ISACA®
Trust in, and value from, information systems

COBIT® 5

กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

COBIT® 5
AN ISACA® FRAMEWORK

ISACA®
ด้วยหน่วยงานภาคพื้นกว่า 95,000 แห่งใน 160 ประเทศ สมาคมไอซาก้า *(ISACA) (www.isaca.org)* เป็นหนึ่งในผู้นำระดับสากลในด้านการให้ความรู้ การให้การรับรองด้วยวุฒิบัตร การสร้างชุมชน(ทางวิชาชีพ) การสนับสนุนและให้การศึกษาทางด้านการให้ความเชื่อมั่นและการรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ การกำกับดูแลและการบริหารจัดการองค์กรในด้านไอที รวมทั้งความเสี่ยงและการปฏิบัติตามกฎระเบียบข้อบังคับที่เกี่ยวข้องกับไอที สมาคมจัดตั้งขึ้นในปีค.ศ. 1969 โดยเป็นองค์กรอิสระที่ไม่แสวงหากำไร จัดการประชุมสัมมนา (เชิงวิชาการ) ในระดับสากล ตีพิมพ์วารสาร *ISACA® Journal* และจัดทำมาตรฐานสากลสำหรับการตรวจสอบและควบคุมระบบสารสนเทศ ซึ่งช่วยให้หน่วยงานภาคพื้นต่างๆ ของสมาคมมั่นใจได้ถึงความเชื่อมั่นและการสร้างคุณค่าจากระบบสารสนเทศ ทั้งยังช่วยสร้างความก้าวหน้าและให้การรับรองทักษะและความรู้ด้านไอทีผ่านทางการให้วุฒิบัตรที่ได้รับการยอมรับกันทั่วโลก ได้แก่ Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) และ Certified in Risk and Information Systems Control™ (CRISC™) สมาคม ISACA ยังคงดำเนินการปรับปรุง COBIT® ให้เป็นปัจจุบันอยู่อย่างต่อเนื่อง ซึ่งช่วยให้ผู้ประกอบวิชาชีพทางด้านไอทีและผู้นำในองค์กรสามารถรับผิดชอบการกำกับดูแลและการบริหารจัดการด้านไอที โดยเฉพาะในด้านการให้ความเชื่อมั่น การรักษาความมั่นคงปลอดภัย ความเสี่ยงและการควบคุม ตลอดจนการส่งมอบคุณค่าให้แก่ธุรกิจ

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

คำแถลงด้านคุณภาพ
เอกสารฉบับนี้แปลเอกสาร COBIT® 5 ฉบับภาษาอังกฤษให้เป็นภาษาไทยโดยสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพฯ ผู้ได้รับอนุญาตจาก ISACA® ซึ่งสมาคมฯ เป็นผู้รับผิดชอบแต่ผู้เดียวในความถูกต้องและความเชื่อถือได้ของการแปล

Disclaimer
ISACA has designed this publication, COBIT® 5 (the 'Work'), primarily as an educational resource 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 or test, readers should apply their own professional judgement to the specific GEIT, assurance, risk and security circumstances presented by the particular systems or information technology environment.

คำสงวนสิทธิ์
ISACA ได้ออกแบบ COBIT® 5 (เอกสารฉบับนี้) โดยมีวัตถุประสงค์หลักเพื่อเป็นแหล่งความรู้สำหรับผู้ประกอบวิชาชีพทางด้านการกำกับดูแลไอทีระดับองค์กร (governance of enterprise IT - GEIT) การให้ความเชื่อมั่น ความเสี่ยง และการรักษาความมั่นคงปลอดภัย ISACA ไม่ได้อ้างว่าการใช้ข้อมูลใดๆ ในเอกสารฉบับนี้จะสามารถรับรองผลสำเร็จ ผู้อ่านไม่ควรถือว่าเอกสารฉบับนี้รวมข้อมูล ขั้นตอนการปฏิบัติงาน และการทดสอบที่จำเป็นทั้งหมดเอาไว้ และไม่ควรพิจารณาข้อมูลในเอกสารฉบับนี้แยกต่างหากโดยไม่คำนึงถึงข้อมูล ขั้นตอนการปฏิบัติงาน และการทดสอบอื่นๆ ที่พอจะสามารถให้ผลลัพธ์ที่เหมือนกันได้ ในการพิจารณาถึงความเหมาะสมของข้อมูล ขั้นตอนการปฏิบัติงาน หรือการทดสอบใดๆ ผู้อ่านควรใช้วิจารณญาณด้านวิชาชีพของตนเพื่อพิจารณาถึงการกำกับดูแลไอทีในระดับองค์กร การให้ความเชื่อมั่น ความเสี่ยง และการรักษาความมั่นคงปลอดภัย ในสภาพแวดล้อมของระบบหรือเทคโนโลยีสารสนเทศนั้นๆ

