 38500

ZASADA 1 — ODPOWIEDZIALNOŚĆ

Co to oznacza w praktyce:

Funkcja biznesowa (klient) oraz IT (dostawca) powinny współpracować w ramach modelu partnerskiego, wykorzystując efektywną komunikację opartą na pozytywnych i zaufanych relacjach oraz precyzyjnie określając zakresy rozliczalności i odpowiedzialności. W przypadku większych przedsiębiorstw komitet wykonawczy ds. IT (nazywany również komitetem strategicznym ds. IT), działający w imieniu zarządu (pod przewodnictwem członka zarządu), to bardzo efektywny organ umożliwiający ocenę, ukierunkowanie i monitorowanie wykorzystania IT w przedsiębiorstwie oraz doradzający zarządowi w kluczowych kwestiach związanych z IT. Dyrektorzy małych i średnich przedsiębiorstw o prostszej strukturze decyzyjnej i krótszych ścieżkach komunikacji muszą przyjąć bardziej bezpośrednie podejście podczas nadzorowania działań IT. We wszystkich przypadkach właściwe struktury organizacyjne, role i zakresy odpowiedzialności w odniesieniu do nadzoru muszą otrzymać odpowiednie uprawnienia od organu nadzorującego, który określa, kto podejmuje kluczowe decyzje, wykonuje zadania i jest za nie rozliczany. Powinno to uwzględniać relacje z kluczowymi zewnętrznymi dostawcami usług IT.

W jaki sposób wytyczne ISACA umożliwiają wykorzystanie dobrych praktyk:

1. W metodyce COBIT 5 zdefiniowano szereg czynników umożliwiających w odniesieniu do nadzoru nad technologiami informatycznymi w przedsiębiorstwie. Szczególnie istotne w tym kontekście są: czynnik umożliwiający „proces” oraz czynnik umożliwiający „struktury organizacyjne” w połączeniu z tabelami RACI[13]. W ich ramach w sposób wyraźny wspierane jest przydzielenie odpowiedzialności i przedstawiono w nich przykładowe role i zakresy odpowiedzialności dla członków zarządu oraz kierownictwa w odniesieniu do wszystkich powiązanych kluczowych procesów i działań.
2. W przewodniku *COBIT 5 — Wdrożenie* wyjaśniono zakresy odpowiedzialności interesariuszy oraz innych zaangażowanych stron w przypadku wdrażania lub optymalizowania ustaleń dotyczących nadzoru nad IT.
3. W ramach metodyki COBIT 5 wyróżnia się dwa poziomy monitorowania. Pierwszy poziom jest istotny w kontekście nadzoru. Proces EDM05 *Zapewnienie przejrzystości dotyczącej interesariuszy* wyjaśnia rolę dyrektora w monitorowaniu i ocenie nadzoru nad IT oraz sprawności IT za pomocą typowej metody określania celów i zadań oraz powiązanych mierników.

ZASADA 2 — STRATEGIA

Co to oznacza w praktyce:

Planowanie strategiczne IT to złożone i kluczowe przedsięwzięcie wymagające ścisłej koordynacji między ogólnofirmowymi planami jednostki biznesowej oraz planami strategicznymi IT. Bardzo istotne jest również przypisanie najwyższego priorytetu planom, które z największym prawdopodobieństwem zapewnią osiągnięcie pożądanych korzyści, a także efektywne przypisanie zasobów. Cele ogólne wymagają przełożenia na możliwe do realizacji plany taktyczne w celu zmniejszenia liczby usterek i niespodzianek. Celem jest zapewnienie wartości wspierającej realizację celów strategicznych, a zarazem uwzględnienie powiązanego ryzyka w odniesieniu do określonego przez zarząd apetytu na ryzyko. Choć ważne jest kaskadowanie planów w sposób odgórny, plany muszą być również elastyczne i łatwe do dostosowania, tak aby można było spełnić szybko zmieniające się wymogi biznesowe oraz wykorzystać szanse IT.

Ponadto istnienie potencjału IT (lub jego brak) może ułatwić (lub utrudnić) realizację strategii biznesowych; w związku z tym planowanie strategiczne IT powinno uwzględniać przejrzyste i odpowiednie planowanie potencjału IT. Powinno ono obejmować oszacowanie potencjału obecnej infrastruktury IT oraz zasobów ludzkich z myślą o spełnieniu przyszłych

[13] W tabelach RACI określono osoby odpowiedzialne, rozliczane, konsultowane oraz informowane w przypadku danego zadania.

wymagań biznesowych oraz z uwzględnieniem przyszłych rozwiązań technologicznych, które mogą zapewnić przewagę konkurencyjną i/lub optymalizację kosztów. Zasoby IT obejmują relacje z wieloma zewnętrznymi dostawcami produktów i usług — niektórzy z nich mogą odgrywać kluczową rolę we wspieraniu działalności. Nadzór nad strategicznym zaopatrzeniem jest więc bardzo istotnym działaniem w ramach planowania strategicznego wymagającym kierowania i nadzorowania na poziomie zarządu.

W jaki sposób wytyczne ISACA umożliwiają wykorzystanie dobrych praktyk:

1. Metodyka COBIT 5 zapewnia szczegółowe wytyczne dotyczące zarządzania inwestycjami w IT oraz (zwłaszcza w przypadku procesu EDM02 *Zapewnienie realizacji korzyści* w domenie nadzoru) sposobu, w jaki realizacja celów strategicznych powinna być poparta odpowiednimi uzasadnieniami biznesowymi (ang. business cases).
2. W ramach domeny APO metodyki COBIT 5 wyjaśniono procesy wymagane do efektywnego planowania i organizacji wewnętrznych i zewnętrznych zasobów IT, z uwzględnieniem planowania strategicznego, planowania technologii i architektury, planowania organizacyjnego, planowania innowacji, zarządzania portfelem projektów, zarządzania inwestycjami, zarządzania ryzykiem, zarządzania relacjami oraz zarządzania jakością. Wyjaśniono również uzgodnienie celów biznesowych z celami IT i podano typowe przykłady sposobu, w jaki wspierają one realizację celów strategicznych dla wszystkich procesów związanych z IT na podstawie badań prowadzonych w całej branży.
3. Identyfikacja oraz dopasowanie celów przedsiębiorstwa i celów związanych z IT umożliwia lepsze zrozumienie kaskadowych zależności między celami przedsiębiorstwa, celami związanymi z IT i czynnikami umożliwiającymi, w tym procesami IT. Przedstawiono bardzo pomocną listę 17 typowych celów przedsiębiorstwa oraz 17 typowych celów związanych z IT, zweryfikowanych i uszeregowanych wg istotności w różnych sektorach. W połączeniu z informacją o powiązaniach między obiema grupami celów stanowi ona solidną podstawę, na której można zbudować typową kaskadę celów biznesowych do celów IT.

ZASADA 3 — NABYCIE

Co to oznacza w praktyce:

Rozwiązania IT istnieją, aby wspierać wspierające realizację procesów biznesowych, i w związku z tym należy zadbać, aby nie rozważano rozwiązań IT w izolacji ani nie traktowano ich jedynie jako projektu lub usługi o charakterze technologicznym. Z drugiej strony niewłaściwy wybór architektury technologicznej, niezapewnienie bieżącej i odpowiedniej infrastruktury technicznej lub brak wykwalifikowanych zasobów ludzkich może skutkować niepowodzeniem realizacji projektu, brakiem możliwości utrzymania operacji biznesowych bądź obniżeniem wartości dla przedsiębiorstwa. Nabycie zasobów IT powinno zostać ocenione w szerszym kontekście zmiany biznesowej wspieranej przez IT. Nabyta technologia musi również wspierać i wykorzystywać istniejące i planowane procesy biznesowe oraz infrastruktury IT. Wdrożenie również nie jest tylko problemem technologicznym, lecz stanowi połączenie zmiany organizacyjnej, weryfikacji procesów biznesowych, szkolenia oraz wspierania zmian. W związku z tym projekty IT powinny być częścią szerszych programów zmian ogólnofirmowych, uwzględniających inne projekty obejmujące pełny zakres działań wymaganych do uzyskania korzystnych rezultatów.

W jaki sposób wytyczne ISACA umożliwiają wykorzystanie dobrych praktyk:

1. W ramach domeny EDM metodyki COBIT 5 przedstawiono wytyczne dotyczące nadzoru nad inwestycjami biznesowymi wspieranymi przez IT oraz zarządzania nimi w całym cyklu ich życia (nabycie, wdrożenie, eksploatacja i wycofanie z użycia). Proces APO05 *Zarządzanie portfelem projektów* odnosi się do sposobu zapewnienia efektywnego zarządzania portfelem projektów i programami w odniesieniu do takich inwestycji z myślą o zapewnieniu realizacji korzyści i optymalizacji kosztów.
2. Domena APO w ramach metodyki COBIT 5 obejmuje wytyczne dotyczące planowania nabywania, obejmującego planowanie inwestycji, zarządzanie ryzykiem, planowanie programów i projektów oraz planowanie jakości.
3. Domena BAI w ramach metodyki COBIT 5 obejmuje wytyczne dotyczące procesów wymaganych do nabycia i wdrożenia rozwiązań IT, obejmujących definiowanie wymogów, identyfikację wykonalnych rozwiązań, przygotowanie dokumentacji oraz szkolenie użytkowników i pracowników wsparcia w celu umożliwienia im korzystania z nowych systemów. Przedstawiono również wytyczne, które pomogą zapewnić właściwe testowanie i kontrolę rozwiązań, gdy zmianę wprowadza się w środowisku operacyjnym (biznesowym oraz IT).
4. Domena MEA oraz proces EDM05 w ramach metodyki COBIT 5 obejmują wytyczne dotyczące sposobu, w jaki dyrektorzy mogą monitorować i oceniać proces nabywania oraz wewnętrzne mechanizmy kontrolne w celu zapewnienia właściwej realizacji procesu nabywania i zarządzania nim.

ZASADA 4 — SPRAWNOŚĆ

Co to oznacza w praktyce:

Skuteczny pomiar sprawności zależy od uwzględnienia dwóch kluczowych aspektów: jasnego zdefiniowania celów dotyczących sprawności oraz ustalenia efektywnych mierników pozwalających na monitorowanie realizacji celów. Konieczny jest również proces pomiaru sprawności, który zapewni spójne i wiarygodne monitorowanie sprawności. Warunkiem zapewnienia skutecznego nadzoru jest odgórne ustalenie celów i dopasowanie ich do ogólnych, zatwierdzonych celów biznesowych, a także oddolne określenie mierników i dopasowanie ich w sposób umożliwiający monitorowanie przez poszczególne poziomy kierownictwa osiągnięcia celów na wszystkich poziomach. Można wskazać dwa kluczowe czynniki sukcesu nadzoru: zatwierdzenie celów przez interesariuszy oraz akceptacja rozliczalności za osiągnięcie celów przez dyrektorów i kierowników. IT to złożone, techniczne zagadnienie; w związku z tym ważne

jest zapewnienie przejrzystości poprzez wyrażenie celów, mierników i raportów dotyczących wydajności w języku zrozumiałym dla interesariuszy, tak aby można było podjąć odpowiednie działania.

W jaki sposób wytyczne ISACA umożliwiają wykorzystanie dobrych praktyk:

1. W ramach metodyki COBIT 5 przedstawiono typowe przykłady celów i mierników dla pełnego zakresu procesów związanych z IT oraz pozostałych czynników umożliwiających i pokazano, w jaki sposób wiążą się one z celami biznesowymi, umożliwiając przedsiębiorstwom dostosowanie ich do swoich potrzeb.
2. Metodyka COBIT 5 zapewnia kierownictwu wytyczne dotyczące ustalania celów IT zgodnie z celami biznesowymi i opisuje sposób monitorowania realizacji tych celów na podstawie wyznaczonych celów biznesowych i mierników. Potencjał procesu można oszacować za pomocą modelu szacowania potencjału zapewnienia zgodności, opartego na normie ISO/IEC 15504.
3. Dwa kluczowe procesy metodyki COBIT 5 obejmują szczegółowe wytyczne:
   – APO02 *Zarządzanie strategią* koncentruje się na ustalaniu celów.
   – APO09 *Zarządzanie umowami o świadczenie usług* koncentruje się na definiowaniu właściwych usług oraz celów usług i dokumentowaniu ich w umowach SLA.
4. W procesie MEA01 *Monitorowanie, ocena i oszacowanie wydajności i zgodności* metodyka COBIT 5 zapewnia wytyczne dotyczące zakresu odpowiedzialności kadry zarządzającej za te działania.
5. W planowanym przewodniku *COBIT 5 —Audyt* wyjaśniono sposób, w jaki specjaliści ds. audytu mogą przeprowadzić niezależny audyt sprawności IT dla dyrektorów.

ZASADA 5 — ZGODNOŚĆ

Co to oznacza w praktyce:

Na obecnym światowym rynku, korzystającym z możliwości, jakie stwarza Internet i zaawansowane technologie, przedsiębiorstwa muszą spełnić coraz większą liczbę wymogów prawnych i regulacyjnych. Skandale w korporacjach oraz porażki finansowe, których świadkami byliśmy w ostatnich latach, zwiększyły świadomość zarządów w zakresie istnienia oraz implikacji bardziej restrykcyjnych przepisów i regulacji. Interesariusze w coraz większym stopniu wymagają zapewnienia, że przedsiębiorstwa przestrzegają przepisów i regulacji oraz stosują dobre praktyki w zakresie ładu korporacyjnego w swoim środowisku działania. Ponadto fakt, że technologie informatyczne umożliwiły płynną realizację procesów biznesowych między przedsiębiorstwami, sprawił, że pojawiła się rosnąca potrzeba uwzględnienia w umowach ważnych wymogów związanych z IT w obszarach takich jak prywatność, poufność, własność intelektualna i bezpieczeństwo.

Dyrektorzy muszą zadbać o uwzględnienie zgodności z wymogami zewnętrznymi w procesie planowania strategicznego, ponieważ zapewnienie zgodności po poniesieniu szkody będzie kosztowne. Muszą również określić najważniejsze wytyczne oraz wprowadzić polityki i procedury oraz wyegzekwować ich przestrzeganie przez kierownictwo i personel z myślą o osiągnięciu celów przedsiębiorstwa, ograniczeniu ryzyka i zapewnieniu zgodności z przepisami. Kierownictwo najwyższego szczebla musi zadbać o odpowiednią równowagę między sprawnością i zgodnością, tak aby cele dotyczące sprawności nie wpłynęły negatywnie na zgodność, a zarazem aby wymogi zapewniania zgodności były odpowiednie i nie ograniczały nadmiernie działalności biznesowej.

W jaki sposób wytyczne ISACA umożliwiają wykorzystanie dobrych praktyk:

1. Praktyki nadzoru i zarządzania w ramach metodyki COBIT 5 zapewniają podstawę umożliwiającą stworzenie odpowiedniego środowiska kontrolnego w przedsiębiorstwie. Oszacowanie potencjału procesu umożliwia kierownictwu ocenę i analizę porównawczą potencjału procesów IT.
2. Proces APO02 *Zarządzanie strategią* w ramach metodyki COBIT 5 ułatwia zapewnienie zgodności planu IT z ogólnymi celami biznesowymi z uwzględnieniem wymogów dotyczących nadzoru.
3. Proces MEA02 *Monitorowanie, ocena i oszacowanie systemu kontroli wewnętrznej* w ramach metodyki COBIT 5 umożliwia dyrektorom oszacowanie, czy mechanizmy kontrolne pozwalają na spełnienie wymogów w zakresie zgodności.
4. Proces MEA03 *Monitorowanie, ocena i oszacowanie zgodności z wymogami zewnętrznymi* w metodyce COBIT 5 ułatwia identyfikację zewnętrznych regulacji, umożliwia dyrektorom określenie wytycznych dotyczących zgodności, a także zapewnia monitorowanie, ocenę i raportowanie zgodności IT w ramach ogólnej zgodności z wymogami przedsiębiorstwa.
5. W planowanym przewodniku *COBIT 5 — Audyt* wyjaśniono sposób, w jaki audytorzy mogą zapewnić niezależny audyt zgodności i przestrzegania wewnętrznych polityk opartych na wewnętrznych wytycznych lub zewnętrznych wymogach prawnych, regulacyjnych lub wynikających z umów, w celu potwierdzenia, że odpowiedzialny właściciel procesu w wyznaczonym terminie podjął wszelkie konieczne działania naprawcze wymagane do usunięcia luk dotyczących zgodności.

ZASADA 6 — ZACHOWANIE PRACOWNIKÓW

Co to oznacza w praktyce:

Wdrożenie każdej zmiany wspieranej przez IT (dotyczy to również samego nadzoru nad IT) zwykle wymaga wprowadzenia istotnej zmiany związanej z kulturą korporacyjną i schematami zachowań w przedsiębiorstwach, a także w przypadku klientów i partnerów biznesowych. Może to wywołać obawy i nieporozumienia wśród personelu, dlatego wdrożeniem należy zarządzać w sposób ostrożny, aby utrzymać pozytywne zaangażowanie pracowników. Dyrektorzy muszą w jasny sposób przedstawiać cele i w sposób pozytywny wspierać wdrożenie proponowanych zmian. Szkolenie oraz doskonalenie umiejętności personelu to kluczowe aspekty zmiany — zwłaszcza jeśli wziąć pod uwagę szybkie tempo zmian w technologii. Z technologiami informatycznymi mają do czynienia osoby na wszystkich poziomach

przedsiębiorstwa — interesariusze, kierownictwo i użytkownicy, a także specjaliści zapewniający usługi i rozwiązania związane z IT wykorzystywane do celów biznesowych. Poza przedsiębiorstwem technologie informatyczne wpływają na klientów i partnerów biznesowych i w coraz większym stopniu umożliwiają samoobsługę i automatyczną realizację transakcji między przedsiębiorstwami (krajowych oraz transgranicznych). Choć procesy biznesowe wspierane przez IT niosą ze sobą nowe korzyści i szanse, wiążą się także z coraz większym ryzykiem. Rosną obawy związane z ochroną prywatności i ryzykiem oszustwa, i jeśli użytkownicy systemów IT mają darzyć je zaufaniem, konieczne jest właściwe zarządzanie tymi problemami oraz innymi rodzajami ryzyka. Systemy przetwarzające informacje mogą również bardzo istotnie wpłynąć na praktyki dotyczące pracy poprzez zautomatyzowanie procedur manualnych.

W jaki sposób wytyczne ISACA umożliwiają wykorzystanie dobrych praktyk:
Poniższe czynniki umożliwiające COBIT 5 (w tym procesy) zapewniają wytyczne dotyczące wymagań odnoszących się do zachowania pracowników:
1. Czynniki umożliwiające COBIT 5 obejmują ludzi, umiejętności i kompetencje oraz kulturę, etykę i zachowanie. Dla każdego czynnika umożliwiającego przedstawiono model dotyczący podejścia do obsługi czynnika umożliwiającego oraz podano przykłady.
2. Proces COBIT 5 APO07 *Zarządzanie zasobami ludzkimi* wyjaśnia sposób, w jaki wyniki pracowników powinny być dopasowane do celów korporacyjnych, sposób, w jaki należy utrzymywać specjalistyczne umiejętności w zakresie IT, oraz sposób definiowania ról i zakresów odpowiedzialności.
3. Proces COBIT 5 BAI02 *Zarządzanie definiowaniem wymagań* ułatwia projektowanie aplikacji w sposób spełniający wymagania dotyczące obsługi przez pracowników wsparcia i użytkowania.
4. Procesy COBIT 5 BAI05 *Zarządzanie wdrażaniem zmian organizacyjnych* oraz BAI08 *Zarządzanie wiedzą* zapewniają użytkownikom możliwość efektywnego korzystania z systemów.

Ponadto ISACA zapewnia cztery certyfikaty dla specjalistów odgrywających kluczowe role związane z nadzorem nad technologiami informatycznymi; korpus wiedzy, którego dotyczą, został w znacznej części ujęty w treści COBIT 5:
• Certified in the Governance of Enterprise IT® (CGEIT®);
• Certified Information Systems Auditor® (CISA®);
• Certified Information Security Manager® (CISM®);
• Certified in Risk and Information Systems Control™ (CRISC™).

Posiadacze tych certyfikatów wykazali zdolności i doświadczenie w pełnieniu tych ról.

ISO/IEC 38500 Ocena, kierowanie i monitorowanie
W JAKI SPOSÓB WYTYCZNE ISACA UMOŻLIWIAJĄ WYKORZYSTANIE DOBRYCH PRAKTYK:
Domena nadzoru w modelu procesów COBIT 5 obejmuje pięć procesów, a w ramach każdego z tych procesów zdefiniowano praktyki EDM (ang. Evaluate, Direct and Monitor — Ocena, Kierowanie i Monitorowanie). To podstawowa lokalizacja w metodyce COBIT 5, w której zdefiniowano działania związane z nadzorem.

Porównanie z innymi normami

Metodykę COBIT 5 opracowano z uwzględnieniem szeregu innych standardów i metodyk; standardy te wymieniono w załączniku A.

Przewodnik *COBIT 5: Procesy umożliwiające* zawiera ogólne mapowanie między każdym z procesów COBIT 5 oraz najistotniejszymi częściami powiązanych standardów i metodyk zawierających dodatkowe wytyczne.

W tej części przedstawiono krótkie omówienie każdej z metodyk lub standardów, wskazując obszary i domeny COBIT 5, do których się odnoszą.

ITIL® V3 2011 oraz ISO/IEC 20000
ITIL V3 2011 i ISO/IEC 20000 obejmują następujące obszary i domeny COBIT 5:
• podzbiór procesów w domenie DSS;
• podzbiór procesów w domenie BAI;
• niektóre procesy w domenie APO.