COBIT® 5
ISBN 978-1-60420-446-9
จัดพิมพ์ในประเทศสหรัฐอเมริกา

คณะผู้แปล ผู้สอบทาน และผู้จัดทำ

สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพฯ
- คุณสุวัฒน์ หลายเจริญทรัพย์ CISM นายกสมาคมฯ
- คุณวรางคณา มุสิกะสังข์ CISA, CRISC อุปนายก
- คุณประทักษ์ วงศ์สินคงมั่น กรรมการ
- คุณวาสนา นริพทะพันธุ์ CISA กรรมการ
- คุณจันทร์เพ็ญ กสิกิจนำชัย CISA, CPA กรรมการ
- คุณสมชัย แพทย์วิบูลย์ CISA, CISSP, PMP, CFE, CIA, CSSLP กรรมการ
- คุณเสนีย์ วัชรศิริธรรม CISA, CRISC, CGEIT กรรมการ
- คุณณัฐชา เฉลิมชัยโกศล CISA, CISM, CISSP, ITIL Expert, ISO20000:2011 (LA), PRINCE2 กรรมการ
- คุณเสาวนีย์ เสตเสถียร เสถียร CISA, CRISC, PMP, AMBCI, ITIL V3, กรรมการ
- ดร.วิเชียร เปรมชัยสวัสดิ์ CISA กรรมการ
- คุณกุสล ปิ่นมุข CISA กรรมการ

อื่นๆ
- คุณสมบัติ ภูวเกียรติกำจร
- คุณณัฐ สิงหลกะ CISA
- คุณรัญชน์ โรจนพิเชฐ

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008
โทรศัพท์ (ประเทศสหรัฐอเมริกา): +1.847.253.1545
โทรสาร: +1.847.253.1443
อีเมล: *info@isaca.org*
เว็บไซต์: *www.isaca.org*

ให้คำติชม: *www.isaca.org/cobit*
เข้ามีส่วนร่วมในศูนย์ความรู้ (Knowledge Center) ของ ISACA: *www.isaca.org/knowledge-center*
ติดตาม ISACA ทางทวิตเตอร์: *https://twitter.com/ISACANews*
ร่วมสนทนาในหัวข้อ COBIT ทางทวิตเตอร์: #COBIT
ร่วมลิงค์อิน ISACA : ISACA (Official), *http://linkd.in/ISACAOfficial*
กดชอบ ISACA บนเฟสบุ๊ค: *www.facebook.com/ISACAHQ*

หน้านี้เป็นหน้าว่าง

กิตติกรรมประกาศ

ISACA ขอขอบคุณ:

คณะทำงาน COBIT 5 (2009–2011)
John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Business Services, USA, Co-chair Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., UK, Co-chair
Pippa G. Andrews, CISA, ACA, CIA, KPMG, Australia Elisabeth Judit Antonsson, CISM, Nordea Bank, Sweden Steven A. Babb, CGEIT, CRISC, Betfair, UK
Steven De Haes, Ph.D., University of Antwerp Management School, Belgium
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, USA Erik H.J.M. Pols, CISA, CISM, Shell International-ITCI, The Netherlands
Vernon Richard Poole, CISM, CGEIT, Sapphire, UK
Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq and Associates, India

ทีมผู้พัฒนา
Floris Ampe, CISA, CGEIT, CIA, ISO 27000, PwC, Belgium
Gert du Preez, CGEIT, PwC, Canada
Stefanie Grijp, PwC, Belgium
Gary Hardy, CGEIT, IT Winners, South Africa
Bart Peeters, PwC, Belgium
Geert Poels, Ghent University, Belgium
Dirk Steuperaert, CISA, CGEIT, CRISC, IT In Balance BVBA, Belgium

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

กิตติกรรมประกาศ (ต่อ)

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

กิตติกรรมประกาศ (ต่อ)

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

คณะกรรมการบริหารของ ISACA
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, International President Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., USA, Vice President
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (retired), USA, Past International President
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, UK, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Director

กิตติกรรมประกาศ (ต่อ)