ISO/IEC serii 27000
Norma ISO/IEC 27000 obejmuje następujące obszary i domeny COBIT 5:
• procesy związane z bezpieczeństwem i ryzykiem w domenach EDM, APO oraz DSS;
• różne działania związane z bezpieczeństwem w ramach procesów w innych domenach;
• działania monitorujące i oceniające z domeny MEA.

ISO/IEC serii 31000
Norma ISO/IEC 31000 obejmuje następujące obszary i domeny COBIT 5:
• procesy związane z zarządzaniem ryzykiem w domenach EDM i APO.

TOGAF® 9

TOGAF 9 obejmuje następujące obszary i domeny COBIT 5:

- procesy związane z zasobami w domenie EDM (nadzór) — komponenty TOGAF 9 dotyczące Rady ds. Architektury, nadzoru nad architekturą oraz modeli dojrzałości architektury odpowiadają optymalizacji zasobów;
- proces związany z architekturą korporacyjną w domenie APO. Rdzeniem TOGAF 9 jest cykl Architecture Development Method (ADM), którego odwzorowaniem są praktyki COBIT 5 dotyczące rozwoju wizji architektury (faza A ADM), definiowania architektury referencyjnej (fazy B, C, D ADM), wyboru szans i rozwiązań (faza E ADM) oraz definiowania wdrożenia architektury (fazy F, G ADM). W praktyce COBIT 5 dotyczącej świadczenia usług w zakresie architektury korporacyjnej odwzorowano kilka komponentów TOGAF 9. Należą do nich:
  - Zarządzanie wymaganiami ADM;
  - Pryncypia architektury;
  - Zarządzanie interesariuszami;
  - Oszacowanie gotowości na przekształcenia działalności biznesowej;
  - Zarządzanie ryzykiem;
  - Planowanie oparte na potencjale;
  - Zgodność architektury;
  - Umowy dotyczące architektury.

Capability Maturity Model Integration (CMMI) (rozwój)

CMMI obejmuje następujące obszary i domeny COBIT 5:

- procesy związane z budowaniem aplikacji oraz nabyciem w domenie BAI;
- niektóre procesy organizacyjne i związane z jakością z domeny APO.

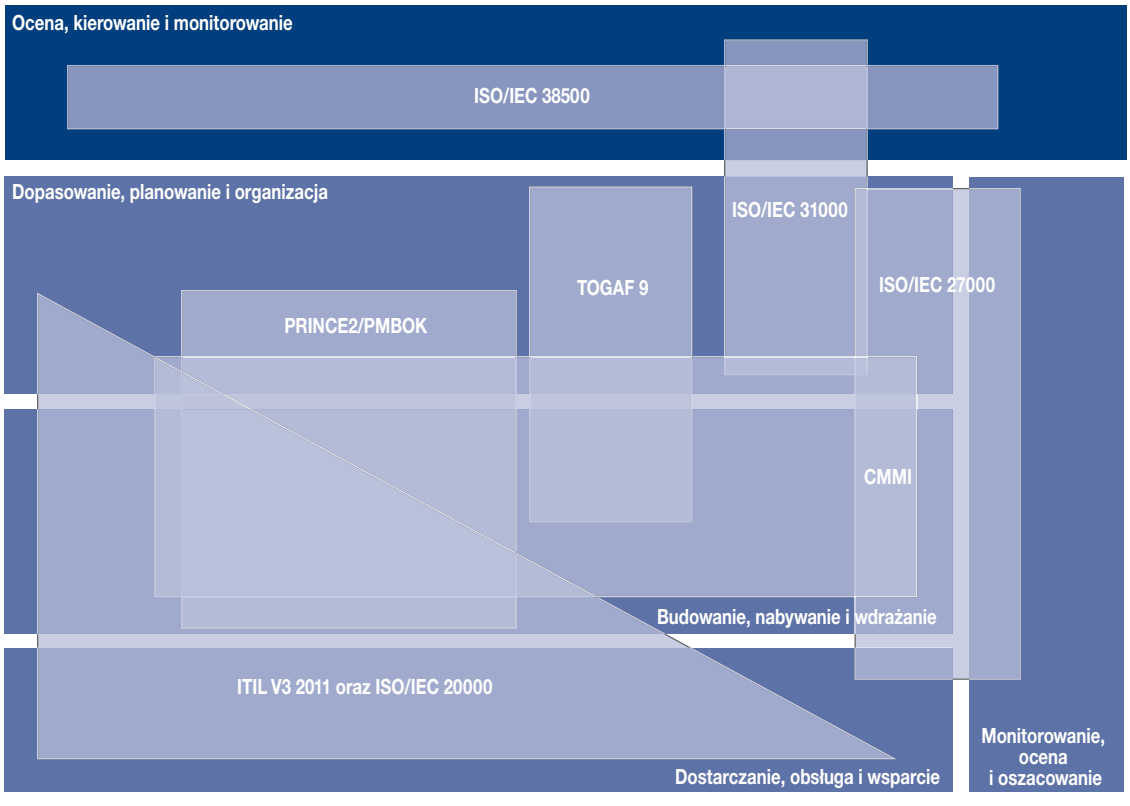
PRINCE2®

PRINCE2 obejmuje następujące obszary i domeny COBIT 5:

- procesy związane z portfelem w domenie APO;
- procesy zarządzania programami i projektami w domenie BAI.

Na **ilustracji 25** przedstawiono zależności między metodyką COBIT 5 i innymi standardami i metodykami.

Ilustracja 25 — Uwzględnienie innych standardów i metodyk w ramach metodyki COBIT 5



Strona celowo pozostawiona pusta

Załącznik F
Porównanie modelu informacji COBIT 5 z kryteriami informacji COBIT 4.1

Jaki jest związek między siedmioma kryteriami informacji w metodyce COBIT 4.1 (skuteczność, wydajność, integralność, wiarygodność, dostępność, poufność, zgodność) i kategoriami jakości informacji oraz wymiarami czynników umożliwiających Informacje w ramach metodyki COBIT 5 zgodnie z załącznikiem G, **ilustracja 36**?

Poniższa tabela zawiera dwie kolumny:
- w pierwszej kolumnie wymieniono każde z siedmiu kryteriów informacji COBIT 4.1;
- w drugiej kolumnie przedstawiono alternatywne opcje w ramach metodyki COBIT 5, tj. odpowiednie cele czynnika umożliwiającego Informacja.

Ilustracja 26 — Zawarte w metodyce COBIT 5 odpowiedniki kryteriów informacji COBIT 4.1

Kryteria informacji w metodyce COBIT 4.1	Odpowiednik COBIT 5
Skuteczność	Informacje są skuteczne, jeśli spełniają potrzeby odbiorców informacji, którzy wykorzystują je do realizacji określonych zadań. Jeśli odbiorca informacji może wykonać zadanie na podstawie informacji, informacje można uznać za efektywne. Odnosi się to do następujących celów jakościowych dotyczących informacji: właściwa ilość, istotność, jasność przekazu, możliwość interpretacji, obiektywność.
Wydajność	O ile skuteczność odnosi się do informacji jako produktu, wydajność wiąże się bardziej z procesem uzyskiwania i wykorzystywania informacji, tak aby zapewnić spójność z podejściem do informacji jako do usługi. Jeśli informacje spełniające potrzeby odbiorcy informacji są uzyskiwane i wykorzystywane w prosty sposób (tj. wymagający użycia niewielu zasobów — wysiłek fizyczny, wysiłek poznawczy, czas, pieniądze), wówczas wykorzystanie informacji jest wydajne. Odnosi się to do następujących celów jakościowych dotyczących informacji: wiarygodność, dostępność, łatwość eksploatacji, reputacja.
Integralność	Integralność informacji oznacza, że są one wolne od błędów i kompletne. Odnosi się do następujących celów jakościowych dotyczących informacji: kompletność, dokładność.
Wiarygodność	Wiarygodność często uważa się za synonim dokładności; informacje uznaje się jednak za wiarygodne wtedy, gdy mogą być uznane za prawdziwe i godne zaufania. W porównaniu z integralnością wiarygodność jest bardziej subiektywna, zależna od sposobu postrzegania i nie odnosi się tylko do suchych faktów. Związana jest z następującymi celami jakościowymi dotyczącymi informacji: wiarygodność, reputacja, obiektywność.
Dostępność	Dostępność jest jednym z celów jakościowych dotyczących informacji w ramach możliwości dostępu i bezpieczeństwa.
Poufność	Poufność odnosi się do celu jakościowego informacji dotyczącego ograniczonego dostępu.
Zgodność	Zgodność informacji ze specyfikacjami została uwzględniona w każdym z celów jakościowych dotyczących informacji, w zależności od wymagań. Zgodność z regulacjami jest najczęściej celem lub wymogiem związanym ze sposobem wykorzystania informacji — w mniejszym stopniu cechą wewnętrzną informacji.

W tabeli wykazano, że wszystkie kryteria informacji w metodyce COBIT 4.1 zostały uwzględnione w metodyce COBIT 5; model informacji w metodyce COBIT 5 umożliwia jednak zdefiniowanie dodatkowego zbioru kryteriów, co stanowi wartość dodaną w stosunku do kryteriów COBIT 4.1.

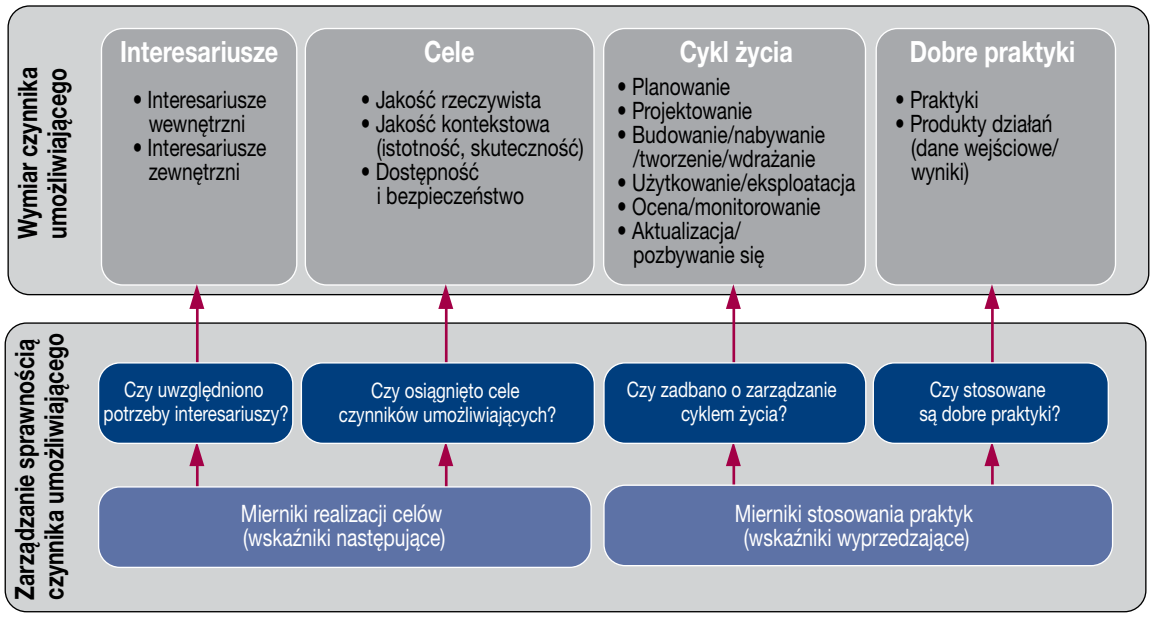
Strona celowo pozostawiona pusta

Załącznik G
Szczegółowy opis czynników umożliwiających COBIT 5

Wprowadzenie

W tej części w sposób bardziej szczegółowy omówiono siedem kategorii czynników umożliwiających stanowiących część metodyki COBIT 5, które wstępnie opisano w rozdziale 5 i powtórnie przedstawiono na **ilustracji 27**.

Ilustracja 27 — Czynniki umożliwiające COBIT 5: Typowe



Wymiary czynnika umożliwiającego

Cztery wspólne wymiary dla czynników umożliwiających to:

- **Interesariusze** — dla każdego czynnika umożliwiającego można wskazać interesariuszy, tj. strony, które odgrywają aktywną rolę i/lub są zainteresowane czynnikiem umożliwiającym. Na przykład: w procesach uczestniczą różne strony, które realizują czynności w ramach procesów i/lub są zainteresowane rezultatami procesów; struktury organizacyjne mają interesariuszy — z ich własnymi rolami i zainteresowaniami — stanowiących część struktur. Interesariusze przedsiębiorstwa mogą być wewnętrzni lub zewnętrzni i wszyscy mają własne — niekiedy wykluczające się — zainteresowania i potrzeby. Potrzeby interesariuszy przekładają się na cele przedsiębiorstwa, które z kolei przekładają się na cele przedsiębiorstwa związane z IT. Listę interesariuszy przedstawiono na **ilustracji 7**.
- **Cele** — Dla każdego czynnika umożliwiającego istnieje określona liczba celów, a czynniki umożliwiające zapewniają wartość poprzez osiągnięcie tych celów. Cele można definiować na podstawie następujących kryteriów:
  – oczekiwane wyniki wykorzystania czynników umożliwiających;
  – zastosowanie lub wykorzystanie samego czynnika umożliwiającego.

  Cele czynników umożliwiających to ostateczny etap w kaskadzie celów COBIT 5. Cele można dodatkowo podzielić na różne kategorie, np.:
  – **Jakość rzeczywista** — stopień, w jakim czynniki umożliwiające działają w sposób dokładny i obiektywny oraz zapewniają dokładne, obiektywne i uznane rezultaty.
  – **Jakość kontekstowa** — stopień, w jakim czynniki umożliwiające oraz ich rezultaty odpowiadają danemu celowi, biorąc pod uwagę kontekst, w którym funkcjonują. Na przykład: wyniki powinny być istotne, kompletne, aktualne, odpowiednie, spójne, zrozumiałe i łatwe do wykorzystania.
  – **Dostęp i bezpieczeństwo** — stopień, w jakim czynniki umożliwiające oraz ich rezultaty są dostępne i zabezpieczone:
    • czynniki umożliwiające są dostępne w razie potrzeby;
    • rezultaty są zabezpieczone, tj. dostęp jest ograniczony do osób uprawnionych i potrzebujących takiego dostępu.
- **Cykl życia** — każdy czynnik umożliwiający ma cykl życia, od rozpoczęcia, przez okres funkcjonowania/żywotności, aż po jego wycofanie. Odnosi się to do informacji, struktur, procesów, polityk itd. Fazy cyklu życia:
  – Planowanie (obejmuje opracowanie oraz wybór koncepcji);
  – Projektowanie;

  – Budowanie/nabywanie/tworzenie/wdrażanie;
  – Użytkowanie/obsługa;
  – Ocena/monitorowanie;
  – Aktualizacja/pozbywanie się.
- **Dobre praktyki** — dla każdego czynnika umożliwiającego można zdefiniować dobre praktyki. Dobre praktyki ułatwiają osiągnięcie celów czynników umożliwiających. Dobre praktyki obejmują przykłady lub sugestie dotyczące optymalnego sposobu wdrożenia czynnika umożliwiającego i określają wymagane produkty działań bądź dane wejściowe i wyniki. W ramach metodyki COBIT 5 zapewniono przykłady dobrych praktyk w odniesieniu do niektórych czynników umożliwiających COBIT 5 (np. procesy). W przypadku innych czynników umożliwiających można wykorzystać wytyczne z innych standardów, metodyk itd.

Zarządzanie sprawnością czynnika umożliwiającego

Przedsiębiorstwa oczekują, że zastosowanie czynników umożliwiających przyniesie pozytywne wyniki. Zarządzanie sprawnością czynników umożliwiających wymaga regularnego monitorowania i udzielania odpowiedzi na poniższe pytania — na podstawie mierników:

- Czy uwzględniono potrzeby interesariuszy?
- Czy osiągnięto cele czynników umożliwiających?
- Czy zadbano o zarządzanie cyklem życia czynników umożliwiających?
- Czy stosowane są dobre praktyki?

Pierwsze dwa punkty dotyczą rzeczywistego wyniku zastosowania czynnika umożliwiającego, a mierniki pozwalające na określenie stopnia, w jakim osiągnięto cele, można nazwać „wskaźnikami następującymi”.

Ostatnie dwa punkty dotyczą rzeczywistego funkcjonowania samego czynnika umożliwiającego, a mierniki stosowane w tym celu można nazwać „wskaźnikami wyprzedzającymi”.

Każdemu czynnikowi umożliwiającego poświęcono osobną część, która rozpoczyna się od rysunku podobnego do **ilustracji 27**, ale zawiera szereg charakterystycznych elementów danego czynnika umożliwiającego, oznaczonych kolorem czerwonym i **pogrubieniem**.

Następnie każdy z czterech komponentów jest omawiany w sposób bardziej szczegółowy, z uwzględnieniem konkretnych elementów i relacji z innymi czynnikami umożliwiającymi.

Przedstawiono również kilka przykładów ilustrujących znaczenie i wykorzystanie czynników umożliwiających.

Celem tej części jest zapewnienie lepszego wglądu w metodykę COBIT 5 oraz sposób, w jaki można zastosować koncepcję czynnika umożliwiającego do wdrożenia i udoskonalenia nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi.

Czynnik umożliwiający COBIT 5: Zasady, polityki i metodyki

Zasady i polityki odnoszą się do mechanizmów komunikacji wdrożonych w celu przekazania wytycznych oraz instrukcji organu nadzorującego i kierownictwa. Szczegóły dotyczące czynnika Zasady, polityki i metodyki w porównaniu z opisem typowego czynnika umożliwiającego przedstawiono na **ilustracji 28**.

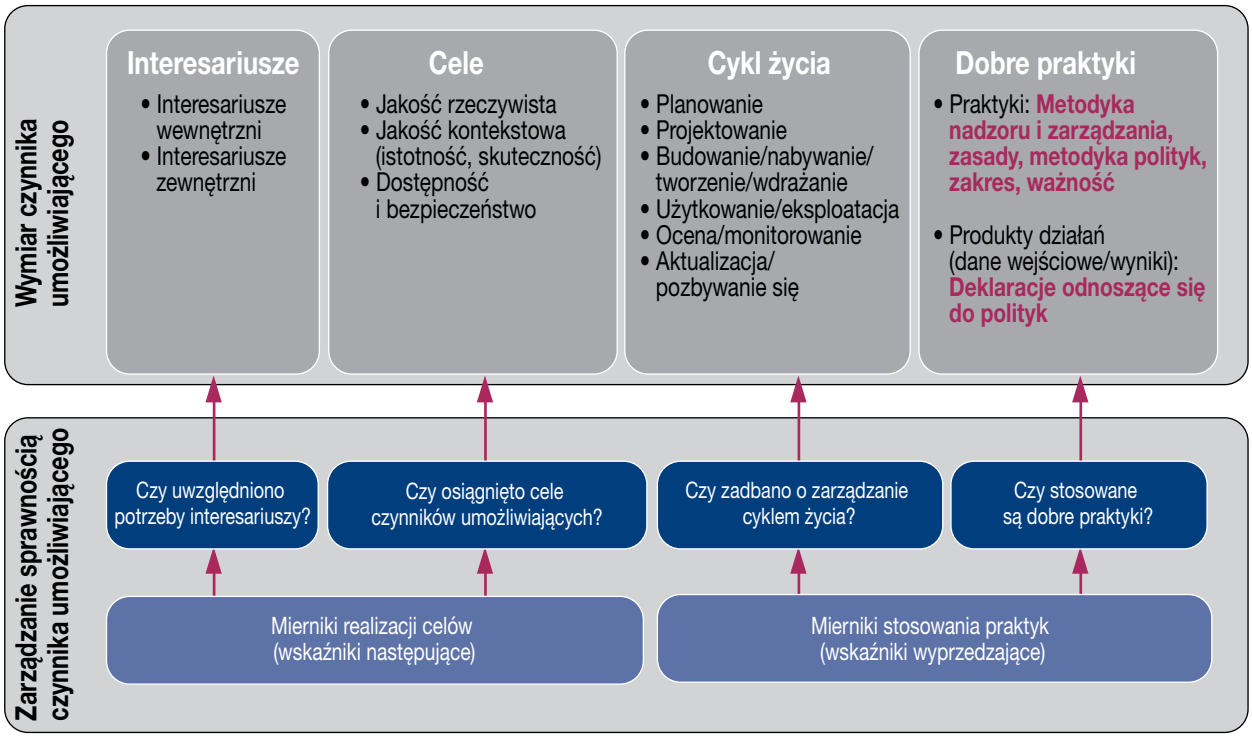
Model zasad, polityk i metodyk składa się z następujących elementów:

- **Interesariusze** — w przypadku każdego przedsiębiorstwa interesariusze w odniesieniu do zasad i polityk mogą być zewnętrzni lub wewnętrzni. Obejmują zarząd oraz kadrę zarządzającą, dyrektorów ds. zgodności, zarządzających ryzykiem, audytorów wewnętrznych i zewnętrznych, dostawców usług i klientów, a także agencje regulacyjne. Ich interesy mają dwojaki charakter: Niektórzy interesariusze definiują i określają polityki, inni muszą zadbać o spójność i zgodność z politykami.
- **Cele i mierniki** — zasady, polityki i metodyki to instrumenty umożliwiające komunikowanie reguł obowiązujących w przedsiębiorstwie, co wspiera osiągnięcie celów w zakresie nadzoru oraz dotrzymanie wartości przedsiębiorstwa, zdefiniowanych przez zarząd i kadrę zarządzającą. Zasady muszą spełniać następujące kryteria:
  – ich liczba musi być ograniczona;
  – muszą być sformułowane prostym językiem i w sposób maksymalnie precyzyjny wyrażać podstawowe wartości przedsiębiorstwa.

Polityki zawierają bardziej szczegółowe wytyczne dotyczące sposobu praktycznego zastosowania zasad i wpływają na sposób, w jaki zasady te są uwzględniane w procesie decyzyjnym. Dobre polityki są:
– skuteczne — umożliwiają osiągnięcie wskazanego celu;
– wydajne — zapewniają wdrożenie zasad w najbardziej wydajny sposób;
– nieingerencyjne — osobom, które muszą ich przestrzegać, wydają się logiczne, tj. nie budzą niepotrzebnego oporu.

Dostęp do polityk — czy wdrożono mechanizm zapewniający wszystkim interesariuszom łatwy dostęp do polityk? Innymi słowy, czy interesariusze wiedzą, gdzie można znaleźć polityki?

Ilustracja 28 — Czynnik umożliwiający COBIT 5: Zasady, polityki i metodyki



Metodyki nadzoru i zarządzania powinny zapewnić kierownictwu strukturę, wytyczne, narzędzia itp. umożliwiające właściwy nadzór nad technologiami informatycznymi oraz zarządzanie nimi w przedsiębiorstwie. Metodyki powinny być:
– kompleksowe, powinny obejmować wszystkie wymagane obszary;
– otwarte i elastyczne, umożliwiające dostosowanie do konkretnej sytuacji przedsiębiorstwa;
– aktualne, tj. odzwierciedlające aktualne ukierunkowanie przedsiębiorstwa oraz aktualne cele nadzoru;
– dostępne dla wszystkich interesariuszy.

- **Cykl życia** — polityki mają cykl życia, który musi wspierać realizację zdefiniowanych celów. Metodyki mają kluczowe znaczenie, ponieważ stanowią strukturę umożliwiającą zdefiniowanie spójnych wytycznych. Na przykład: metodyka dotycząca polityk zapewnia strukturę, w ramach której można utworzyć i utrzymać spójny zbiór polityk, a także ułatwia poruszanie się pomiędzy poszczególnymi politykami i wewnątrz każdej z nich.

  W zależności od środowiska zewnętrznego, w którym funkcjonuje przedsiębiorstwo, mogą istnieć różne stopnie wymogów regulacyjnych wobec silnej kontroli wewnętrznej, a co za tym idzie – solidnej struktury polityk. Kluczowym aspektem metodyk i polityk, na który należy zwrócić szczególną uwagę, jest aktualność polityk: czy i kiedy aktualizuje się polityki, czy wdrożono efektywne mechanizmy zwiększające świadomość tych aktualizacji wśród pracowników, zapewniające łatwy dostęp do najnowszej wersji (zob. wcześniejszy punkt) oraz zapewniające właściwą archiwizację i pozbywanie się nieaktualnych informacji?
- **Dobre praktyki:**
  - Zgodnie z dobrą praktyką polityki powinny być częścią ogólnej metodyki nadzoru i zarządzania, stanowiącej (hierarchiczną) strukturę, w której każda z polityk powinna mieć swoje miejsce oraz wyraźnie odnosić się do podstawowych zasad.
  - W ramach struktury polityk muszą zostać opisane następujące elementy:
    - zakres i prawidłowość;
    - konsekwencje nieprzestrzegania polityki;
    - sposób obsługi wyjątków;
    - sposób kontroli i pomiaru zgodności z polityką.
  - Ogólnie uznane struktury nadzoru i zarządzania mogą zapewnić cenne wytyczne dotyczące właściwych treści, które mają zostać uwzględnione w politykach.
  - Polityki powinny być dopasowane do apetytu na ryzyko w danym przedsiębiorstwie. Polityki stanowią kluczowy komponent systemu kontroli wewnętrznej w przedsiębiorstwie, którego celem jest zarządzanie ryzykiem i ograniczanie go. W ramach czynności związanych z nadzorem nad ryzykiem definiuje się apetyt na ryzyko w przedsiębiorstwie, który powinien zostać odzwierciedlony w politykach. Przedsiębiorstwo niechętnie podejmujące ryzyko ma bardziej restrykcyjne polityki niż przedsiębiorstwo skłonne do agresywnego podejmowania ryzyka.
  - Polityki muszą być przedłużane i/lub aktualizowane w regularnych odstępach czasu.
- **Relacje z innymi czynnikami umożliwiającymi** — powiązania z innymi czynnikami umożliwiającymi:
  - Zasady, polityki i metodyki powinny odzwierciedlać kulturę i wartości etyczne przedsiębiorstwa oraz powinny promować pożądane zachowanie; to oznacza, że istnieje silny związek z czynnikiem umożliwiającym Kultura, etyka i zachowanie.
  - Praktyki i działania dotyczące procesów są najistotniejszym środkiem realizacji polityk.
  - Struktury organizacyjne mogą zdefiniować i wdrożyć polityki mieszczące się w ich zakresie kontroli, a ich działania są również definiowane przez polityki.
  - Polityki stanowią również informacje, więc wszystkie dobre praktyki odnoszące się do informacji odnoszą się również do polityk.

PRZYKŁAD 9 – MEDIA SPOŁECZNOŚCIOWE

Przedsiębiorstwo rozważa sposób postępowania wobec rosnącej popularności mediów społecznościowych oraz presji ze strony pracowników domagających się pełnego dostępu do nich. Dotychczas organizacja stosowała konserwatywne, ograniczające podejście do udzielania dostępu do tego rodzaju usług, głównie ze względu na bezpieczeństwo.

Z różnych stron odczuwana jest presja zmiany stosunku do mediów społecznościowych. Pracownicy oczekują poziomu dostępu podobnego to tego, z którego korzystają w domu; sama organizacja również chce czerpać korzyści z dostępu do mediów społecznościowych dla celów marketingowych oraz związanych ze zwiększeniem publicznej świadomości.

Podjęto decyzję o ustanowieniu polityki dotyczącej korzystania z mediów społecznościowych w sieciach i systemach przedsiębiorstwa, w tym na laptopach udostępnianych przez przedsiębiorstwo pracownikom. Nowa polityka wpasowuje się w istniejącą strukturę polityk w kategorii „polityki akceptowalnego użytkowania" i jest mniej restrykcyjna niż wcześniejsze polityki. W związku z tym opracowuje się komunikaty wyjaśniające powody wprowadzenia nowej polityki. Nowa polityka wpływa również na niektóre z pozostałych czynników umożliwiających:

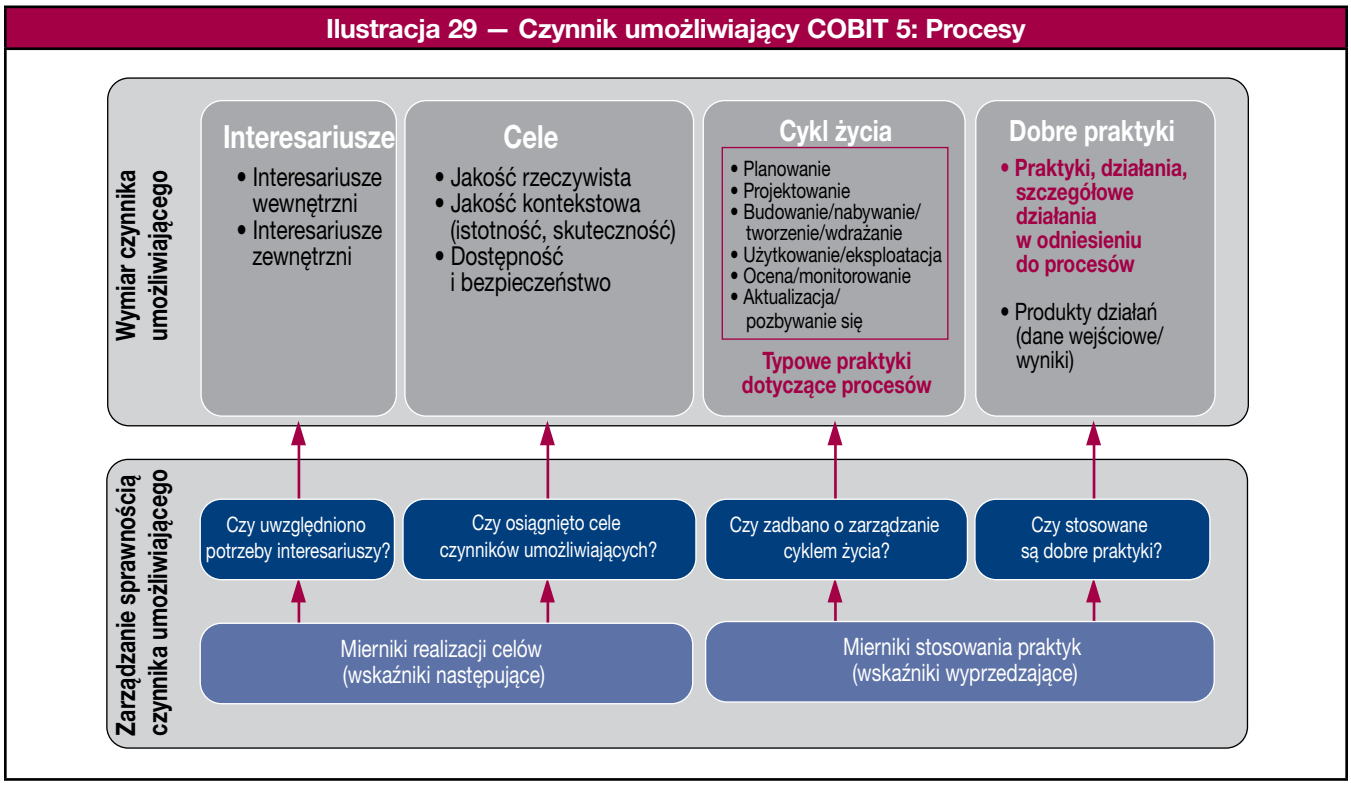
- Pracownicy muszą zapoznać się z zasadami korzystania z nowych mediów w celu uniknięcia sytuacji, które mogą być kłopotliwe dla przedsiębiorstwa. Muszą przyswoić sobie wzorce zachowania zgodne z nowymi wytycznymi przedsiębiorstwa i rozwinąć właściwe umiejętności.
- Konieczna jest zmiana szeregu procesów odnoszących się do bezpieczeństwa. Zapewniony zostaje dostęp do mediów społecznościowych, co wymaga zmiany ustawień i konfiguracji bezpieczeństwa. Konieczne może być również zdefiniowanie środków kompensujących.

Uwaga: COBIT 5 jest przykładem metodyki opisanej w ramach tego czynnika umożliwiającego.

Czynnik umożliwiający COBIT 5: Procesy

Szczegóły czynnika umożliwiającego dotyczącego procesów w porównaniu z opisem typowego czynnika umożliwiającego przedstawiono na **ilustracji 29.**

Ilustracja 29 — Czynnik umożliwiający COBIT 5: Procesy



Proces definiuje się jako **„zbiór praktyk ukierunkowanych przez polityki i procedury przedsiębiorstwa, które wykorzystują dane wejściowe z różnych źródeł (również z innych procesów), przetwarzają je i dostarczają wyniki (np. produkty, usługi)”.**

Model procesów składa się z następujących elementów:

- **Interesariusze** — w odniesieniu do procesów można wskazać interesariuszy wewnętrznych i zewnętrznych, pełniących określone role; interesariuszy oraz ich stopień odpowiedzialności ujęto w tabeli RACI. Interesariuszami zewnętrznymi są klienci, partnerzy biznesowi, udziałowcy i organy regulacyjne. Do interesariuszy wewnętrznych należy zarząd, kierownictwo, pracownicy i wolontariusze.
- **Cele** — cele procesu definiuje się jako „stwierdzenie opisujące pożądany wynik procesu. Wynikiem może być pozostałość, istotna zmiana stanu lub istotna poprawa potencjału innych procesów”. Stanowią część kaskady celów, tj. cele procesu wspierają realizację celów związanych z IT, które z kolei wspierają osiągnięcie celów przedsiębiorstwa.

Cele procesu można podzielić według następujących kategorii:

– **Cele wewnętrzne** — czy proces ma jakość rzeczywistą? Czy jest odpowiedni i zgodny z dobrą praktyką? Czy jest zgodny z regułami wewnętrznymi i zewnętrznymi?
– **Cele dotyczące zgodności z kontekstem** — czy proces został dostosowany i dopasowany do konkretnej sytuacji przedsiębiorstwa? Czy proces jest odpowiedni, zrozumiały i łatwy do zastosowania?
– **Cele dotyczące dostępności i bezpieczeństwa** — proces pozostaje poufny, gdy jest to wymagane, oraz jest znany i dostępny dla osób, które tego potrzebują.

Na każdym poziomie kaskady celów, a więc również w przypadku procesów, definiuje się mierniki umożliwiające pomiar stopnia, w jakim zrealizowano cele. Mierniki można zdefiniować jako „wymierną jednostkę umożliwiającą pomiar realizacji celu procesu. Mierniki powinny spełniać kryteria SMART — muszą być specyficzne, wymierne, składające się z konkretnych działań, istotne i terminowe”.

Aby umożliwiać efektywne i wydajne zarządzanie czynnikiem umożliwiającym, mierniki muszą zostać zdefiniowane w taki sposób, aby umożliwiały pomiar stopnia, w jakim osiągnięto oczekiwane wyniki. Ponadto drugi aspekt zarządzania sprawnością czynnika umożliwiającego opisuje zakres, w jakim zastosowano dobrą praktykę. W tym przypadku również istnieje możliwość zdefiniowania powiązanych mierników, które ułatwią zarządzanie czynnikiem umożliwiającym.

- **Cykl życia** — każdy proces ma cykl życia. Jest on definiowany, tworzony, obsługiwany, monitorowany oraz dostosowywany/aktualizowany lub wycofywany. Typowe praktyki procesów, takie jak te zdefiniowane w ramach modelu oceny procesu metodyki COBIT, oparte na normie ISO/IEC 15504, mogą ułatwić definiowanie, realizację, monitorowanie i optymalizację procesów.
- **Dobre praktyki** — *przewodnik COBIT 5: Procesy umożliwiające* zawiera model referencyjny procesu, w którym opisano wewnętrzne dobre praktyki dotyczące procesów zgodnie z rosnącym poziomem szczegółowości: praktyki, działania i szczegółowe działania[14]:

Praktyki:

- W odniesieniu do każdego procesu w ramach metodyki COBIT 5 praktyki nadzoru/zarządzania zapewniają kompletny zbiór ogólnych wymogów dotyczących efektywnego i praktycznego nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi. Są one:
  - deklaracjami dotyczącymi działań umożliwiającymi uzyskanie korzyści, optymalizację poziomu ryzyka oraz optymalizację wykorzystania zasobów;
  - dopasowane do istotnych ogólnie akceptowanych norm i dobrych praktyk;
  - typowe i w związku z tym muszą zostać dostosowane do potrzeb każdego przedsiębiorstwa;
  - obejmujące osoby odgrywające role w ramach funkcji biznesowej oraz IT w procesie (mają charakter kompleksowy).
- Organ nadzorujący oraz kadra kierownicza w przedsiębiorstwie muszą dokonywać wyborów w odniesieniu do tych praktyk nadzoru i zarządzania poprzez:
  - wybór tych, które są właściwe, i podejmowanie decyzji o wdrożeniu wybranych praktyk;
  - wprowadzanie nowych praktyk i/lub dostosowywanie praktyk w odpowiednich przypadkach;
  - definiowanie i wdrażanie praktyk niezwiązanych z IT dla celów integracji z procesami biznesowymi;
  - wybór sposobu ich wdrożenia (częstotliwość, zakres, automatyzacja itp.);
  - akceptację ryzyka niewdrożenia praktyk, które mogą mieć zastosowanie.

Działania — w metodyce COBIT są to podstawowe czynność podejmowane w ramach obsługi procesu.

- Definiuje się je jako „wytyczne dotyczące wdrożenia praktyk zarządzania ukierunkowane na zapewnienie skutecznego nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi". Działania w ramach metodyki COBIT 5 określają sposób, powody oraz przedmiot wdrożenia dla poszczególnych praktyk nadzoru i zarządzania w celu zwiększenia sprawności IT i/lub uwzględnienia ryzyka związanego z rozwiązaniami IT i świadczeniem usług IT. Materiały te są przydatne dla następujących osób:
  - kadra kierownicza, dostawcy usług, użytkownicy końcowi oraz specjaliści ds. IT, którzy muszą planować, budować, eksploatować i monitorować technologie informatyczne w przedsiębiorstwie;
  - specjaliści ds. audytu, którzy mogą zostać poproszeni o opinię na temat aktualnych lub proponowanych wdrożeń bądź koniecznych usprawnień.
- Pełny zbiór typowych i szczegółowych działań zapewniających jedno podejście obejmujące wszystkie kroki konieczne (i wystarczające) do osiągnięcia kluczowej praktyki nadzoru (GP)/praktyki zarządzania (MP). Zapewniają ogólne wytyczne, na poziomie niższym niż GP/MP, dla celów oszacowania rzeczywistej sprawności oraz w celu rozważenia potencjalnych udoskonaleń. Działania:
  - opisują zbiór koniecznych i wystarczających kroków zorientowanych na działanie wymaganych do wdrożenia praktyki nadzoru/praktyki zarządzania (GP/MP);
  - uwzględniają dane wejściowe i wyniki procesu;
  - są oparte na ogólnie akceptowanych normach i dobrych praktykach;
  - ułatwiają wyznaczenie zrozumiałych ról i zakresów odpowiedzialności;
  - nie mają charakteru normatywnego i muszą zostać dostosowane oraz rozwinięte w celu opracowania konkretnych procedur odpowiednich dla przedsiębiorstwa.

Szczegółowe działania — działania mogą nie być wystarczająco szczegółowe dla celów wdrożenia, zatem konieczne mogą okazać się dodatkowe wytyczne, które można:

- uzyskać ze szczegółowych istotnych standardów i dobrych praktyk, takich jak ITIL, ISO/IEC serii 27000 oraz PRINCE2;
- opracować jako bardziej szczegółowe działania w ramach dodatkowych rozwiązań w samej rodzinie produktów COBIT 5.

Dane wejściowe i wyniki — dane wejściowe i wyniki w ramach metodyki COBIT 5 to produkty działań/pozostałości związane z procesem, uznane za niezbędne do wspierania realizacji procesu. Umożliwiają podejmowanie kluczowych decyzji, zapewniają rejestr oraz ścieżkę rewizyjną dla działań w ramach procesu i pozwalają na weryfikację w przypadku wystąpienia incydentu. Definiuje się je na poziomie kluczowych praktyk nadzoru/zarządzania; mogą one obejmować niektóre produkty działań wykorzystywane tylko w ramach samego procesu i stanowią często niezbędne dane wejściowe dla innych procesów[15].

[14] W ramach bieżącego projektu opracowuje się tylko praktyki i działania. Bardziej szczegółowe poziomy wymagają dodatkowych prac — np. bardziej wyczerpujące wytyczne dotyczące poszczególnych obszarów mogą zostać zawarte w różnych specjalistycznych przewodnikach. Ponadto dodatkowe wytyczne można znaleźć w powiązanych standardach i metodykach wskazanych w szczegółowych opisach procesów.

[15] Lista przykładowych danych wejściowych i wyników COBIT 5 nie jest kompletna, ponieważ na podstawie określonego środowiska i struktury procesów w przedsiębiorstwie można zdefiniować dodatkowe przepływy informacji.

Zewnętrzne dobre praktyki mogą mieć dowolną formę lub poziom szczegółowości i odnoszą się głównie do innych norm i metodyk. Użytkownicy mogą zawsze odwołać się do tych zewnętrznych dobrych praktyk, wiedząc, że metodyka COBIT jest dopasowana do tych norm (w odpowiednich przypadkach) i że udostępnione zostaną informacje dotyczące zestawienia metodyki z tymi źródłami.

Zarządzanie sprawnością czynnika umożliwiającego

Przedsiębiorstwa oczekują, że zastosowanie czynników umożliwiających przyniesie pozytywne wyniki. Zarządzanie sprawnością czynników umożliwiających wymaga regularnego monitorowania i udzielania odpowiedzi na poniższe pytania — na podstawie mierników:
- Czy uwzględniono potrzeby interesariuszy?
- Czy osiągnięto cele czynników umożliwiających?
- Czy zadbano o zarządzanie cyklem życia czynników umożliwiających?
- Czy stosowane są dobre praktyki?

W przypadku czynnika umożliwiającego Procesy pierwsze dwa punkty dotyczą rzeczywistego wyniku procesu. Mierniki pozwalające na określenie stopnia, w jakim osiągnięto cele, można nazwać „wskaźnikami następującymi". W przewodniku *COBIT 5: Procesy umożliwiające* zdefiniowano kilka mierników dla każdego z celów procesu.

Ostatnie dwa punkty dotyczą rzeczywistego funkcjonowania samego czynnika umożliwiającego, a mierniki stosowane w tym celu można nazwać „wskaźnikami wyprzedzającymi".

Poziom potencjału procesu — metodyka COBIT 5 wykorzystuje schemat szacowania potencjału procesu oparty na normie ISO/IEC 15504. Kwestię tę omówiono w rozdziale 8 przewodnika COBIT 5, a dodatkowe wytyczne można znaleźć w osobnych publikacjach ISACA COBIT 5. Krótko mówiąc, poziom potencjału procesu umożliwia pomiar realizacji celów oraz stosowania dobrej praktyki.

Relacje z innymi czynnikami umożliwiającymi — powiązania między procesami i innymi kategoriami czynników umożliwiających są oparte na następujących relacjach:
- Procesy wymagają informacji (stanowiących jeden z typów danych wejściowych) oraz mogą dostarczać informacji (jako produktów działań).
- Realizacja procesów wymaga istnienia struktur organizacyjnych i ról określonych w tabelach RACI , np. komitet sterujący ds. IT, komitet ds. zarządzania ryzykiem w przedsiębiorstwie, zarząd, dział audytu, dyrektor ds. informatyki (CIO), dyrektor generalny (CEO).
- Procesy zapewniają (lecz także wymagają) zdolności do świadczenia usług (infrastruktura, aplikacje itd.).
- Procesy mogą zależeć (i zależą) od innych procesów.
- Procesy umożliwiają uzyskanie (lub wymagają istnienia) polityk i procedur zapewniających spójne wdrożenie i realizację.
- Aspekty związane z zachowaniem i kulturą determinują skuteczność realizacji procesów.