คณะกรรมการบริหารด้านความรู้
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Chairman
Michael A. Berardi Jr., CISA, CGEIT, Bank of America, USA
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapore
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jon Singleton, CISA, FCA, Auditor General of Manitoba (retired), Canada
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France

คณะกรรมการด้านกรอบการดำเนินงาน (2009-2012)
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France, Chairman
Georges Ataya, CISA, CISM, CGEIT, CRISC, CISSP, Solvay Brussels School of Economics and Management, Belgium, Past Vice President
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Sergio Fleginsky, CISA, Akzo Nobel, Uruguay
John W. Lainhart, IV, CISA, CISM, CGEIT, CRISC, IBM Global Business Services, USA Mario C. Micallef, CGEIT, CPAA, FIA, Malta
Anthony P. Noble, CISA, CCP, Viacom, USA
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., UK
Robert G. Parker, CISA, CA, CMC, FCA, Deloitte & Touche LLP (retired), Canada
Rolf M. von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, Forfa AG, Switzerland
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia
Robert E. Stroud, CGEIT, CA Inc., USA

ขอบคุณเป็นพิเศษ
ISACA Los Angeles Chapter สำหรับการให้การสนับสนุนด้านการเงิน

พันธมิตรและผู้สนับสนุน ISACA และ IT Governance Institute® (ITGI®)
American Institute of Certified Public Accountants Commonwealth Association for Corporate Governance Inc. FIDA
Inform
Information Security Forum
Institute of Management Accountants Inc. ISACA chapters
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.

สารบัญ

สารบัญรูปภาพ 11

COBIT 5: กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูและการบริหารจัดการไอทีระดับองค์กร..... 13

บทสรุปสำหรับผู้บริหาร..... 15

บทที่ 1. ภาพรวมของ COBIT 5 17
ภาพรวมของเอกสารฉบับนี้..... 18

บทที่ 2. หลักการที่ 1: การตอบสนองต่อความต้องการของผู้มีส่วนได้เสีย..... 19
บทนำ..... 19
การส่งทอดเป้าหมายใน COBIT 5..... 19
ขั้นตอนที่ 1. ปัจจัยผลักดันผู้มีส่วนได้เสียมีอิทธิผลต่อความต้องการของผู้มีส่วนได้เสีย..... 19
ขั้นตอนที่ 2. ส่งทอดความต้องการของผู้มีส่วนได้เสียไปยังเป้าหมายระดับองค์กร..... 19
ขั้นตอนที่ 3. เป้าหมายระดับองค์กรส่งทอดไปยังเป้าหมายที่เกี่ยวข้องกับไอที..... 20
ขั้นตอนที่ 4. เป้าหมายที่เกี่ยวข้องกับไอทีส่งทอดไปยังเป้าหมายของปัจจัยเอื้อ..... 20
การใช้การส่งทอดเป้าหมายของ COBIT 5..... 22
ประโยชน์ของการส่งทอดเป้าหมายของ COBIT 5..... 22
การใช้การส่งทอดเป้าหมายของ COBIT 5 อย่างระมัดระวัง..... 22
การใช้การส่งทอดเป้าหมายของ COBIT 5 ในทางปฏิบัติ..... 22
คำถามเกี่ยวกับการกำกับดูแลและการบริหารจัดการด้านไอที..... 23
เราจะหาคำตอบสำหรับคำถามเหล่านี้ได้อย่างไร..... 24

บทที่ 3. หลักการที่ 2: ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร...... 25
วิธีปฏิบัติสำหรับการกำกับดูแล..... 25
ปัจจัยเอื้อเพื่อการกำกับดูแล 26
ขอบเขตของการกำกับดูแล..... 26
บทบาท กิจกรรม และความสัมพันธ์..... 26

บทที่ 4. หลักการที่ 3: ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว..... 27
COBIT 5 เป็นที่รวบรวมกรอบการดำเนินงานต่างๆ 27

บทที่ 5. หลักการที่ 4: เอื้อให้วิธีปฏิบัติแบบองค์รวมส่งผลสัมฤทธิ์ผล..... 29
ปัจจัยเอื้อของ COBIT 5 29
การกำกับดูแลและการบริหารจัดการอย่างเป็นระบบด้วยปัจจัยเอื้อที่เชื่อมต่อถึงกัน..... 29
มิติต่างๆ ของปัจจัยเอื้อใน COBIT5..... 30
มิติต่างๆ ของปัจจัยเอื้อ..... 30
การบริหารจัดการประสิทธิภาพของปัจจัยเอื้อ 31
ตัวอย่างของปัจจัยเอื้อในทางปฏิบัติ..... 32