Przykład czynnika umożliwiającego Proces w praktyce

Na przykładzie 10 przedstawiono czynnik umożliwiający Proces, jego wzajemne powiązania oraz wymiary czynnika umożliwiającego. Przykład ten jest oparty na przykładzie 5 podanym we wcześniejszej części dokumentu.

Model referencyjny procesu COBIT 5

PROCESY NADZORU I ZARZĄDZANIA

Jedną z głównych zasad w metodyce COBIT jest rozróżnienie nadzoru i zarządzania. Zgodnie z tą zasadą od każdego przedsiębiorstwa oczekuje się wdrożenia szeregu procesów nadzoru oraz procesów zarządzania, które umożliwią kompleksowy nadzór nad technologiami informatycznymi w przedsiębiorstwie oraz zarządzanie nimi.

Rozważając procesy w zakresie nadzoru i zarządzania w kontekście przedsiębiorstwa, należy zauważyć, że różnica między typami procesów tkwi w celach procesów:
- **Proces nadzoru** — procesy nadzoru odnoszą się do celów związanych z nadzorem w odniesieniu do interesariuszy — dostarczania wartości, optymalizacji ryzyka oraz optymalizacji zasobów. Obejmują praktyki i działania, których celem jest ocena strategicznych opcji, ukierunkowanie IT i monitorowanie wyników (EDM — zgodnie z koncepcjami normy ISO/IEC 38500).
- **Zarządzanie** — Zgodnie z definicją zarządzania praktyki i działania w ramach procesów zarządzania obejmują obszary odpowiedzialności w zakresie PBRM (planowania, budowania, realizacji i monitorowania) obszaru IT przedsiębiorstwa i muszą zapewniać całościowy wgląd w działalność IT.

PRZYKŁAD 10 – WZAJEMNE POWIĄZANIA CZYNNIKA UMOŻLIWIAJĄCEGO PROCES

Organizacja wyznaczyła „kierowników ds. procesów” dla procesów związanych z IT. Ich obowiązkiem jest definiowanie i realizacja skutecznych i wydajnych procesów związanych z IT w kontekście dobrego nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi.

Początkowo kierownicy ds. procesów skupią się na czynniku umożliwiającym Proces, rozważając jego następujące wymiary:

- **Interesariusze:** Interesariuszami procesów są wszystkie podmioty zaangażowane w ich realizację, tj. wszystkie strony odpowiedzialne, rozliczane, konsultowane lub informowane (RACI) w związku z działaniami w ramach procesów. Można się tu posłużyć tabelą RACI opisaną w przewodniku *COBIT 5: Procesy umożliwiające*.
- **Cele:** Dla każdego procesu muszą zostać zdefiniowane odpowiednie cele i powiązane mierniki. Na przykład dla procesu APO08 *Zarządzanie relacjami* (w metodyce *COBIT 5: Procesy umożliwiające*) można znaleźć zbiór celów i mierników procesu, takich jak:
  - **Cel:** Strategie biznesowe, plany i wymogi są dobrze zrozumiane, udokumentowane i zatwierdzone.
    - **Miernik:** Odsetek programów spójnych z wymogami/priorytetami biznesowymi przedsiębiorstwa;
  - **Cel:** Istnieją dobre relacje miedzy przedsiębiorstwem i działem IT.
    - **Miernik:** Wskaźniki na podstawie badań dotyczących zadowolenia użytkowników i personelu IT;
- **Cykl życia:** Dla każdego procesu można wskazać cykl życia, tj. musi on zostać utworzony i zrealizowany oraz być monitorowany, a także (w stosownych wypadkach) dostosowywany. Ostatecznie procesy przestają istnieć. W tym przypadku kierownicy ds. procesów musieliby najpierw zaprojektować i zdefiniować proces. Mogą wykorzystać kilka elementów z przewodnika *COBIT 5: Procesy umożliwiające* w celu zaprojektowania procesów, tj. zdefiniowania zakresów odpowiedzialności oraz podziału procesów na praktyki i działania, a także zdefiniowania produktów działań w ramach procesów (dane wejściowe i wyniki). Na późniejszym etapie konieczne jest zwiększenie wydajności i solidności procesów. W tym celu kierownicy ds. procesów mogą podnieść poziom potencjału procesu. W tym celu można wykorzystać Model potencjału procesu COBIT 5 inspirowany normą ISO/IEC 15504 oraz atrybuty potencjału procesów, np.:
  - Poziom 2 potencjału procesu wymaga osiągnięcia dwóch atrybutów: Zarządzanie sprawnością i zarządzanie produktami działań: Pierwszy atrybut wymaga szeregu działań związanych z fazą planowania:
    - Definiowanie celów dotyczących realizacji procesu;
    - Planowanie realizacji procesu;
    - Definiowanie odpowiedzialności za realizację procesu;
    - Identyfikowanie zasobów;
    - itd.

    Ten sam poziom potencjału wiąże się z szeregiem działań dla fazy „monitorowanie” w cyklu życia procesu:
    - Monitorowanie realizacji procesu;
    - Dostosowanie realizacji procesu, tak aby pozwoliła na osiągnięcie planów.
    - itd.
  - To samo podejście może zostać zastosowane w celu uzyskania wytycznych dla różnych faz w cyklu życia na podstawie różnych atrybutów potencjału realizacji na coraz wyższych poziomach potencjału procesów.
- **Dobra praktyka:** W ramach metodyki COBIT 5 opisane są z dużą szczegółowością dobre praktyki wobec procesów w przewodniku *COBIT 5: Procesy umożliwiające*, wspomniane we wcześniejszym punkcie. W publikacji tej można znaleźć sugestie i przykładowe procesy, obejmujące pełne spektrum działań wymaganych dla skutecznego nadzoru nad technologiami informatycznymi w przedsiębiorstwie oraz zarządzania nimi.

Oprócz wytycznych dotyczących czynnika umożliwiającego Proces kierownicy ds. procesów mogą przyjrzeć się kilku innym czynnikom umożliwiającym:

- Tabele RACI, opisujące role i zakresy odpowiedzialności. Inne czynniki umożliwiające pozwalają na przejście do szczegółów tego wymiaru, np.:
  - W przypadku czynnika Umiejętności i kompetencje istnieje możliwość zdefiniowania umiejętności i kompetencji dla każdej roli, a także określenia właściwych celów (np. poziomy umiejętności technicznych i behawioralnych) oraz powiązanych mierników.
  - Tabela RACI zawiera również szereg struktur organizacyjnych. Struktury te mogą zostać dodatkowo omówione w związku z czynnikiem umożliwiającym Struktury organizacyjne. Można wówczas przedstawić bardziej szczegółowy opis struktury oraz zdefiniować oczekiwane wyniki i powiązane wskaźniki (np. decyzje), a także określić dobre praktyki (np. zakres kontroli, zasady działania struktury, poziom uprawnień).
- Zasady i polityki sformalizują proces i określą, dlaczego istnieje, kogo dotyczy oraz w jaki sposób ma być wykorzystywany. To obszar, którego dotyczy czynnik umożliwiający Zasady i polityki.

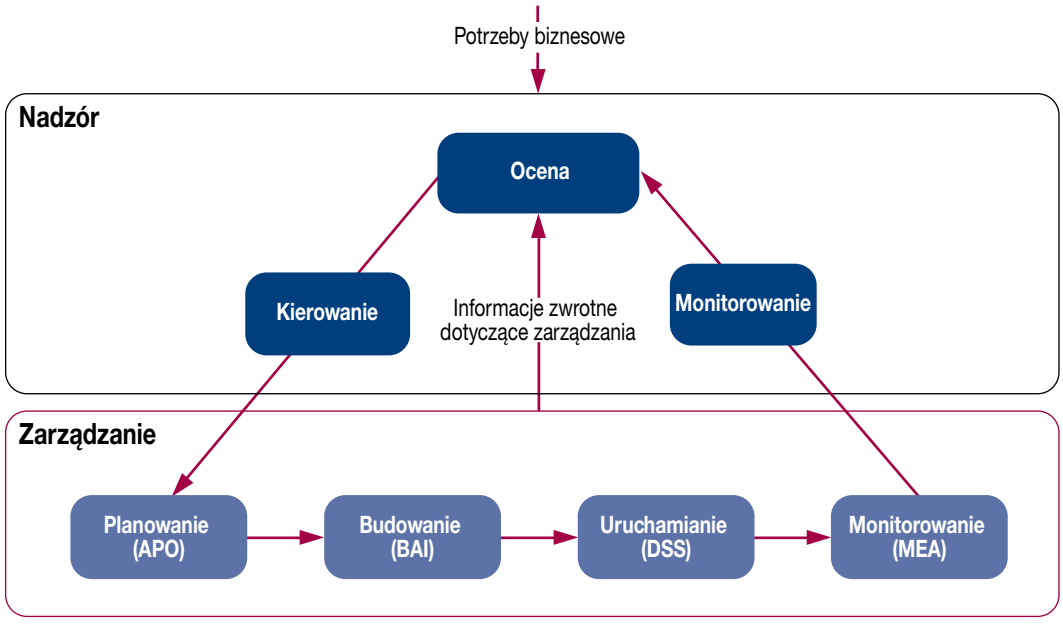
Choć wynik obu typów procesów jest inny i skierowany do innych odbiorców, wewnętrznie, w kontekście samego procesu wszystkie procesy realizowane w ramach przedsiębiorstwa wymagają działań dotyczących planowania, budowania lub wdrażania i monitorowania w ramach procesu.

MODEL REFERENCYJNY PROCESU COBIT 5

Metodyka COBIT 5 nie ma charakteru normatywnego, ale z wcześniejszego tekstu wynika jasno, że zaleca ona wdrożenie procesów nadzoru i zarządzania w przedsiębiorstwie, tak aby obejmowały kluczowe obszary, zgodnie z **ilustracją 30**.

Teoretycznie przedsiębiorstwo może organizować swoje procesy w sposób, który uznaje za odpowiedni, o ile obejmują one wszystkie podstawowe cele w zakresie nadzoru i zarządzania. W mniejszych przedsiębiorstwach liczba procesów może być niższa; większe i bardziej złożone przedsiębiorstwa mogą mieć wiele procesów, z których wszystkie służą tym samym celom.

Ilustracja 30 — Kluczowe obszary nadzoru i zarządzania w ramach metodyki COBIT 5



Niezależnie od wcześniejszego tekstu metodyka COBIT 5 obejmuje model referencyjny procesu, który w sposób szczegółowy definiuje i opisuje szereg procesów nadzoru i zarządzania. Zapewnia ona model referencyjny procesu obejmujący wszystkie procesy związane z działaniami w ramach IT zwykle realizowane w przedsiębiorstwie, oferując wspólny model odniesienia zrozumiały dla kierownictwa operacyjnego działu IT obszaru biznesowego. Proponowany model procesów jest kompletny i kompleksowy, ale nie jest to jedyny możliwy model procesów. Każde przedsiębiorstwo musi zdefiniować własny zbiór procesów, uwzględniając specyfikę swojej działalności.

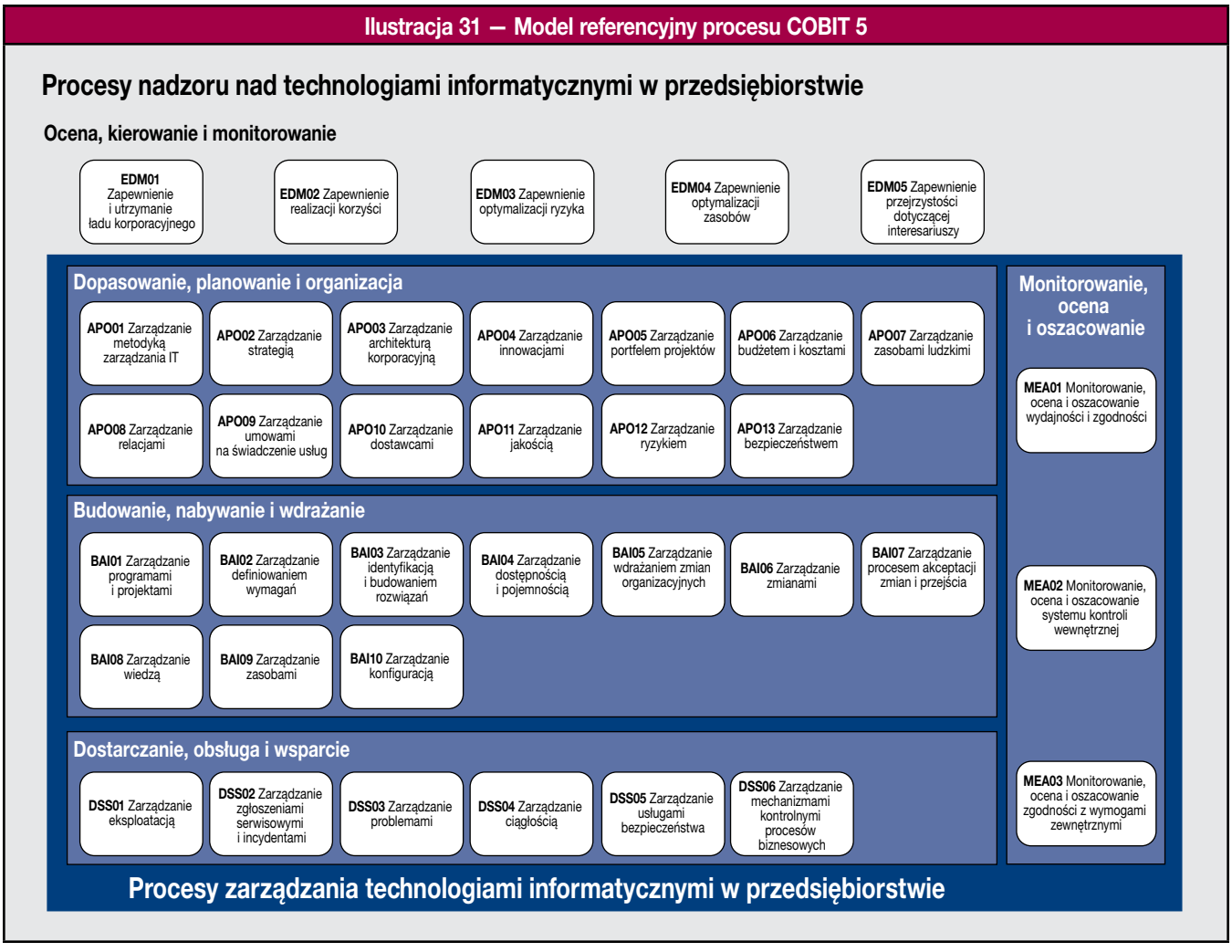
Wprowadzenie modelu operacyjnego i wspólnego języka komunikacji we wszystkich obszarach przedsiębiorstwa związanych z działaniami IT jest jednym z najważniejszych i kluczowych kroków w kierunku odpowiedniego nadzoru. Zapewnia to również metodykę pomiaru i monitorowania sprawności IT, komunikacji z dostawcami usług oraz wdrażania najlepszych praktyk zarządzania.

W modelu referencyjnym procesu COBIT 5 dodatkowo podzielono procesy nadzoru i zarządzania w zakresie technologii informatycznych w przedsiębiorstwie na dwa główne obszary działania — nadzór oraz zarządzanie — podzielone na domeny i procesy:
- **Nadzór** — Ta domena obejmuje pięć procesów nadzoru; w ramach każdego procesu zdefiniowano praktyki EDM;
- **Zarządzanie** — Te cztery domeny są zgodne z obszarami odpowiedzialności w zakresie PBRM (rozwinięcie domen metodyki COBIT 4.1), zapewniając całościowy wgląd w działalność IT. Każda domena obejmuje szereg procesów, tak jak w metodyce COBIT 4.1 i wcześniejszych wersjach. Choć, jak wcześniej opisano, większość procesów wymaga działań związanych z planowaniem, wdrożeniem, realizacją i monitorowaniem w ramach procesów lub w ramach konkretnego problemu (np. jakość, bezpieczeństwo), są one umieszczane w domenach odpowiadających najbardziej właściwemu obszarowi działania, gdy rozpatruje się IT z poziomu przedsiębiorstwa.

W metodyce COBIT 5 procesy obejmują również pełny zakres działań biznesowych oraz IT związanych z nadzorem nad technologiami informatycznymi w przedsiębiorstwie i zarządzaniem nimi, co sprawia, że model procesów dotyczy faktycznie całego przedsiębiorstwa.

Model referencyjny procesu COBIT 5 jest następcą modelu procesów COBIT 4.1, łączy w sobie również modele procesów Risk IT oraz Val IT. Na **ilustracji 31** przedstawiono pełny zestaw 37 procesów nadzoru i zarządzania w ramach metodyki COBIT 5. Szczegóły wszystkich procesów, zgodnie z opisanym wcześniej modelem procesów, można znaleźć w przewodniku *COBIT 5: Procesy umożliwiające*.

Ilustracja 31 — Model referencyjny procesu COBIT 5

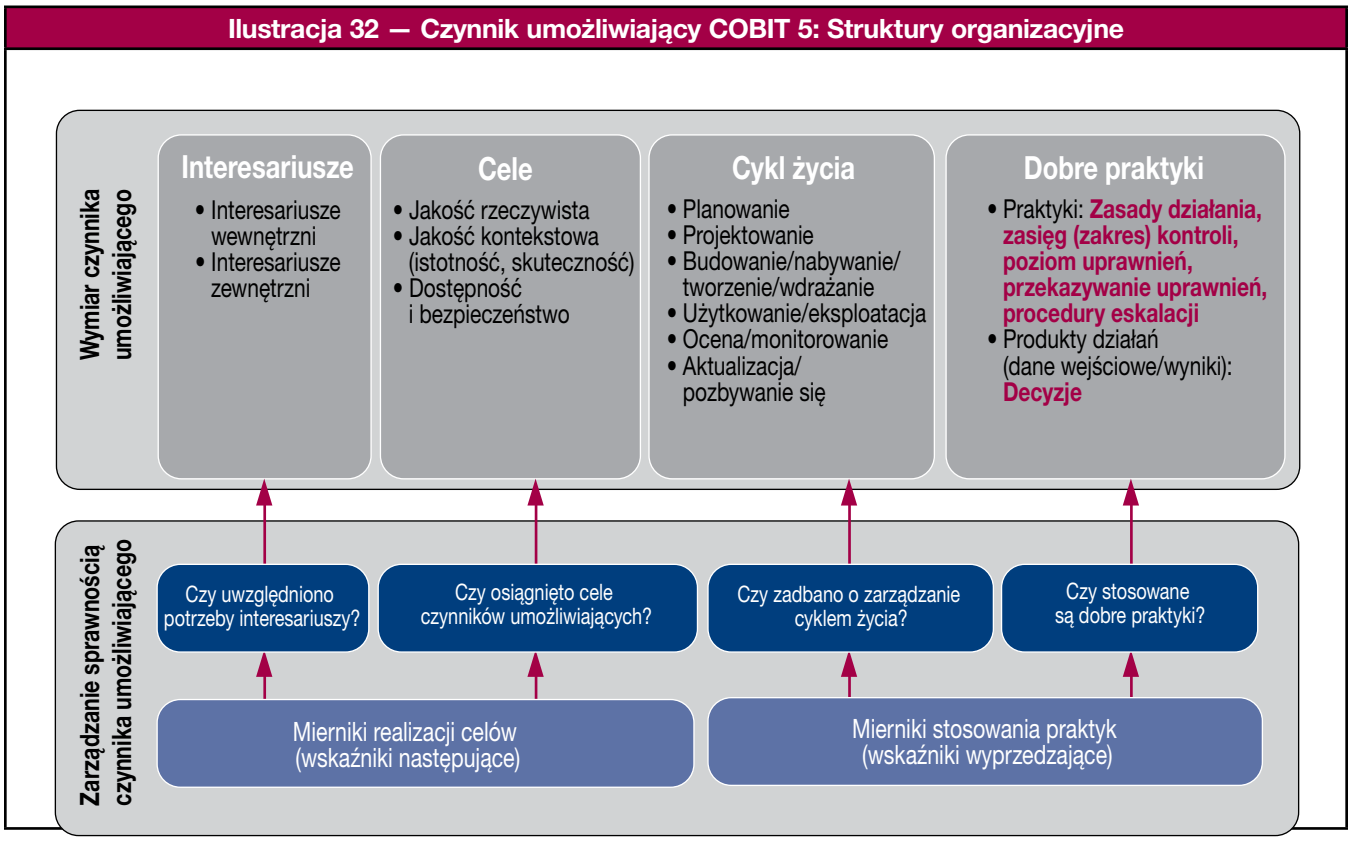


Czynnik umożliwiający COBIT 5: Struktury organizacyjne

Szczegóły czynnika umożliwiającego dotyczącego struktur organizacyjnych w porównaniu z opisem typowego czynnika umożliwiającego przedstawiono na **ilustracji 32**.