บทที่ 6. หลักการที่ 5: ความแตกต่างระหว่างการกำกับดูแลและการบริหารจัดการ..... 33
การกำกับดูแลและการบริหารจัดการ..... 33
ความสัมพันธ์ระหว่างการกำกับดูแลและการบริหารจัดการ..... 33
ต้นแบบอ้างอิงของกระบวนการใน COBIT 5..... 34

บทที่ 7. แนวทางในการนำไปใช้งาน 37
บทนำ..... 37
ข้อควรพิจารณาในบริบทขององค์กร..... 37
การสร้างสภาพแวดล้อมที่เหมาะสม 38
การรับรู้จุดที่มีปัญหาและเหตุการณ์จุดชนวน 38
การเอื้อให้เกิดการเปลี่ยนแปลง 39
วิธีปฏิบัติแบบวัฏจักร..... 40
เริ่มต้น: สร้างเหตุผลทางธุรกิจ..... 41

บทที่ 8. ต้นแบบความสามารถของกระบวนการใน COBIT 5 43
บทนำ..... 43
ความแตกต่างระหว่างต้นแบบวุฒิภาวะใน COBIT4.1และต้นแบบวุฒิภาวะของกระบวรการใน COBIT 5..... 43
แนวปฏิบัติที่แตกต่างกัน..... 45
ประโยชน์จากการเปลี่ยนแปลง..... 47
ดำเนินการประเมินความสามารถของกระบวนการตาม COBIT 5..... 47

ภาคผนวก A. ข้อมูลอ้างอิง..... 49

ภาคผนวก B. รายละเอียดความสัมพันธ์ระหว่างเป้าหมายระดับองค์กร กับเป้าหมายที่เกี่ยวข้องกับไอที..... 51

ภาคผนวก C. รายละเอียดความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอที และกระบวนการที่เกี่ยวข้องกับไอที..... 53

ภาคผนวก D. ความต้องการของผู้มีส่วนได้เสียและเป้าหมายระดับองค์กร..... 57
ภาคผนวก E. การเทียบ COBIT 5 กับมาตรฐาน/กรอบการดำเนินงานอื่นที่เกี่ยวข้อง และเกี่ยวเนื่องกันมากที่สุด..... 59
บทนำ..... 59
COBIT 5 และ ISO/IEC 38500..... 59
หลักการของ ISO/IEC 38500..... 59
ISO/IEC 38500 ประเมิน สั่งการ และเฝ้าติดตาม..... 62
การเปรียบเทียบกับมาตรฐานอื่นๆ 62
ITIL® V3 2011 และ ISO/IEC 20000..... 63
ชุดของ ISO/IEC 27000..... 63
ชุด ISO/IEC 31000..... 63
TOGAF®..... 63
Capability Maturity Model Integration (CMMI) (development)..... 63
PRINCE2®..... 63

ภาคผนวก F. การเปรียบเทียบระหว่างต้นแบบสารสนเทศใน COBIT 5 กับเกณฑ์คุณสมบัติของสารสนเทศใน COBIT 4.1..... 65

ภาคผนวก G. คำอธิบายอย่างละเอียดของปัจจัยเอื้อใน COBIT 5..... 67
บทนำ..... 67
มิติต่างๆ ของปัจจัยเอื้อ..... 67
การบริหารจัดการประสิทธิภาพของปัจจัยเอื้อ..... 68
ปัจจัยเอื้อใน COBIT 5: หลักการ นโยบาย และกรอบการดำเนินงาน..... 69
ปัจจัยเอื้อใน COBIT 5: กระบวนการ..... 71
การบริหารจัดการประสิทธิภาพของการดำเนินงานของปัจจัยเอื้อ..... 73
ตัวอย่างในเชิงปฏิบัติของปัจจัยเอื้อด้านกระบวนการ..... 73
ต้นแบบอ้างอิงของกระบวนการใน COBIT 5..... 73
ปัจจัยเอื้อใน COBIT 5: โครงสร้างการจัดองค์กร..... 77
ปัจจัยเอื้อใน COBIT 5: วัฒนธรรม จริยธรรม และพฤติกรรม..... 81
ปัจจัยเอื้อใน COBIT 5: สารสนเทศ..... 83
บทนำ—วัฏจักรของสารสนเทศ..... 83
ปัจจัยเอื้อด้านสารสนเทศของ COBIT 5..... 83
ปัจจัยเอื้อใน COBIT 5: บริการ โครงสร้างพื้นฐาน และระบบงาน..... 89
ปัจจัยเอื้อใน COBIT 5: บุคลากร ทักษะ และศักยภาพ..... 91

ภาคผนวก H. อภิธานศัพท์..... 93

สารบัญรูปภาพ

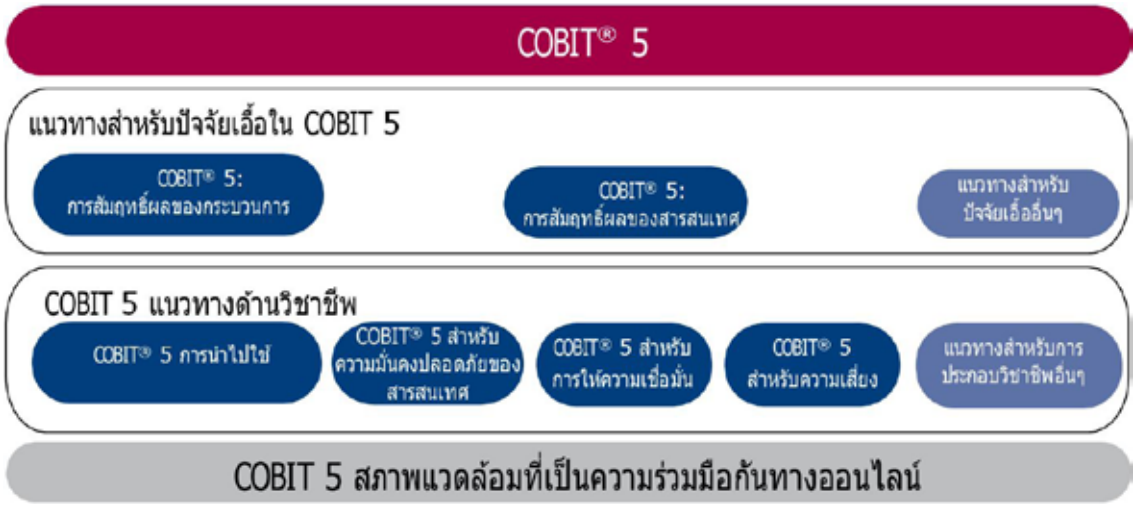
รูปภาพที่ 1—ชุดผลิตภัณฑ์ของ COBIT 5 13
รูปภาพที่ 2—หลักการของ COBIT 5 15
รูปภาพที่ 3—วัตถุประสงค์ในการกำกับดูแล: การสร้างคุณค่า 19
รูปภาพที่ 4—ภาพรวมของการส่งทอดเป้าหมายใน COBIT 5 20
รูปภาพที่ 5—เป้าหมายระดับองค์กรของ COBIT 5 21
รูปภาพที่ 6—เป้าหมายที่เกี่ยวข้องกับไอที 21
รูปภาพที่ 7—คำถามเกี่ยวกับการกำกับดูแลและการบริหารจัดการไอที 24
รูปภาพที่ 8—การกำกับดูแลและการบริหารจัดการ COBIT 5 25
รูปภาพที่ 9—บทบาทหน้าที่ กิจกรรม และความสัมพันธ์ที่สำคัญ 26
รูปภาพที่ 10—กรอบการดำเนินงานที่รวมกันเป็นหนึ่งเดียวของ COBIT 5 27
รูปภาพที่ 11—ชุดผลิตภัณฑ์ของ COBIT 5 28
รูปภาพที่ 12—ปัจจัยเอื้อขององค์กรใน COBIT 5 29
รูปภาพที่ 13—ปัจจัยเอื้อทั่วไปใน COBIT 5 30
รูปภาพที่ 14—COBIT 5 ความสัมพันธ์ระหว่าง การกำกับดูแลและการบริหารจัดการ 33
รูปภาพที่ 15—จุดสำคัญในการกำกับดูแลและการบริหารจัดการของ COBIT 5 34
รูปภาพที่ 16—ต้นแบบอ้างอิงของกระบวนการใน COBIT 5 35
รูปภาพที่ 17—วัฏจักรการนำไปใช้ 7 ระยะ 40
รูปภาพที่ 18—สรุปต้นแบบวุฒิภาวะใน COBIT 4.1 43
รูปภาพที่ 19—สรุปต้นแบบวุฒิภาวะของกระบวนการใน COBIT 5 44
รูปภาพที่ 20—ตารางเปรียบเทียบระดับวุฒิภาวะ (COBIT 4.1)
และระดับความสามารถของกระบวนการ (COBIT 5) 46
รูปภาพที่ 21—ตารางเปรียบเทียบคุณลักษณะของวุฒิภาวะ (COBIT 4.1)
และคุณลักษณะของกระบวนการ (COBIT 5) 47
รูปภาพที่ 22—ความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรใน COBIT 5 กับเป้าหมายที่เกี่ยวข้องกับไอที 52
รูปภาพที่ 23—ความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีกับกระบวนการต่างๆ ใน COBIT 5 54
รูปภาพที่ 24—ความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรของ COBIT 5 กับคำถามของผู้บริหาร 57
รูปภาพที่ 25—ความสัมพันธ์ระหว่าง COBIT 5 กับมาตรฐานและกรอบการดำเนินงานอื่นๆ 64
รูปภาพที่ 26—COBIT 5 ที่เทียบได้กับเกณฑ์คุณสมบัติของสารสนเทศใน COBIT 4.1 65
รูปภาพที่ 27—ปัจจัยเอื้อทั่วไปใน COBIT 5 67
รูปภาพที่ 28—ปัจจัยเอื้อใน COBIT 5: หลักการ นโยบาย และกรอบการดำเนินงาน 69
รูปภาพที่ 29—ปัจจัยเอื้อใน COBIT 5: กระบวนการ 71
รูปภาพที่ 30—จุดสำคัญในการกำกับดูแลและการบริหารจัดการของ COBIT 5 75
รูปภาพที่ 31—ต้นแบบอ้างอิงของกระบวนการใน COBIT 5 76
รูปภาพที่ 32—ปัจจัยเอื้อใน COBIT 5: โครงสร้างการจัดองค์กร 77
รูปภาพที่ 33—บทบาทหน้าที่และโครงสร้างการจัดองค์กรของ COBIT 5 78
รูปภาพที่ 34—ปัจจัยเอื้อใน COBIT 5: วัฒนธรรม จริยธรรม และพฤติกรรม 81
รูปภาพที่ 35—ข้อมูลคำนิยามของข้อมูลใน COBIT 5—วัฏจักรของสารสนเทศ 83
รูปภาพที่ 36—ปัจจัยเอื้อใน COBIT 5: สารสนเทศ 83
รูปภาพที่ 37—ปัจจัยเอื้อใน COBIT 5: บริการ โครงสร้างพื้นฐาน และระบบงาน 89
รูปภาพที่ 38—ปัจจัยเอื้อใน COBIT 5: บุคลากร ทักษะ และศักยภาพ 91
รูปภาพที่ 39—ประเภทของทักษะใน COBIT 5 92