Model struktur organizacyjnych składa się z następujących elementów:
- **Interesariusze** — interesariusze w odniesieniu do struktur organizacyjnych przedsiębiorstwa mogą być wewnętrzni lub zewnętrzni; do ich grona należą poszczególni członkowie struktury, inne struktury, organizacje, klienci, dostawcy i organy regulacyjne. Ich role są różnorodne i obejmują podejmowanie decyzji, wywieranie wpływu i doradztwo. Różnią się także interesy każdego z interesariuszy, tj. ich zaangażowanie w decyzje podejmowane w ramach struktury.
- **Cele** — dla czynnika umożliwiającego dotyczącego struktur organizacyjnych obejmowałyby posiadanie właściwego umocowania, dobrze zdefiniowanych zasad działania oraz stosowanie innych dobrych praktyk. Wynik czynnika umożliwiającego dotyczącego struktur organizacyjnych powinien obejmować szereg odpowiednich działań i decyzji.
- **Cykl życia** — struktura organizacyjna ma cykl życia. Zostaje utworzona, istnieje, jest dostosowywana, a ostatecznie może zostać rozwiązana. W chwili jej założenia musi zostać zdefiniowany mandat — powód i cel jej istnienia.
- **Dobre praktyki** — można wyróżnić szereg dobrych praktyk dotyczących struktur organizacyjnych, np.:
  - Zasady działania — praktyczne ustalenia dotyczące sposobu działania struktury, np. częstotliwość zebrań, reguły dokumentacji i zachowania właściwego porządku;
  - Skład — struktury składają się z członków, którzy są interesariuszami wewnętrznymi lub zewnętrznymi;
  - Zakres kontroli — granice uprawnień decyzyjnych struktury organizacyjnej;
  - Poziom decyzyjny/uprawnienia decyzyjne — decyzje, do których podjęcia struktura jest uprawniona;
  - Przekazywanie uprawnień — struktury mogą przekazywać uprawnienia decyzyjne (lub ich podzbiór) innym, podległym im strukturom;
  - Procedury eskalacji — ścieżka eskalacji dla struktury, opisująca wymagane działania w przypadku problemów z podjęciem decyzji.

Ilustracja 32 — Czynnik umożliwiający COBIT 5: Struktury organizacyjne



Relacje z innymi czynnikami umożliwiającymi — powiązania z innymi czynnikami umożliwiającymi:
- Tabele RACI umożliwiają powiązanie działań w ramach procesów ze strukturami organizacyjnymi i/lub poszczególnymi rolami w przedsiębiorstwie. Opisują one stopień zaangażowania każdej z ról w realizację poszczególnych praktyk procesów: strona odpowiedzialna, rozliczana, konsultowana lub informowana.
- Kultura, etyka i zachowanie determinują wydajność i skuteczność struktur organizacyjnych oraz ich decyzji.
- Skład struktur organizacyjnych powinien uwzględniać i odzwierciedlać właściwy zbiór umiejętności ich członków.
- Mandat i zasady działania struktur organizacyjnych są określone we wdrożonej strukturze polityk.

• Dane wejściowe i wyniki — struktura podejmuje świadome decyzje na podstawie danych wejściowych (zazwyczaj informacji) i przedstawia wyniki, na przykład decyzje, inne informacje lub żądania dodatkowych danych wejściowych.

PRZYKŁADOWE STRUKTURY ORGANIZACYJNE W METODYCE COBIT 5

Jak wspomniano przy okazji omówienia modelu procesów COBIT 5, przykładowy model referencyjny procesu COBIT 5 został utworzony i szczegółowo opisany w przewodniku *COBIT 5: Procesy umożliwiające*. Model obejmuje tabele RACI, wykorzystujące szereg ról i struktur. Na **ilustracji 33** opisano te wstępnie zdefiniowane role i struktury.

Uwagi:
• Nie muszą one odpowiadać rzeczywistym funkcjom wdrożonym przez przedsiębiorstwa, niemniej są one wartościowe w tym sensie, że opisany cel struktury lub roli zachowuje ważność w przypadku większości przedsiębiorstw.
• Celem tej tabeli nie jest określenie uniwersalnej struktury organizacyjnej dla każdego przedsiębiorstwa. Ma ona jedynie charakter ilustracyjny.

Ilustracja 33 — Role i struktury organizacyjne w ramach metodyki COBIT 5

Rola/struktura	Definicja/opis
Zarząd	Grupa przedstawicieli kadry kierowniczej najwyższego szczebla i/lub dyrektorów niewykonawczych w przedsiębiorstwie rozliczanych za nadzór nad przedsiębiorstwem i sprawujących ogólną kontrolę nad jego zasobami.
Dyrektor generalny (CEO)	Najwyższy rangą dyrektor odpowiedzialny za pełne zarządzanie przedsiębiorstwem.
Dyrektor ds. finansowych (CFO)	Menedżer najwyższego szczebla w przedsiębiorstwie odpowiedzialny za wszystkie aspekty zarządzania finansami, w tym za ryzyko finansowe i mechanizmy kontrolne, a także za wiarygodną i dokładną rachunkowość.
Dyrektor ds. operacyjnych (COO)	Menedżer najwyższego szczebla odpowiedzialny za funkcjonowanie przedsiębiorstwa.
Dyrektor ds. ryzyka (CRO)	Menedżer najwyższego szczebla odpowiedzialny w odniesieniu do wszystkich aspektów zarządzania ryzykiem w ramach całego przedsiębiorstwa. Ustanowiona może zostać funkcja dyrektora ds. ryzyka informatycznego, który będzie sprawować nadzór nad ryzykiem związanym z IT.
Dyrektor ds. informatyki (CIO)	Menedżer najwyższego szczebla w przedsiębiorstwie odpowiedzialny za dopasowanie strategii IT i strategii biznesowej oraz odpowiedzialny za planowanie, optymalizację zasobów oraz zarządzanie dostarczaniem usług i rozwiązań IT w ramach wspierania realizacji celów przedsiębiorstwa.
Dyrektor ds. bezpieczeństwa informacji (CISO)	Dyrektor najwyższego szczebla w przedsiębiorstwie odpowiedzialny za bezpieczeństwo informacji przedsiębiorstwa we wszystkich formach.
Członek naczelnego kierownictwa	Przedstawiciel kierownictwa wyższego szczebla odpowiedzialny za działalność danej jednostki biznesowej lub spółki zależnej.
Właściciel procesu biznesowego	Osoba odpowiedzialna za sprawność procesu przez realizację jego celów, dążenie do doskonalenia procesu oraz zatwierdzanie zmian dotyczących procesu.
Komitet ds. strategii (wykonawczy IT)	Grupa członków kadry kierowniczej wyższego szczebla wyznaczonych przez zarząd w celu zadbania o angażowanie zarządu w najważniejsze kwestie i decyzje związane z IT oraz informowanie go o nich. Komitet jest rozliczany za zarządzanie portfelami inwestycji wspieranych przez IT, usług IT i zasobów IT, dbając o uzyskanie wartości i zarządzanie ryzykiem. Przewodniczącym komitetu jest zazwyczaj członek zarządu, nie zaś dyrektor ds. informatyki (CIO).
Komitety sterujące (ds. realizacji projektów i programów)	Grupa interesariuszy i ekspertów odpowiedzialnych za wytyczne w odniesieniu do programów i projektów, w tym dotyczące zarządzania planami i monitorowania ich, przydzielania zasobów, dostarczania korzyści i wartości oraz zarządzania ryzykiem związanym z programami i projektami.
Rada ds. Architektury	Grupa interesariuszy i ekspertów odpowiedzialna za wytyczne odnoszące się do kwestii i decyzji dotyczących architektury korporacyjnej oraz za opracowywanie polityk i standardów w zakresie architektury.
Komitet ds. zarządzania ryzykiem w przedsiębiorstwie	Grupa członków kadry kierowniczej odpowiedzialna za współpracę i uzgadnianie wspólnego stanowiska na poziomie przedsiębiorstwa, wymaganych w celu wspierania działań i decyzji w zakresie zarządzania ryzykiem przedsiębiorstwa (ERM). Może zostać powołana rada ds. ryzyka informatycznego, która bardziej szczegółowo zajmie się ryzykiem informatycznym w przedsiębiorstwie i będzie doradzać komitetowi ds. ryzyka.
Dyrektor ds. zarządzania zasobami ludzkimi	Menedżer najwyższego szczebla odpowiedzialny za planowanie i polityki w odniesieniu do zarządzania zasobami ludzkimi w tym przedsiębiorstwie.
Zgodność	Funkcja w przedsiębiorstwie odpowiedzialna za wytyczne dotyczące zgodności z wymogami prawnymi, regulacyjnymi i wynikającymi z umów.
Audyt	Funkcja w przedsiębiorstwie odpowiedzialna za przeprowadzanie audytów wewnętrznych.
Dyrektor ds. architektury	Członek wyższej kadry kierowniczej odpowiedzialny za proces związany z architekturą korporacyjną.
Dyrektor ds. rozwoju	Członek wyższej kadry kierowniczej odpowiedzialny za procesy związane z rozwojem rozwiązań w zakresie IT.
Dyrektor ds. operacji IT	Członek wyższej kadry kierowniczej odpowiedzialny za środowiska operacyjne oraz infrastrukturę IT.

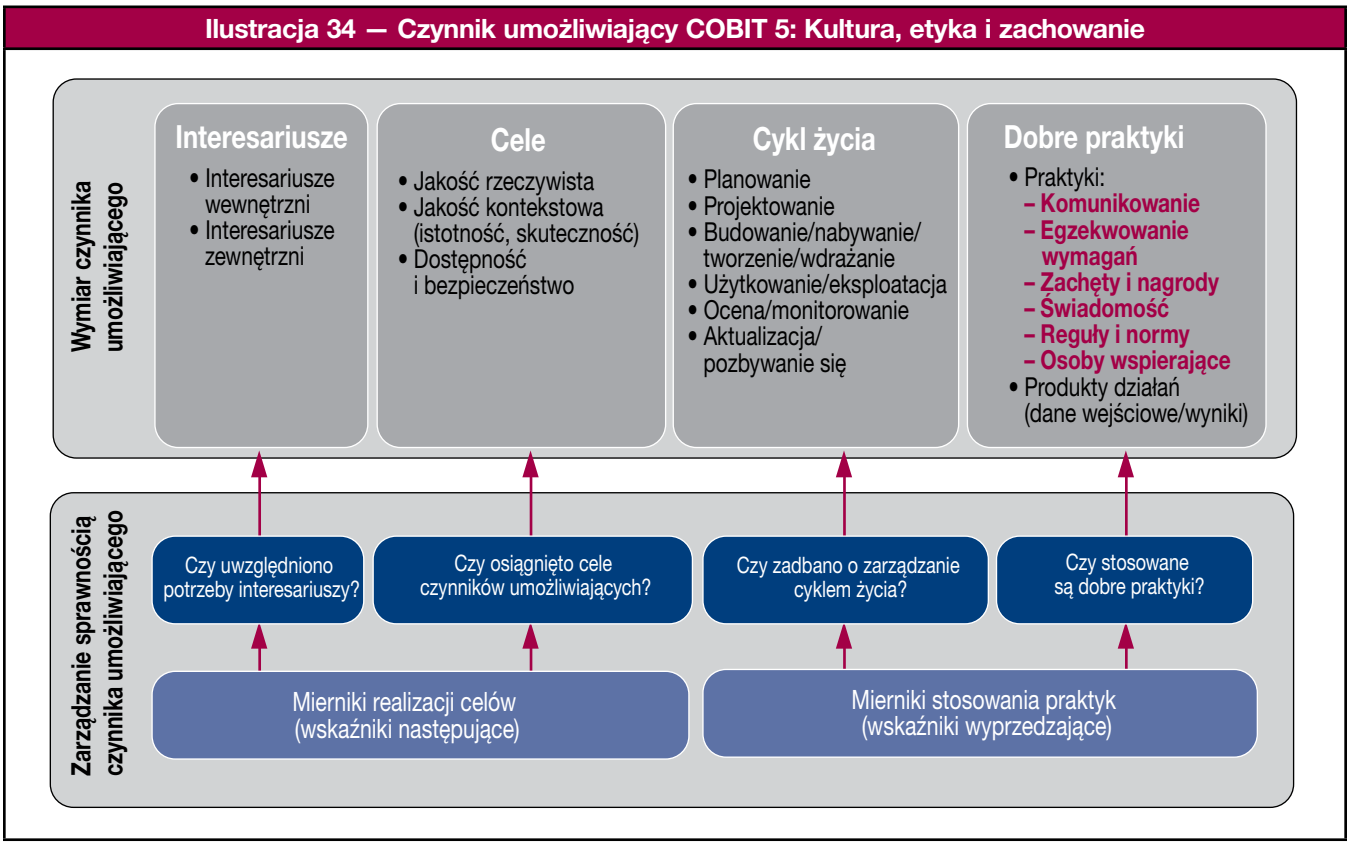
Ilustracja 33 — Role i struktury organizacyjne w ramach metodyki COBIT 5 *(ciąg dalszy)*	
Rola/struktura	**Definicja/opis**
Dyrektor ds. administracji IT	Członek wyższej kadry kierowniczej odpowiedzialny za zapisy związane z IT oraz kwestie administracyjne związane z IT.
Biuro zarządzania projektami i programami (PMO)	Funkcja odpowiedzialna za wspieranie kierowników programów i projektów oraz za gromadzenie, ocenę i raportowanie informacji dotyczących realizacji programów oraz projektów wchodzących w ich skład.
Biuro zarządzania wartością (VMO)	Funkcja działająca jako sekretariat ds. zarządzania portfelem inwestycji i portfelem usług, z uwzględnieniem szacowania i doradztwa w odniesieniu do szans inwestycyjnych oraz uzasadnień biznesowych, zalecania metod i mechanizmów kontrolnych w zakresie nadzoru/zarządzania wartością, a także raportowania postępów procesu utrzymania i tworzenia wartości dzięki inwestycjom i usługom.
Kierownik ds. usług	Osoba zarządzająca rozwojem, wdrożeniem i oceną nowych oraz istniejących produktów i usług, a także zarządzaniem nimi, na rzecz określonego klienta (użytkownika) lub grupy klientów (użytkowników).
Kierownik ds. bezpieczeństwa informacji	Osoba zajmująca się projektowaniem, nadzorowaniem i/lub oceną bezpieczeństwa informacji oraz zarządzaniem nim w przedsiębiorstwie.
Kierownik ds. ciągłości działalności biznesowej	Osoba odpowiedzialna za zarządzanie potencjałem przedsiębiorstwa w zakresie zapewniania ciągłości działalności biznesowej, a także projektowanie, nadzorowanie i/lub ocenę tych zdolności, w celu zadbania o ciągłość działania funkcji krytycznych w przedsiębiorstwie po zdarzeniach powodujących zakłócenia.
Dyrektor ds. prywatności	Osoba odpowiedzialna za monitorowanie ryzyka oraz wpływu na biznes przepisów w zakresie ochrony prywatności, a także za ukierunkowanie i koordynację wdrażania polityk i działań, które zapewnią przestrzeganie dyrektyw dotyczących prywatności. Zwany również dyrektorem ds. ochrony danych

Strona celowo pozostawiona pusta

Czynnik umożliwiający COBIT 5: Kultura, etyka i zachowanie

Kultura, etyka i zachowanie odnoszą się do zbioru zachowań indywidualnych i zbiorowych w ramach przedsiębiorstwa. Szczegóły czynnika umożliwiającego dotyczącego kultury, etyki i zachowania w porównaniu z opisem typowego czynnika umożliwiającego przedstawiono na **ilustracji 34**.

Ilustracja 34 — Czynnik umożliwiający COBIT 5: Kultura, etyka i zachowanie



Model kultury, etyki i zachowania składa się z następujących elementów:

- **Interesariusze** — interesariusze w odniesieniu do kultury, etyki i zachowania mogą być wewnętrzni i zewnętrzni wobec przedsiębiorstwa. Do interesariuszy wewnętrznych należą osoby w całym przedsiębiorstwie, zaś interesariuszami zewnętrznymi są m.in. organy regulacyjne, np. audytorzy zewnętrzni lub organy nadzorujące. Ich interesy mają dwojaki charakter: Niektórzy interesariusze, np. dyrektorzy działów prawnych, kierownicy ds. ryzyka, kierownicy ds. zarządzania zasobami ludzkimi, rady i dyrektorzy ds. wynagrodzeń, zajmują się definiowaniem, wdrażaniem i egzekwowaniem pożądanych wzorców zachowań, podczas gdy inni muszą zadbać o zgodność ze zdefiniowanymi regułami i normami.
- **Cele** — cele w zakresie czynnika umożliwiającego dotyczącego Kultura, etyka i zachowanie odnoszą się do:
  – etyki organizacji determinowanej przez wartości, które mają być podstawą funkcjonowania przedsiębiorstwa;
  – etyki indywidualnej determinowanej osobistymi wartościami każdego z pracowników przedsiębiorstwa i uzależnionej — w znacznym stopniu — od czynników zewnętrznych, takich jak religia, pochodzenie, status społeczno-ekonomiczny, obszar geograficzny i osobiste doświadczenia;
  – indywidualnych wzorców zachowań, które łącznie określają kulturę przedsiębiorstwa. Na zachowania wpływa wiele czynników, takich jak wymienione wyżej czynniki zewnętrzne, ale także relacje interpersonalne w przedsiębiorstwach, osobiste cele i ambicje. Niektóre rodzaje zachowań, które mogą być istotne w tym kontekście, obejmują:
    - Zachowanie związane z podejmowaniem ryzyka — jak duże ryzyko przedsiębiorstwo może w swojej ocenie przyjąć i jakie ryzyko jest gotowe podjąć?
    - Zachowanie związane z przestrzeganiem polityki — w jakim stopniu pracownicy przyjmują politykę i przestrzegają jej?
    - Zachowanie w przypadku negatywnych wyników — w jaki sposób przedsiębiorstwo radzi sobie z negatywnymi wynikami, tj. wystąpieniem szkody lub utraconymi szansami? Czy przedsiębiorstwo traktuje je jako okazję do nauki i stara się zmienić sposób funkcjonowania, czy też poprzestaje na przypisaniu winy bez wyeliminowania pierwotnej przyczyny?
- **Cykl życia** — kultura organizacyjna, postawa etyczna oraz wzorce zachowań poszczególnych pracowników itp. mają swoje cykle życia. Zaczynając od istniejącej kultury, przedsiębiorstwo może zidentyfikować wymagane zmiany i zadbać o ich wdrożenie. Można wykorzystać kilka narzędzi opisanych w dobrych praktykach.

- **Dobre praktyki** — dobre praktyki dotyczące tworzenia, promowania i utrzymywania pożądanych wzorców zachowań w ramach całego przedsiębiorstwa obejmują następujące elementy:
  – komunikowanie pożądanych wzorców zachowań oraz wartości korporacyjnych, na których się opierają, w ramach całego przedsiębiorstwa;
  – zwiększanie świadomości pożądanych wzorców zachowań dzięki przykładowi kierownictwa wyższego szczebla oraz innych osób wspierających;
  – zachęty oraz środki zniechęcające w celu promowania pożądanego zachowania. Istnieje wyraźny związek między zachowaniem poszczególnych pracowników oraz schematem wynagradzania realizowanym przez dział zarządzania zasobami ludzkimi, wdrożonym przez przedsiębiorstwo.
  – Reguły i normy zawierające dodatkowe wytyczne dotyczące pożądanych wzorców zachowań w organizacji. Są one wyraźnie powiązane z zasadami i politykami wdrożonymi przez przedsiębiorstwo.
- **Relacje z innymi czynnikami umożliwiającymi** — powiązania z innymi czynnikami umożliwiającymi:
  – Procesy mogą zostać zaprojektowane w sposób doskonały, ale jeśli interesariusze procesu nie zechcą zrealizować działań w ramach procesu we właściwy sposób (tj. jeśli ich zachowanie nastawione jest na niespełnienie kryteriów zgodności), wyniki procesu nie zostaną uzyskane.
  – Podobnie struktury organizacyjne mogą zostać zaprojektowane i utworzone w sposób podręcznikowy, ale jeśli ich decyzje nie będą wdrażane — ze względu na różnice w zamiarach poszczególnych osób, brak zachęt itd. — nie zapewnią odpowiedniego nadzoru i zarządzania w odniesieniu do technologii informatycznych w przedsiębiorstwie.
  – Zasady i polityki są bardzo ważnym mechanizmem komunikowania wartości korporacyjnych oraz pożądanego zachowania.

PRZYKŁAD 11 – POPRAWA JAKOŚCI

Przedsiębiorstwo zmaga się z poważnymi, nawracającymi problemami dotyczącymi jakości nowych aplikacji. Mimo wdrożenia rzetelnej metodyki rozwoju projektów w zakresie oprogramowania problemy związane z oprogramowaniem zbyt często powodują problemy operacyjne w codziennym funkcjonowaniu przedsiębiorstwa.

Przeprowadzone dochodzenie wykazało, że członkowie zespołu projektowego oraz jego kierownicy są oceniani i wynagradzani na podstawie terminowej realizacji projektów w ramach przyznanego budżetu. Nie stosuje się kryteriów jakościowych ani kryteriów dotyczących korzyści biznesowych. W związku z tym podczas projektowania koncentrują się na czasie realizacji oraz ograniczaniu kosztów (np. poprzez skrócenie czasu testowania). W wyniku dochodzenia wykazano również, że zgodność z przyjętą metodyką i procedurami właściwie nie istnieje, ponieważ oznaczałaby ograniczenie czasu przeznaczonego w budżecie na rozwój (kosztem czasu poświęconego na zapewnienie jakości). Ponadto – zgodnie ze strukturą organizacyjną – oficjalne zaangażowanie osób odpowiedzialnych za rozwój kończy się z chwilą przekazania obowiązków zespołowi ds. operacji. Od tego momentu zaangażowanie osób odpowiedzialnych za rozwój jest jedynie pośrednie i odbywa się wyłącznie w ramach procesu zarządzania incydentami i problemami.

Wyciągnięto wniosek, że konieczne jest wprowadzenie lepszych zachęt dla kierownictwa i zespołów odpowiedzialnych za rozwój rozwiązań w celu zachęcenia ich do położenia większego nacisku na jakość.

PRZYKŁAD 12 – RYZYKO ZWIĄZANE Z IT

Niektóre symptomy nieodpowiedniej lub problematycznej kultury w odniesieniu do ryzyka związanego z IT:

- Brak spójności między rzeczywistym apetytem na ryzyko a jego przełożeniem na polityki. Rzeczywiste podejście kadry kierowniczej do ryzyka może być stosunkowo agresywne (może być ona skłonna do podejmowania ryzyka), podczas gdy tworzone polityki odzwierciedlają znacznie bardziej konserwatywną postawę. Oznacza to, że istnieje rozbieżność między przyjętymi wartościami oraz środkami podejmowanymi w celu realizacji tych wartości, co w sposób nieuchronny prowadzi do konfliktu. Mogą na przykład występować konflikty między zachętami dla kadry kierowniczej a egzekwowaniem niedopasowanych polityk.
- Istnienie „kultury obwiniania innych". Należy za wszelką cenę unikać tego rodzaju kultury; to najważniejszy czynnik blokujący właściwą i skuteczną komunikację. W kulturze obwiniania innych jednostki biznesowe obwiniają dział IT, gdy projekty nie są realizowane w sposób terminowy i nie spełniają oczekiwań. W związku z tym nie zdają sobie sprawy ze sposobu, w jaki zaangażowanie jednostki biznesowej od samego początku wpływa na sukces projektu. W skrajnych przypadkach jednostka biznesowa może zarzucać działowi IT niespełnienie oczekiwań, które nigdy nie zostały przez nią wyraźnie przedstawione. Wzajemne obwinianie się utrudnia efektywną komunikację między jednostkami, co dodatkowo zwiększa opóźnienia. Kierownictwo musi zidentyfikować oraz szybko ograniczyć kulturę wzajemnego obwiniania się, jeśli chce wspierać współpracę w ramach całego przedsiębiorstwa.

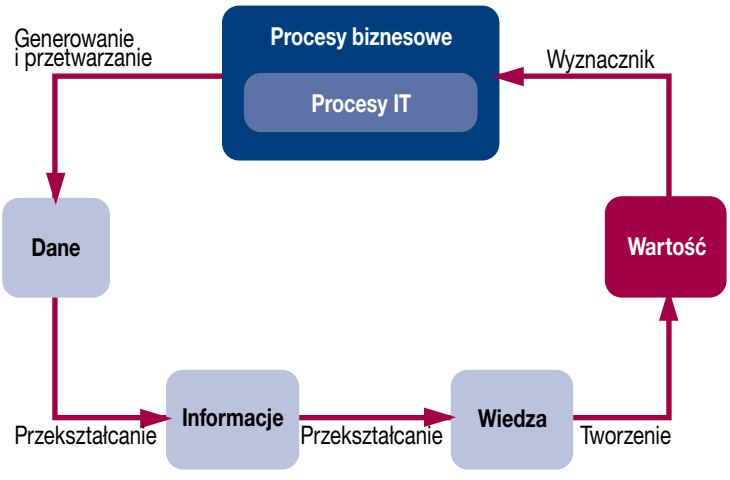
Czynnik umożliwiający COBIT 5: Informacje

Wprowadzenie — Cykl informacji

Czynnik umożliwiający Informacja odnosi się do wszystkich informacji istotnych dla przedsiębiorstw, nie tylko do zautomatyzowanych informacji. Informacje mogą być ustrukturyzowane lub nieustrukturyzowane, sformalizowane lub niesformalizowane.

Informacje można uznać za jeden z etapów cyklu informacji przedsiębiorstwa. W cyklu informacji (**ilustracja 35**) procesy biznesowe generują i przetwarzają dane, przekształcając je w informacje i wiedzę, a na koniec generując wartość dla przedsiębiorstwa. Zakres czynnika umożliwiającego Informacja dotyczy głównie fazy „informacje" w cyklu życia informacji, ale w metodyce COBIT 5 uwzględniono również aspekty danych i wiedzy.

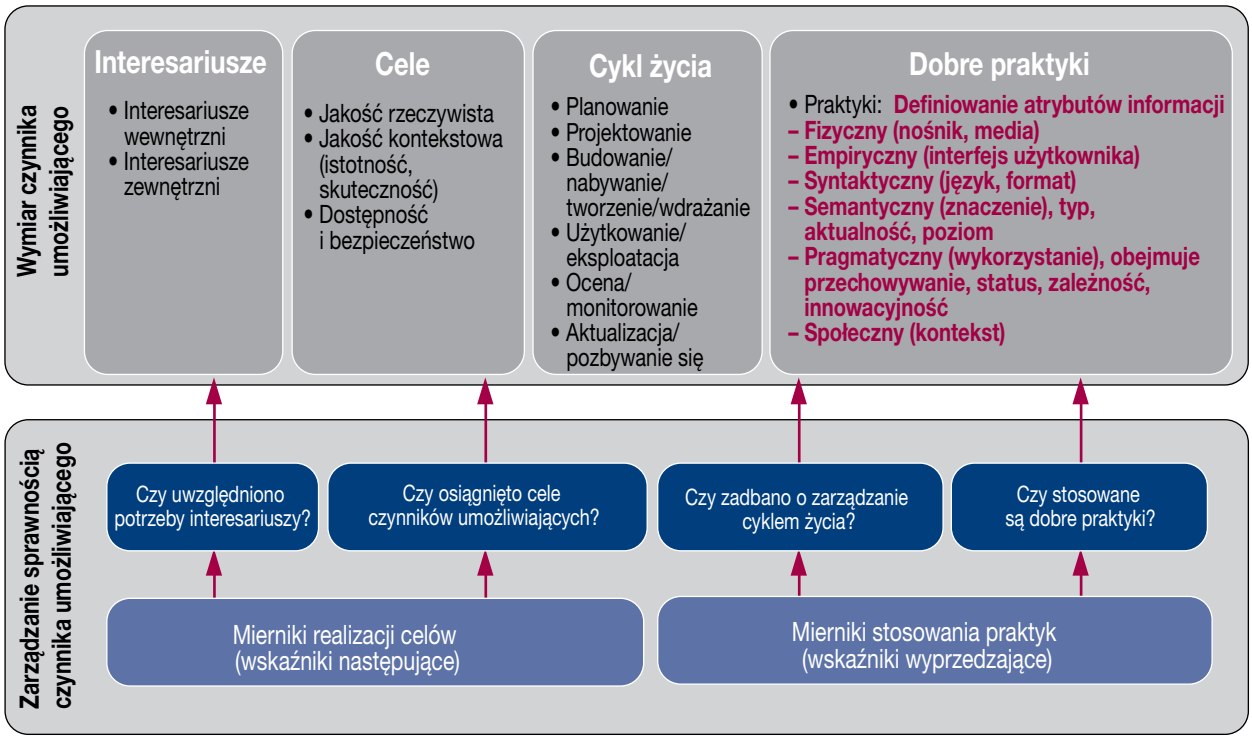
Ilustracja 35 — Metadane metodyki COBIT 5 — cykl informacji



Czynnik umożliwiający Informacja w ramach metodyki COBIT 5

Szczegóły czynnika umożliwiającego dotyczącego informacji w porównaniu z opisem typowego czynnika umożliwiającego przedstawiono na **ilustracji 36**.

Ilustracja 36 — Czynnik umożliwiający COBIT 5: Informacje



Model informacji składa się z następujących elementów:

- **Interesariuszy** — w przypadku każdego przedsiębiorstwa istnieją interesariusze wewnętrzni i zewnętrzni. Zgodnie z typowym modelem oprócz zidentyfikowania samych interesariuszy konieczne jest również określenie interesów, którymi się kierują, tj. stwierdzenie, na czym polega ich zaangażowanie lub dlaczego są zainteresowani informacjami.

  W zależności od tego, którzy interesariusze informacji występują w przedsiębiorstwie, można wyróżnić kilka kategorii ról dotyczących informacji — od szczegółowych ról wiążących się z wykorzystywaniem danych lub informacji (przykładem może być architekt, właściciel, zarządca, powiernik, dostawca, beneficjent, twórca modeli, zarządzający jakością lub zarządzający bezpieczeństwem), po role bardziej ogólne (np. wytwórcy informacji, opiekunowie informacji i konsumenci informacji):
  – wytwórca informacji — odpowiedzialny za tworzenie informacji;
  – opiekun informacji — odpowiedzialny za przechowywanie i utrzymywanie informacji;
  – konsument informacji — odpowiedzialny za korzystanie z informacji.
  Kategorie te odnoszą się do konkretnych działań dotyczących zasobu informacyjnego. Rodzaj działań zależy od fazy cyklu życia informacji; w związku z tym w celu znalezienia kategorii ról o odpowiednim poziomie szczegółowości dla modelu informacji można wykorzystać wymiar cyklu życia modelu informacji. Oznacza to, że role interesariuszy informacji (np. specjaliści ds. planowania informacji, osoby uzyskujące informacje, użytkownicy informacji) można zdefiniować, odwołując się do faz cyklu życia informacji. Zarazem oznacza to, że wymiar interesariusza informacji nie jest niezależnym wymiarem; dla poszczególnych faz cyklu życia istnieją różni interesariusze.

  Stosowne role zależą od fazy cyklu życia informacji, natomiast interesy mogą być związane z celami dotyczącymi informacji.
- **Cele** — cele dotyczące informacji dzielą się na trzy podwymiary jakości:
  Jakość rzeczywista — stopień, w jakim wartości danych są zgodne z faktycznymi lub prawdziwymi wartościami. Obejmuje ona:
  – dokładność — stopień, w jakim informacje są poprawne i wiarygodne;
  – obiektywność — stopień, w jakim informacje są nienacechowane z góry wyrobionym osądem, pozbawione uprzedzeń i bezstronne;
  – wiarygodność — stopień, w jakim informacje uważa się za prawdziwe i godne zaufania;
  – reputację — stopień, w jakim informacje są cenione ze względu na wartość źródła lub treści.
  Jakość zgodności z kontekstem i jakość reprezentacji — stopień, w jakim informacje są odpowiednie do realizacji zadania przez użytkownika informacji i zostały przedstawione w sposób zrozumiały i jasny, z uwzględnieniem faktu, że jakość informacji zależy od kontekstu, w jakim się je wykorzystuje. Obejmuje ona:
  – istotność — stopień, w jakim informacje dają się zastosować i są pomocne dla wykonywanego zadania;
  – kompletność — stopień, w jakim żadnych informacji nie brakuje oraz informacje mają właściwy zakres i stopień szczegółowości dla wykonywanego zadania;
  – aktualność — stopień, w jakim informacje są wystarczająco aktualne do realizacji konkretnego zadania;
  – odpowiednia ilość informacji — stopień, w jakim wolumen informacji jest odpowiedni dla wykonywanych zadań;
  – zwięzłe przedstawienie — stopień, w jakim informacje są reprezentowane w zwięzły sposób;
  – spójne przedstawienie — stopień, w jakim informacje są prezentowane w tym samym formacie;
  – możliwość interpretacji — stopień, w jakim informacje są podane w odpowiednich językach, zawierają poprawne symbole i jednostki, a definicje są jasne;
  – jasność przekazu — stopień, w jakim informacje są łatwo zrozumiałe;
  – łatwość posługiwania się — stopień, w jakim informacje są łatwe do przekształcania i można je wykorzystać do realizacji różnych zadań;
  Jakość bezpieczeństwa/dostępności — stopień, w jakim informacje są dostępne lub możliwe do uzyskania. Obejmuje ona:
  – dostępność/terminowość — stopień, w jakim informacje są dostępne, gdy są wymagane, lub istnieje możliwość ich łatwego i szybkiego uzyskania;
  – ograniczony dostęp — stopień, w jakim informacje są udostępniane wyłącznie upoważnionym stronom.

  W złączniku F. przedstawiono szczegółowe porównanie kryteriów dotyczących jakości informacji metodyki COBIT 5 z kryteriami informacji COBIT 4.1. Na przykład: integralność (zgodnie z definicją zawartą w metodyce COBIT 4.1) została uwzględniona w ramach celów dotyczących kompletności i dokładności.
- **Cykl życia** — uwzględniony musi zostać pełny cykl życia informacji, przy czym dla poszczególnych faz cyklu życia informacji wymagane mogą być odmienne podejścia. Dla czynnika umożliwiającego COBIT 5 dotyczącego informacji można wyróżnić następujące fazy:
  – **Planowanie** — faza przygotowania do tworzenia i wykorzystywania zasobu informacyjnego. Działania w tej fazie mogą odnosić się do identyfikacji celów, planowania architektury informacji, a także opracowania standardów i definicji (np. definicje danych, procedury gromadzenia danych).
  – **Projektowanie**
  – **Budowanie/nabywanie** — faza, w której nabywany jest zasób informacyjny. Działania w tej fazie mogą dotyczyć tworzenia zapisów danych, nabywania danych oraz ładowania plików zewnętrznych.
  – **Użytkowanie/obsługa, które obejmują:**
    • Przechowywanie — faza, w której informacje są przechowywane w postaci elektronicznej lub papierowej (a nawet

tylko w ludzkiej pamięci). Działania w tej fazie mogą odnosić się do przechowywania informacji w postaci elektronicznej (np. pliki elektroniczne, bazy danych, hurtownie danych) lub tradycyjnej (np. dokumenty papierowe).
- Udostępnianie — faza, w której udostępnia się informacje do wykorzystania za pomocą jednej z metod dystrybucji. Działania w tej fazie mogą odnosić się do procesów związanych z dostarczaniem informacji do miejsc, w których można do nich uzyskać dostęp i wykorzystać je (np. dystrybucja dokumentów za pośrednictwem poczty e-mail). W przypadku informacji przechowywanych w formie elektronicznej ta faza cyklu życia może w znacznym stopniu nakładać się na fazę przechowywania (np. udostępnianie informacji poprzez zapewnienie dostępu do bazy danych, serwerów plików/dokumentów).
- Wykorzystanie — faza, w której informacje wykorzystuje się do osiągnięcia celów. Działania w tej fazie mogą odnosić się do wszystkich typów wykorzystania informacji (np. podejmowania decyzji zarządczych, prowadzenia zautomatyzowanych procesów), a także mogą obejmować działania takie jak pozyskiwanie informacji oraz konwertowanie informacji (z jednej postaci na inną).

Zgodnie z podejściem zaprezentowanym w publikacji Taking Governance Forward informacje są czynnikiem umożliwiającym dla ładu korporacyjnego; w związku z tym wykorzystanie informacji w sposób zdefiniowany w modelu informacji można pojmować jako cel, do którego interesariusze przedsiębiorstwa potrzebują informacji, przyjmując swoje role, realizując działania i wchodząc w interakcje między sobą.

Owe role, działania i relacje przedstawiono na **ilustracji 9**. Interakcje między interesariuszami wymagają przepływu informacji, którego cele zostały zaznaczone na schemacie: rozliczalność, delegowanie, monitorowanie, określanie kierunku, dopasowanie, realizacja i kontrola.
- Ocena/monitorowanie — faza, w której dba się o to, aby zasób informacyjny nadal prawidłowo funkcjonował (tj. zachował wartość). Działania w tej fazie mogą polegać na zapewnieniu aktualności informacji, a także wykonywaniu innych działań związanych z zarządzaniem informacjami (np. wzbogacanie, czyszczenie, scalanie i usuwanie zduplikowanych danych w hurtowniach danych).
- Aktualizacja/pozbywanie się — faza, w której zasób informacyjny jest aktualizowany z myślą o dalszym korzystaniu lub usuwany, gdy nie jest już potrzebny. Działania podejmowane w tej fazie mogą odnosić się do archiwizowania lub niszczenia informacji.

• **Dobra praktyka** — pojęcie informacji jest rozumiane w odmienny sposób w różnych dyscyplinach, takich jak ekonomia, teoria komunikacji, informatyka, zarządzanie wiedzą i systemy informatyczne; w związku z tym nie istnieje ogólnie akceptowana definicja informacji. Charakter informacji można jednak wyjaśnić dzięki zdefiniowaniu i opisaniu ich właściwości.

Do przedstawienia struktury różnych właściwości informacji można wykorzystać schemat składający się z sześciu poziomów (warstw) umożliwiających zdefiniowanie i opisanie właściwości informacji. Owe sześć poziomów stanowi kontinuum atrybutów — od fizycznego świata informacji, w którym atrybuty są powiązane z technologiami informatycznymi oraz nośnikami umożliwiającymi uzyskiwanie, przechowywanie, przetwarzanie, dystrybucję i prezentację informacji, po społeczny świat korzystania z informacji, analizowania ich i działania na ich podstawie.

Poszczególne poziomy (warstwy) oraz atrybuty informacji można opisać w następujący sposób:
• **Warstwa świata fizycznego** — świat, w którym zachodzą wszystkie zjawiska obserwowalne empirycznie;
– Nośnik informacji/media — atrybut, który identyfikuje fizyczny nośnik informacji (np. papier, sygnały elektryczne, fale dźwiękowe);
• **Warstwa empiryczna** — empiryczna obserwacja znaków wykorzystywanych do kodowania informacji, a także rozróżnianie poszczególnych znaków i odróżnianie ich od zakłóceń w tle;
– Kanał dostępu do informacji — atrybut, który identyfikuje kanał dostępu do informacji (np. interfejsy użytkownika);
• **Warstwa syntaktyczna** — zasady i reguły budowania zdań w językach naturalnych i sztucznych. Składnia odnosi się do formy informacji;
– Kod/język — atrybut, który identyfikuje język przedstawienia/format wykorzystany do kodowania informacji; reguły łączenia symboli języka w celu utworzenia struktur składniowych;
• **Warstwa semantyczna** — zasady i reguły rozpoznawania znaczenia struktur składniowych. Semantyka odnosi się do znaczenia informacji;
– Typ informacji — atrybut identyfikujący rodzaj informacji, np. informacje finansowe i informacje niefinansowe, informacje pochodzące spoza przedsiębiorstwa a informacje utworzone w ramach przedsiębiorstwa, wartości prognozowane/przewidywane a wartości zaobserwowane, wartości zaplanowane a wartości uzyskane;
– Aktualność informacji — atrybut identyfikujący horyzont czasowy, do którego odnoszą się informacje, tj. informacje dotyczące przeszłości, teraźniejszości lub przyszłości;
– Poziom informacji — atrybut identyfikujący stopień szczegółowości informacji (np. sprzedaż roczna, kwartalna, miesięczna);
• **Warstwa pragmatyczna** — reguły i struktury dotyczące budowania większych struktur językowych służących określonym celom w komunikacji międzyludzkiej. Pragmatyka odnosi się do sposobu wykorzystania informacji;
– Okres przechowywania — atrybut, który wskazuje maksymalny okres przechowywania informacji, zanim zostaną zniszczone;
– Status informacji — atrybut, który wskazuje, czy informacje są operacyjne, czy historyczne;

  - Innowacyjność — atrybut, który wskazuje, czy informacje niosą ze sobą nową wiedzę, czy też stanowią potwierdzenie istniejącej wiedzy (tj. poinformowanie czy potwierdzenie);
  - Zależność — atrybut identyfikujący informacje, które muszą poprzedzać określone informacje (aby można je było uznać za informacje);
- **Warstwa świata społecznego** — świat skonstruowany w wymiarze społecznym poprzez wykorzystanie struktur językowych na pragmatycznym poziomie semiotyki (np. umowy, prawo, kultura);
  - Kontekst — atrybut wskazujący kontekst, w którym informacje są interpretowane, wykorzystywane, mają wartość itd., np. kontekst kulturowy, kontekst dziedziny tematycznej.

Dodatkowe uwagi dotyczące informacji — inwestycje w informacje i powiązane technologie oparte są na uzasadnieniach biznesowych (ang. business cases) obejmujących rachunek kosztów i korzyści. Koszty i korzyści odnoszą się nie tylko do łatwo uchwytnych, wymiernych czynników, ale obejmują również czynniki niewymierne, takie jak przewaga konkurencyjna, zadowolenie klienta i niepewność technologiczna. Przedsiębiorstwo może osiągać korzyści z informacji dopiero wówczas, gdy zasób informacyjny zostanie zastosowany lub wykorzystany, więc wartość informacji jest określana wyłącznie na podstawie możliwości ich wykorzystania (wewnętrznie lub poprzez ich sprzedaż) — informacje nie mają wartości same w sobie. Korzyści można uzyskać dopiero dzięki ich właściwemu wykorzystaniu.

IM (model informacji) to nowy model złożony z wielu różnych komponentów. Zostanie on szczegółowo omówiony w osobnej publikacji. Aby zwiększyć jego czytelność dla użytkowników metodyki COBIT 5 i lepiej opisać jego przydatność w ogólnym kontekście metodyki COBIT 5, przedstawiono przykłady 13, 14 i 15 dotyczące możliwego wykorzystania IM.

PRZYKŁAD 13 — MODEL INFORMACJI WYKORZYSTYWANY DO OKREŚLENIA SPECYFIKACJI INFORMACJI

Podczas opracowywania nowej aplikacji można wykorzystać model informacji, aby na jego podstawie określić specyfikację aplikacji oraz powiązanych modeli informacji lub danych.

Atrybuty informacji zawarte w modelu informacji mogą posłużyć do zdefiniowania specyfikacji dla aplikacji oraz procesów biznesowych, które będą wykorzystywać informacje.

Na przykład projekt i specyfikacje nowego systemu muszą określać następujące elementy:

- **Warstwa fizyczna** — Gdzie będą przechowywane informacje?
- **Warstwa empiryczna** — Jak można uzyskać dostęp do informacji?
- **Warstwa syntaktyczna** — Jaka będzie struktura informacji i jakie strony kodowe zostaną użyte?
- **Warstwa semantyczna** — Jakiego rodzaju są to informacje? Jaki jest poziom szczegółowości informacji?
- **Warstwa pragmatyczna** — Jakie są wymogi dotyczące przechowywania? Jakie inne informacje są wymagane w celu zapewnienia przydatności i możliwości wykorzystania tych informacji?

Analiza dwóch wymiarów informacji — interesariuszy i cyklu życia — pozwala określić, jaki rodzaj dostępu do danych jest wymagany w przypadku poszczególnych osób (dla poszczególnych faz cyklu życia informacji).

Podczas testowania aplikacji testerzy mogą przeanalizować kryteria dotyczące jakości informacji w celu opracowania kompleksowego zbioru przypadków testowych.

PRZYKŁAD 14 — MODEL INFORMACJI WYKORZYSTYWANY DO OKREŚLENIA WYMAGANEJ OCHRONY

Zespoły ds. bezpieczeństwa funkcjonujące w przedsiębiorstwie mogą skorzystać z wymiaru atrybutów modelu informacji. W ramach obowiązków związanych z ochroną informacji muszą one przeanalizować następujące warstwy:

- **Warstwa fizyczna** — Jak i gdzie fizycznie przechowuje się informacje?
- **Warstwa empiryczna** — Jakie są kanały dostępu do informacji?
- **Warstwa semantyczna** — Jakiego typu są to informacje? Czy informacje są aktualne, dotyczą przeszłości czy odnoszą się do przyszłości?
- **Warstwa pragmatyczna** — Jakie są wymogi dotyczące przechowywania? Czy informacje są historyczne, czy w użyciu produkcyjnym?

Za pomocą tych atrybutów użytkownik może określić poziom ochrony danych i wymagane mechanizmy zabezpieczające.

Analizując kolejny wymiar modelu informacji, specjaliści ds. bezpieczeństwa mogą również uwzględnić etapy cyklu życia informacji, ponieważ informacje wymagają ochrony we wszystkich fazach cyklu życia. O bezpieczeństwo należy zadbać już w fazie planowania informacji. Wymaga to zastosowania różnych mechanizmów zabezpieczających dotyczących przechowywania, udostępniania i pozbywania się informacji. Model informacji zapewnia ochronę informacji przez cały ich cykl życia.

PRZYKŁAD 15 — MODEL INFORMACJI WYKORZYSTYWANY DO OKREŚLENIA ŁATWOŚCI KORZYSTANIA Z DANYCH

Wykorzystanie modelu informacji w ramach weryfikacji procesu biznesowego (lub aplikacji) może być pomocne podczas ogólnego przeglądu informacji przetwarzanych i dostarczanych przez proces oraz zastosowanych systemów przetwarzających informacje. Kryteria jakościowe mogą zostać wykorzystane do oszacowania stopnia dostępności informacji — czy są kompletne, dostępne na czas, zgodne z faktami, istotne i dostępne w odpowiedniej ilości. Można również uwzględnić kryteria dostępności — czy informacje są dostępne, gdy jest to wymagane, i czy zapewniono im odpowiednią ochronę.

Przegląd może zostać dodatkowo rozszerzony, tak aby obejmował kryteria przedstawienia, np. zrozumiałość informacji, łatwość ich interpretacji i posługiwania się nimi.

Przegląd oparty na kryteriach modelu informacji dotyczących jakości informacji pozwala przedsiębiorstwu na uzyskanie wszechstronnego i pełnego obrazu aktualnej jakości danych wykorzystywanych w procesach biznesowych.

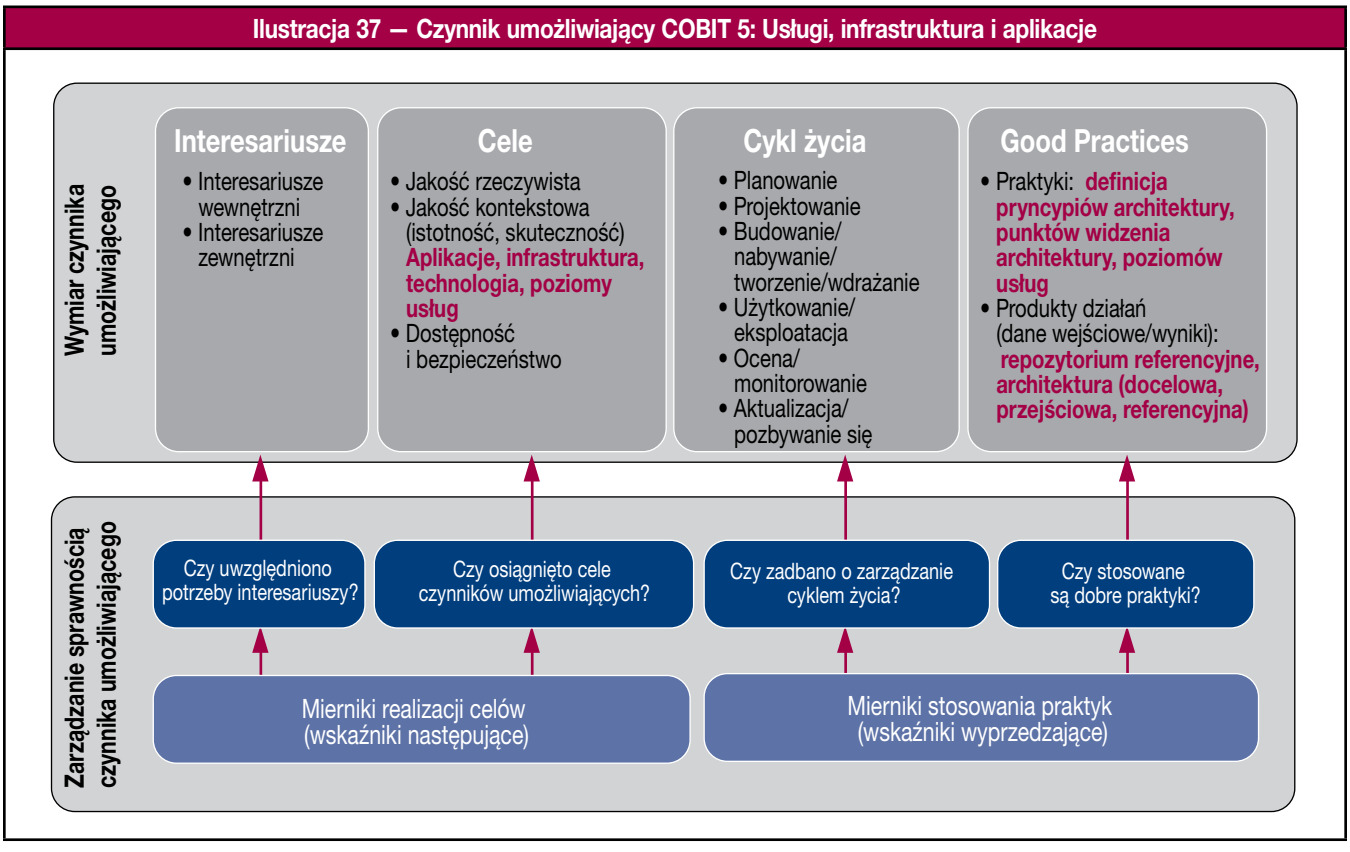
Czynnik umożliwiający COBIT 5: Usługi, infrastruktura i aplikacje

Zdolność do świadczenia usług odnosi się do zasobów takich jak aplikacje oraz infrastruktura, które wykorzystuje się do świadczenia usług związanych z IT.

Szczegóły czynnika umożliwiającego związanego ze zdolnością do świadczenia usług w porównaniu z opisem typowego czynnika umożliwiającego przedstawiono na **ilustracji 37**.

Model usług, infrastruktury i aplikacji składa się z następujących elementów:
- **Interesariuszy** — interesariusze w odniesieniu do zdolności do świadczenia usług (termin obejmujący łącznie usługi, infrastrukturę i aplikacje) mogą być wewnętrzni i zewnętrzni. Usługi mogą być dostarczane przez strony wewnętrzne i zewnętrzne — wewnętrzne działy IT, kierowników ds. operacji, dostawców zatrudnionych w ramach outsourcingu. Użytkownicy usług również mogą być wewnętrzni (użytkownicy biznesowi) lub zewnętrzni (partnerzy, klienci, dostawcy). Należy zidentyfikować interesy każdego z interesariuszy, które polegają na świadczeniu odpowiednich usług lub otrzymywaniu zamówionych usług od dostawców.
- **Cele** — dotyczące zdolności związanych z poziomem usług przedstawiono w odniesieniu do usług (aplikacje, infrastruktura, technologia) oraz poziomów usług, ze wskazaniem usług i poziomów usług, które są najbardziej ekonomiczne dla przedsiębiorstwa. Również w tym przypadku cele odnoszą się do usług i sposobu ich świadczenia, a także ich wyników, tj. wkładu w zapewnienie skutecznie wspieranych procesów biznesowych.
- **Cykl życia** — zdolność do świadczenia usług ma cykl życia. Przyszła lub planowana zdolność do świadczenia usług jest zwykle opisana w docelowej architekturze. Obejmuje ona takie istotne elementy jak przyszłe aplikacje i docelowy model infrastruktury, a także opisuje relacje i powiązania między owymi elementami.

Ilustracja 37 — Czynnik umożliwiający COBIT 5: Usługi, infrastruktura i aplikacje



Aktualna zdolność do świadczenia usług wykorzystywana do dostarczania bieżących usług IT została opisana w architekturze referencyjnej. W zależności od ram czasowych docelowej architektury zdefiniowana może zostać także architektura przejściowa, w której odzwierciedlone będą kolejne etapy prac nad architekturą docelową przedsiębiorstwa (na podstawie architektury referencyjnej).
- **Dobre praktyki** — dobre praktyki dotyczące zdolności do świadczenia usług:
  – Definicja pryncypiów architektury — zasady dotyczące architektury stanowią ogólne wytyczne odnoszące się do wdrożenia i wykorzystania zasobów związanych z IT w ramach przedsiębiorstwa. Przykłady możliwych pryncypiów architektury:

  - **Ponowne wykorzystanie** — wspólne komponenty architektury powinny być wykorzystywane podczas projektowania i wdrażania rozwiązań w ramach architektury docelowej lub przejściowej.
  - **Nabywanie lub samodzielne tworzenie** — rozwiązania należy nabywać, chyba że istnieje zatwierdzony powód, aby opracować je w ramach przedsiębiorstwa.
  - **Prostota** — architekturę korporacyjną należy zaprojektować i utrzymywać w taki sposób, aby była możliwie najprostsza, a zarazem spełniała wymagania przedsiębiorstwa.
  - **Zwinność** — architektura korporacyjna powinna charakteryzować się zwinnością, która pozwoli na spełnienie zmieniających się potrzeb biznesowych w sposób skuteczny i wydajny.
  - **Otwartość** — architektura korporacyjna powinna być oparta na otwartych standardach branżowych.
- Przyjęta w przedsiębiorstwie definicja najbardziej odpowiednich punktów widzenia architektury (w celu spełnienia potrzeb różnych interesariuszy). Są to modele, katalogi i macierze wykorzystywane do opisania architektury bazowej, docelowej lub przejściowej. Na przykład: architekturę aplikacji można opisać za pomocą schematu interfejsu aplikacji przedstawiającego wykorzystywane (lub planowane) aplikacje oraz interfejsy między nimi.
- Dysponowanie repozytorium architektury, które może być wykorzystywane do przechowywania różnych typów wyników dotyczących architektury (np. pryncypia i normy dotyczące architektury, modele referencyjne architektury oraz inne efekty procesów związanych z architekturą) i w którym zdefiniowano najważniejsze elementy usług, takie jak:
  - aplikacje zapewniające funkcjonalność biznesową;
  - infrastruktura techniczna, w tym sprzęt, oprogramowanie systemowe oraz infrastruktura sieciowa;
  - infrastruktura fizyczna.
- Poziomy usług, które muszą zostać zdefiniowane i uzyskane przez dostawców usług.

Istnieją zewnętrzne dobre praktyki dotyczące struktur architektury oraz zdolności do świadczenia usług. Są to wytyczne, szablony lub normy, które można wykorzystać do szybszego uzyskania wyników procesu związanych z architekturą. Przykłady:
- Struktura TOGAF[16] zapewnia techniczny model referencyjny oraz model referencyjny zintegrowanej infrastruktury informatycznej.
- Metodyka ITIL zawiera kompleksowe wytyczne dotyczące sposobu projektowania i wykonywania usług.

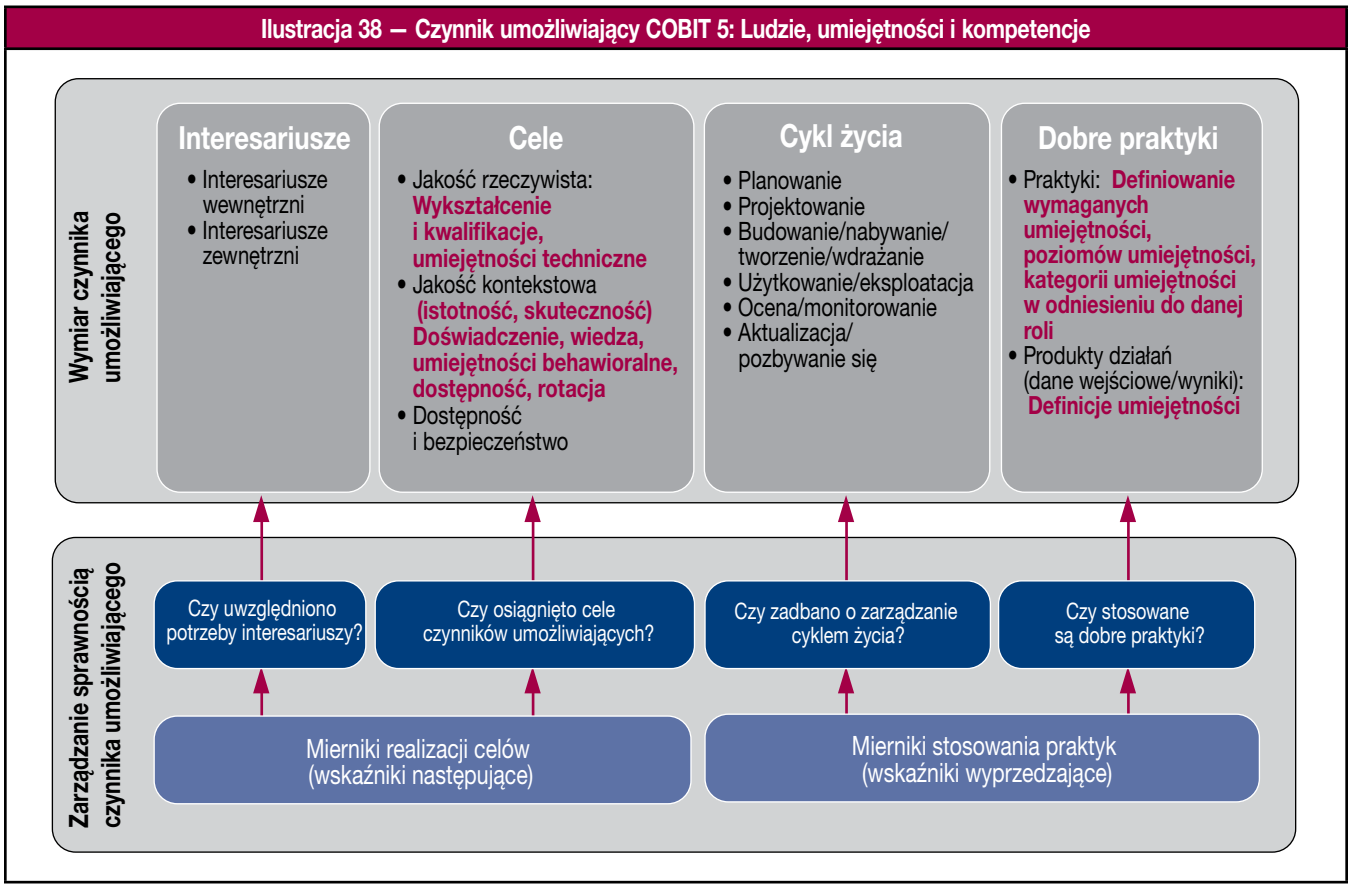
- **Relacje z innymi czynnikami umożliwiającymi** — powiązania z innymi czynnikami umożliwiającymi:
  - Informacje stanowią jedną ze zdolności do świadczenia usług, a zdolności te wykorzystuje się poprzez procesy pozwalające na świadczeniu usług wewnętrznych i zewnętrznych.
  - Gdy konieczne jest zbudowanie kultury ukierunkowanej na usługi, istotne są również aspekty związane z zachowaniem i kulturą.
  - W ramach metodyki COBIT 5 dane wejściowe i wyniki praktyk oraz działań dotyczących zarządzania mogą obejmować zdolności do świadczenia usług, wymagane jako dane wejściowe lub uzyskiwane jako wyniki.

[16] *www.opengroup.org/togaf*

Czynnik umożliwiający COBIT 5: Ludzie, umiejętności i kompetencje

Szczegóły czynnika umożliwiającego dotyczącego ludzi, umiejętności i kompetencji w porównaniu z opisem typowego czynnika umożliwiającego przedstawiono na **ilustracji 38**.

Ilustracja 38 — Czynnik umożliwiający COBIT 5: Ludzie, umiejętności i kompetencje



Model dotyczący ludzi, umiejętności i kompetencji składa się z następujących elementów:

- **Interesariuszy** — interesariusze przedsiębiorstwa w odniesieniu do umiejętności i kompetencji mogą być wewnętrzni lub zewnętrzni. Różni interesariusze pełnią odmienne role (kierownicy obszaru biznesowego, kierownicy projektów, partnerzy, konkurenci, osoby odpowiedzialne za rekrutację, specjaliści ds. szkoleń, programiści, specjaliści techniczni ds. IT itd.), a każda rola wymaga osobnego zestawu umiejętności.
- **Cele** — cele dotyczące umiejętności i kompetencji odnoszą się do wykształcenia i poziomu kwalifikacji, umiejętności technicznych doświadczenia, wiedzy i umiejętności behawioralnych wymaganych do zapewnienia i skutecznej realizacji działań w ramach procesów, ról organizacyjnych itd. Cele dotyczące osób obejmują odpowiednie poziomy dostępności personelu i wskaźnik rotacji.
- **Cykl życia**:
  - Umiejętności i kompetencje mają cykl życia. Przedsiębiorstwo musi mieć wgląd w aktualną bazę umiejętności i odpowiednio ją planować. Istotny wpływ mają w tym przypadku (oprócz innych kwestii) strategia i cele przedsiębiorstwa. Umiejętności należy rozwijać (np. poprzez szkolenia) lub pozyskiwać (np. poprzez rekrutację) i wdrażać w różnych rolach w ramach struktury organizacyjnej. Może zaistnieć potrzeba pozbycia się umiejętności, np. gdy dane działanie zostało zautomatyzowane lub zlecone w ramach outsourcingu.
  - Okresowo (np. raz w roku) przedsiębiorstwo musi ocenić bazę umiejętności w celu zrozumienia zmiany, która nastąpiła. Zostanie ona włączona do procesu planowania w odniesieniu do kolejnego okresu.
  - Wyniki oceny mogą również zostać włączone do procesu wyróżniania i wynagradzania dla celów zarządzania zasobami ludzkimi.
- **Dobre praktyki:**
  - Dobra praktyka dotycząca umiejętności i kompetencji obejmuje zdefiniowanie wymogów dotyczących obiektywnych zestawów umiejętności dla każdej z ról odgrywanych przez różnych interesariuszy. Można to opisać za pomocą różnych poziomów umiejętności w poszczególnych kategoriach umiejętności. Dla każdego odpowiedniego poziomu umiejętności w poszczególnych kategoriach powinna być dostępna definicja umiejętności. Kategorie umiejętności odnoszą się do podejmowanych działań związanych z IT, np. zarządzania informacjami, analizy biznesowej.

– Inne dobre praktyki:
  • Istnieją zewnętrzne źródła dobrych praktyk, takie jak Skills Framework for the Information Age (SFIA)[17], metodyka zawierająca kompleksowe definicje umiejętności.
  • Przykłady potencjalnych kategorii umiejętności przyporządkowanych do domen procesów COBIT 5 przedstawiono na **ilustracji 39**.

Ilustracja 39 — Kategorie umiejętności w ramach metodyki COBIT 5

Domena procesów	Przykłady kategorii umiejętności
Ocena, kierowanie i monitorowanie (EDM)	• Nadzór nad technologiami informatycznymi w przedsiębiorstwie
Dopasowanie, planowanie i organizacja (APO)	• Opracowanie polityki IT • Strategia IT • Architektura korporacyjna • Innowacje • Zarządzanie finansowe • Zarządzanie portfelami projektów
Budowanie, nabywanie i wdrażanie (BAI)	• Analiza biznesowa • Zarządzanie projektami • Ocena użyteczności • Definiowanie wymagań i zarządzanie nimi • Programowanie • Ergonomia systemu • Wycofanie oprogramowania z użycia • Zarządzanie pojemnością
Dostarczanie, obsługa i wsparcie (DSS)	• Zarządzanie dostępnością • Zarządzanie problemami • Zarządzanie jednostką Service Desk i incydentami • Administracja bezpieczeństwa • Eksploatacja IT • Administrowanie bazami danych
Monitorowanie, ocena i oszacowanie (MEA)	• Weryfikacja zgodności • Monitorowanie sprawności • Audyt mechanizmów kontrolnych

• **Relacje z innymi czynnikami umożliwiającymi** — powiązania z innymi czynnikami umożliwiającymi:
  – Realizacja działań w ramach procesów oraz podejmowanie decyzji w strukturach organizacyjnych wymaga umiejętności i kompetencji. Z drugiej strony niektóre procesy mają na celu zapewnienie wsparcia dla cyklu życia umiejętności i kompetencji.
  – Istnieje również związek z kulturą, etyką i zachowaniem poprzez umiejętności behawioralne, które wpływają na zachowanie poszczególnych pracowników i są determinowane przez etykę indywidualną i organizacyjną.
  – Definicje umiejętności są również informacjami, dla których należy rozważyć dobre praktyki przypisane do czynnika umożliwiającego Informacja.

[17] *www.sfia.org.uk*

Załącznik H
Terminologia

TERMIN	DEFINICJA
Strona rozliczana (RACI)	Osoba, grupa lub jednostka ostatecznie odpowiedzialna za daną kwestię, proces lub zakres. W tabeli RACI odpowiada na pytanie: **Kto odpowiada za powodzenie zadania?**
Rozliczalność za nadzór	Nadzór zapewnia realizację celów przedsiębiorstwa dzięki ocenie potrzeb, warunków i opcji interesariuszy, określaniu kierunków poprzez nadanie priorytetów i podejmowanie decyzji oraz dzięki monitorowaniu sprawności, zgodności i postępów działań w odniesieniu do planów. W większości przedsiębiorstw za nadzór odpowiada zarząd pod przywództwem prezesa.
Działanie	W metodyce COBIT jest to podstawowa czynność podejmowana w ramach obsługi procesu. Stanowi wytyczną dotyczącą praktyk zarządzania ukierunkowaną na zapewnienie skutecznego nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi. Działania: • Opisują zbiór koniecznych i wystarczających kroków zorientowanych na działanie, wymaganych do wdrożenia praktyki nadzoru lub praktyki zarządzania. • Uwzględniają dane wejściowe i wyniki procesu. • Są oparte na ogólnie akceptowanych normach i dobrych praktykach. • Ułatwiają wyznaczenie jasnych ról i zakresów odpowiedzialności. • Nie mają charakteru normatywnego i muszą zostać dostosowane oraz rozwinięte w celu opracowania konkretnych procedur odpowiednich dla przedsiębiorstwa.
Dopasowanie	Stan, w którym czynniki umożliwiające w odniesieniu do nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi wspierają realizację celów i strategii przedsiębiorstwa.
Architektura aplikacji	Opis logicznego grupowania zdolności, które pozwalają na zarządzanie obiektami niezbędnymi do przetwarzania informacji oraz wspierają realizację celów przedsiębiorstwa.
Rada ds. Architektury	Grupa interesariuszy i ekspertów odpowiedzialna za wytyczne odnoszące się do kwestii i decyzji dotyczących architektury korporacyjnej oraz za opracowywanie polityk i standardów w zakresie architektury.
Uwierzytelnienie	Akt weryfikacji tożsamości użytkownika oraz jego uprawnień dostępu do informacji w systemach komputerowych. Uwaga na temat zakresu: Audyt: Uwierzytelnienie ma na celu ochronę przed nieuprawnionym logowaniem. Może również odnosić się do weryfikacji poprawności danych.
Architektura referencyjna	Istniejący opis podstawowego projektu komponentów systemu biznesowego przed rozpoczęciem cyklu przeglądu i ponownego projektowania architektury.
Realizacja korzyści	Jeden z celów nadzoru. Uzyskiwanie przez przedsiębiorstwo nowych korzyści, utrzymanie i rozszerzenie istniejących form korzyści oraz wyeliminowanie inicjatyw i zasobów, które nie generują wystarczającej wartości.
Ciągłość działalności biznesowej	Zapobieganie zakłóceniom działalności, łagodzenie ich skutków i odtwarzanie. W tym kontekście używane bywają również terminy „planowanie wznowienia działalności biznesowej”, „planowanie odtworzenia po katastrofie” oraz „planowanie awaryjne”; koncentrują się one na aspektach ciągłości związanych z odtwarzaniem, w związku z czym pod uwagę należy brać również aspekt dotyczący odporności.
Cel biznesowy	Przełożenie misji przedsiębiorstwa z deklaracji zamiaru na cele działania i wyniki.
Mechanizmy kontrolne procesów biznesowych	Polityki, procedury, praktyki i struktury organizacyjne stworzone w celu racjonalnego zapewnienia realizacji celów biznesowych związanych z danym procesem biznesowym.
Refundacja	Redystrybucja wydatków do jednostek wewnątrz przedsiębiorstwa, w których powstały. Uwaga na temat zakresu: Refundacja jest ważna, ponieważ bez takiej polityki może powstać nieprawdziwy obraz rzeczywistej rentowności produktu lub usługi wynikający ze zignorowania określonych kluczowych wydatków bądź obliczenia ich na podstawie arbitralnej formuły.

TERMIN	DEFINICJA
Metodyka COBIT	1. COBIT 5: Wcześniej posługiwano się pełną nazwą: Control Objectives for Information and related Technology [Cele kontrolne dotyczące informacji i powiązanych technologii] (COBIT); obecnie w użyciu jest tylko akronim (w piątej iteracji metodyki). Kompletna, powszechnie uznawana metodyka w zakresie nadzoru nad technologiami informatycznymi (IT) w przedsiębiorstwie oraz zarządzania nimi, ułatwiająca kadrze kierowniczej i zarządowi definiowanie i realizację celów biznesowych oraz powiązanych celów IT. W ramach metodyki COBIT opisano pięć zasad i siedem czynników umożliwiających, które ułatwiają przedsiębiorstwom rozwój, wdrażanie, ciągłe doskonalenie i monitorowanie dobrych praktyk nadzoru i zarządzania związanych z IT. Uwaga dotycząca zakresu: Wcześniejsze wersje metodyki COBIT skupiały się na celach kontrolnych związanych z procesami IT, na zarządzaniu procesami IT oraz ich kontroli, a także na aspektach nadzoru nad IT. Przyjęcie i wykorzystywanie metodyki COBIT opiera się na wytycznych zawartych w coraz liczniejszej rodzinie produktów zapewniających wsparcie. (Więcej informacji można znaleźć na stronie *www.isaca.org/cobit*.) 2. COBIT 4.1 i wcześniejsze metodyki: Wcześniej posługiwano się pełną nazwą: Control Objectives for Information and related Technology (COBIT). Kompletna, powszechnie uznawana struktura procesów w zakresie IT, która ułatwia kadrze kierowniczej (w ramach funkcji biznesowej oraz IT) oraz zarządowi definiowanie i realizację celów biznesowych oraz powiązanych celów IT, zapewniając kompleksowy model nadzoru nad IT, zarządzania, kontroli i audytu. W metodyce COBIT opisano procesy IT oraz powiązane cele kontrolne, wytyczne dotyczące zarządzania (działania, zakresy odpowiedzialności i rozliczalności oraz mierniki sprawności), a także modele dojrzałości. COBIT ułatwia kadrze kierowniczej przedsiębiorstwa rozwój, wdrażanie, ciągłe doskonalenie oraz monitorowanie dobrych praktyk związanych z IT. Uwaga dotycząca zakresu: Przyjęcie i wykorzystanie metodyki COBIT jest wspierane przez wytyczne dla kadry kierowniczej i zarządu (*Board Briefing on IT Governance, 2nd Edition*), osób odpowiedzialnych za wdrożenie nadzoru nad IT (*COBIT Quickstart, 2nd Edition; IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition*; *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance*) oraz specjalistów ds. audytu i zapewnienia kontroli IT (*IT Assurance Guide Using COBIT*). Istnieją również wytyczne wspierające możliwość wykorzystania tej metodyki w odniesieniu do określonych wymogów prawnych i regulacyjnych (np. *IT Control Objectives for Sarbanes-Oxley, IT Control Objectives for Basel II*) oraz jej zastosowania w przypadku bezpieczeństwa informacji (*COBIT Security Baseline*). Metodyka COBIT została zestawiona z innymi metodykami i standardami w celu zilustrowania pełnego uwzględnienia cyklu życia zarządzania technologiami informatycznymi i wsparcia dla jej wykorzystania w przedsiębiorstwach korzystających z różnych metodyk i norm związanych z IT.
Kodeks etyki	Dokument, który opracowano z myślą o wywarciu wpływu na zachowanie pracowników oraz organizacji poprzez zdefiniowanie wartości organizacyjnych oraz reguł, które będą stosowane w określonych sytuacjach. Przyjmuje się go z myślą o ułatwieniu osobom odpowiedzialnym za podejmowanie decyzji w przedsiębiorstwie zrozumienia różnicy między właściwym i niewłaściwym postępowaniem oraz stosowania tej wiedzy podczas podejmowania decyzji.
Kompetencja	Zdolność do wykonania z powodzeniem konkretnego zadania, czynności lub do pełnienia funkcji.
Strona konsultowana (RACI)	Odnosi się do osób, u których zasięga się opinii na temat danego działania (komunikacja dwukierunkowa). W tabeli RACI odpowiada na pytanie: **Kto zapewnia dane wejściowe?** Kluczowe role zapewniające dane wejściowe. Należy zauważyć, że zadaniem osób odpowiedzialnych lub rozliczanych jest również uzyskanie informacji od innych jednostek lub partnerów zewnętrznych; powinny one jednak uwzględnić dane wejściowe pochodzące od wymienionych stron konsultowanych i, jeśli będzie to wymagane, podjąć właściwe działania związane z eskalacją, w tym poinformować właściciela procesu i/lub komitet sterujący.

TERMIN	DEFINICJA
Kontekst	Ogólny zbiór czynników wewnętrznych i zewnętrznych, które mogą wpłynąć na sposób działania przedsiębiorstwa, jednostki, procesu lub osób. Uwaga na temat zakresu: Kontekst obejmuje: • Kontekst technologiczny — czynniki technologiczne, które wpływają na zdolność organizacji do uzyskania wartości z danych • Kontekst danych — dokładność, dostępność, aktualność i jakość danych • Umiejętność i wiedzę — ogólne doświadczenie oraz umiejętności analityczne, techniczne i biznesowe • Kontekst organizacyjny i kulturowy — czynniki polityczne oraz ustalenie, czy organizacja woli polegać na danych zamiast na intuicji • Kontekst strategiczny — strategiczne cele przedsiębiorstwa
Kontrola	Metody zarządzania ryzykiem, w tym polityki, procedury, wytyczne, praktyki lub struktury organizacyjne, które mogą mieć charakter administracyjny, techniczny, zarządczy lub prawny. Termin używany również jako synonim mechanizmu ochrony lub środka zaradczego.
Kultura	Wzorzec zachowań, poglądów, założeń, postaw i sposobów działania.
Wyznacznik	Czynniki zewnętrzne i wewnętrzne, które inicjują i wpływają na sposób funkcjonowania przedsiębiorstwa lub osób bądź dokonywania przez nie zmian.
Cel przedsiębiorstwa	Zob. Cel biznesowy
Ład korporacyjny	Zbiór obowiązków i praktyk zarządu i kadry zarządzającej, których celem jest zapewnienie strategicznych wytycznych i dopilnowanie, aby osiągnięto wyznaczone cele, właściwie zarządzano ryzykiem i sprawdzono, czy zasoby przedsiębiorstwa są wykorzystywane w sposób odpowiedzialny. Termin może również oznaczać obraz nadzoru skupiający się na całościowych aspektach działania przedsiębiorstwa; najwyższego poziomu obraz nadzoru, do którego należy dostosować pozostałe aspekty.
Pełny cykl życia ekonomicznego	Okres, w którym oczekuje się istotnych korzyści biznesowych i/lub istotnych wydatków (obejmuje to inwestycje, koszty eksploatacji i wycofania) w ramach programu inwestycyjnego.
Dobra praktyka	Sprawdzone działanie lub proces, który jest z powodzeniem wykorzystywany w wielu przedsiębiorstwach i który, jak wykazano, umożliwia uzyskanie wiarygodnych wyników.
Nadzór	Dzięki nadzorowi zyskuje się pewność, że oceniono potrzeby, warunki i opcje interesariuszy w celu ustalenia zrównoważonych, uzgodnionych celów przedsiębiorstwa, które mają zostać osiągnięte. Nadzór polega również na ukierunkowaniu działań poprzez nadanie priorytetów i podejmowanie decyzji, a także na monitorowaniu sprawności i zgodności w odniesieniu do uzgodnionego kierunku i szczegółowych celów.
Praktyka nadzoru/zarządzania	W odniesieniu do każdego procesu w ramach metodyki COBIT praktyki nadzoru i zarządzania zapewniają kompletny zbiór ogólnych wymogów dotyczących skutecznego i praktycznego nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi. Stanowią one deklaracje dotyczące działań ze strony organów nadzorujących i zarządczych.
Czynnik umożliwiający nadzór	Coś (materialnego lub niematerialnego), co wspiera sprawowanie skutecznego nadzoru.
Metodyka nadzoru	Metodyka to podstawowa struktura koncepcyjna wykorzystywana do rozwiązywania lub uwzględniania złożonych problemów; czynnik umożliwiający nadzór; zbiór pojęć, założeń i praktyk definiujący sposób podejścia do danej kwestii lub jej rozumienia, relacje między zaangażowanymi jednostkami, role zaangażowanych stron, oraz ograniczenia (co obejmuje system nadzoru, a czego nie). Przykłady: *Internal Control — Integrated Framework* [Kontrola wewnętrzna — zintegrowana struktura ramowa] COBIT i COSO
Nadzór nad technologiami informatycznymi w przedsiębiorstwie	Obraz nadzoru, dzięki któremu zyskuje się pewność, że informacje (i powiązana technologia) wspierają i umożliwiają realizację strategii przedsiębiorstwa oraz osiągnięcie celów przedsiębiorstwa. Obejmuje to również nadzór funkcjonalny nad technologiami informatycznymi, tj. zapewnianie skutecznych i wydajnych zdolności w zakresie IT.

TERMIN	DEFINICJA
Informacje	Zasób, który (tak jak inne ważne aktywa biznesowe) jest niezbędny do prowadzenia działalności w przedsiębiorstwie. Informacje mogą istnieć w wielu postaciach (drukowanej, papierowej lub elektronicznej) i mogą być przesyłane pocztą, drogą elektroniczną, pokazywane w formie filmu lub przekazywane podczas rozmowy.
Strona informowana (RACI)	Odnosi się do osób, które otrzymują aktualne dane dotyczące postępów w realizacji działań (komunikacja jednokierunkowa). W tabeli RACI odpowiada na pytanie: **Kto otrzymuje informacje?** Role informowane o osiągnięciach i/lub efektach realizacji zadania. Oczywiście rola „rozliczana" powinna zawsze otrzymywać odpowiednie informacje, tak aby mogła nadzorować realizację zadania — tak jak role odpowiedzialne za dany obszar.
Dane wejściowe i wyniki	Produkty działań/pozostałości związane z procesem, uznane za niezbędne do wspierania realizacji procesu. Umożliwiają podejmowanie kluczowych decyzji, zapewniają rejestr oraz ścieżkę rewizyjną dla działań w ramach procesu i pozwalają na weryfikację w przypadku wystąpienia incydentu. Definiuje się je na poziomie kluczowych praktyk zarządzania; mogą one obejmować niektóre produkty działań wykorzystywane tylko w ramach procesów i stanowią często niezbędne dane wejściowe dla innych procesów. Lista przykładowych danych wejściowych i wyników COBIT 5 nie jest wyczerpująca, ponieważ określone środowisko i struktury procesów w przedsiębiorstwie mogą wymagać zdefiniowania dodatkowych przepływów informacji.
Portfel inwestycyjny	Zbiór rozważanych i/lub realizowanych inwestycji.
Aplikacja IT	Funkcjonalność elektroniczna stanowiąca część procesów biznesowych podejmowanych przez dział IT lub z jego pomocą.
Cel IT	Deklaracja opisująca pożądany wynik IT w przedsiębiorstwie wspierający realizację celów przedsiębiorstwa. Wynikiem może być pozostałość, istotna zmiana stanu lub istotna poprawa potencjału.
Usługi IT	Codzienne zapewnianie klientom infrastruktury i aplikacji IT oraz wsparcia przy korzystaniu z nich. Przykładem może być jednostka Service Desk, dostarczanie i przemieszczanie sprzętu oraz autoryzacja w zakresie bezpieczeństwa.
Zarządzanie	Zarządzanie polega na planowaniu, budowaniu, realizacji i monitorowaniu działań w sposób spójny z kierunkiem wskazanym przez organ nadzorujący, aby osiągnąć cele przedsiębiorstwa.
Model	Sposób opisania danego zbioru komponentów oraz ich wzajemnych relacji w celu opisania podstawowego sposobu działania obiektu, systemu lub koncepcji.
Miernik	Wymierna jednostka umożliwiająca pomiar osiągnięcia celu procesu. Mierniki powinny spełniać kryteria SMART — muszą być specyficzne, wymierne, składające się z konkretnych działań, istotne i terminowe. W pełnych wytycznych dotyczących miernika definiuje się wykorzystywaną jednostkę, częstotliwość pomiaru, idealną wartość docelową (w odpowiednich przypadkach) oraz procedurę przeprowadzania pomiaru, a także procedurę interpretacji wyniku oceny.
Cel	Deklaracja dotycząca pożądanego wyniku.
Struktura organizacyjna	Czynnik umożliwiający w odniesieniu do nadzoru i zarządzania. Obejmuje przedsiębiorstwo i jego struktury, hierarchie oraz zależności. Przykład: Komitet sterujący
Wynik	Zob. Dane wejściowe i wyniki
Właściciel	Osoba lub grupa otrzymująca lub posiadająca prawa i obowiązki związane z przedsiębiorstwem, jednostką lub zasobem, np. właściciel procesu, właściciel systemu.
Polityka	Ogólne zamierzenia i wytyczne formalnie wyrażone przez kierownictwo.

TERMIN	DEFINICJA
Zasada	Czynnik umożliwiający w odniesieniu do nadzoru i zarządzania. Obejmuje wartości i podstawowe założenia przedsiębiorstwa oraz poglądy, które określają (i ograniczają) sposób podejmowania decyzji i komunikowania się w ramach przedsiębiorstwa i poza nim, a także dozór — troskę o zasoby będące cudzą własnością. Przykład: Karta etyki, karta odpowiedzialności społecznej
Proces	Zasadniczo jest to zbiór praktyk ukierunkowanych przez polityki i procedury przedsiębiorstwa oraz wykorzystujących dane wejściowe z różnych źródeł (również z innych procesów), przetwarzających je i dostarczających wyniki (np. produkty, usługi). Uwaga na temat zakresu: Istnieją jasne przesłanki biznesowe dla realizacji procesów, określa się rozliczanych właścicieli, jasne role i zakresy odpowiedzialności związane z realizacją procesu oraz środki pomiaru sprawności.
Atrybut (potencjału) procesu	ISO/IEC 15504: Mierzalna cecha potencjału procesu odnosząca się do każdego procesu.
Potencjał procesu	ISO/IEC 15504: Charakterystyka zdolności do osiągnięcia aktualnych lub projektowanych celów biznesowych w wyniku realizacji procesu.
Cel procesu	Deklaracja opisująca pożądany wynik procesu. Wynikiem może być pozostałość, istotna zmiana stanu lub istotna poprawa potencjału innych procesów.
Biuro zarządzania projektami i programami (PMO)	Funkcja odpowiedzialna za wspieranie kierowników programów i projektów oraz za gromadzenie, ocenę i raportowanie informacji dotyczących realizacji programów oraz projektów wchodzących w ich skład.
Jakość	Przydatność dla danego celu (uzyskanie zamierzonej wartości).
Tabela RACI	Określa osoby odpowiedzialne, rozliczane, konsultowane oraz informowane w ramach struktury organizacyjnej.
Zasób	Każdy zasób przedsiębiorstwa, który ułatwia organizacji osiągnięcie jej celów.
Optymalizacja zasobów	Jeden z celów nadzoru. Obejmuje skuteczne, wydajne i odpowiedzialne wykorzystanie wszystkich zasobów — ludzkich, finansowych, sprzętu, infrastruktury itd.
Strona odpowiedzialna (RACI)	Odnosi się do osoby, która musi zadbać o skuteczną realizacje działań. W tabeli RACI odpowiada na pytanie: **Kto zajmuje się realizacją zadania?** Role w największym stopniu zaangażowane operacyjnie w wykonywanie wymienionych działań i uzyskiwanie zamierzonych wyników.
Ryzyko	Połączenie prawdopodobieństwa zdarzenia i jego konsekwencji (ISO/IEC 73).
Zarządzanie ryzykiem	Jeden z celów nadzoru. Wiąże się z rozpoznawaniem ryzyka, oszacowaniem wpływu i prawdopodobieństwa takiego ryzyka oraz opracowaniem strategii, takich jak unikanie ryzyka, ograniczanie negatywnego wpływu ryzyka i/lub transfer ryzyka oraz zarządzanie nim w kontekście apetytu na ryzyko w przedsiębiorstwie.
Katalog usług	Ustrukturyzowane informacje dotyczące wszystkich usług IT dostępnych dla klientów
Usługi	Zob. Usługi IT
Umiejętność	Wyuczona zdolność do osiągania wcześniej określonych rezultatów.
Interesariusz	Każda osoba, na której spoczywa odpowiedzialność za przedsiębiorstwo, mająca wobec niego oczekiwania lub jakiś udział w przedsiębiorstwie, np. udziałowcy, użytkownicy, rząd, dostawcy, klienci oraz opinia publiczna.
System kontroli wewnętrznej	Polityki, standardy, plany i procedury oraz struktury organizacyjne stworzone z myślą o racjonalnym zapewnieniu realizacji celów przedsiębiorstwa oraz uniknięciu niepożądanych zdarzeń lub ich wykryciu i skorygowaniu.
Tworzenie wartości	Główny cel nadzoru w przedsiębiorstwie, który osiąga się po zapewnieniu równowagi między trzema podstawowymi celami (realizacja korzyści, optymalizacja ryzyka i optymalizacja zasobów).

Strona celowo pozostawiona pusta