หน้านี้เป็นหน้าว่าง

COBIT 5: กรอบการดำเนินงานสำหรับ การกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

เอกสาร COBIT 5 บรรจุเนื้อหาที่เป็นกรอบการดำเนินงานของ COBIT 5 ที่ใช้สำหรับการกับดูแลและการบริหารจัดการไอทีระดับองค์กร เอกสารฉบับนี้เป็นหนึ่งในชุดผลิตภัณฑ์ของ COBIT 5 ดังที่แสดงไว้ใน **รูปภาพที่ 1**

รูปภาพที่ 1—ชุดผลิตภัณฑ์ของ COBIT 5



กรอบการดำเนินงานของ COBIT 5 จัดทำขึ้นบนหลักการ 5 ประการซึ่งจะได้กล่าวถึงในรายละเอียดต่อไป และรวมถึงแนวทางที่ครอบคลุมของปัจจัยเอื้อ (Enablers) สำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

ชุดผลิตภัณฑ์ COBIT 5 มีผลิตภัณฑ์ต่างๆ ดังต่อไปนี้

- COBIT 5 (กรอบดำเนินงาน (framework))
- COBIT 5 แนวทางสำหรับปัจจัยเอื้อ (Enabler Guide) ซึ่งอธิบายในรายละเอียดถึงปัจจัยเอื้อด้านการกำกับดูแลและการบริหารจัดการ อันประกอบด้วย
  - COBIT 5: การสัมฤทธิ์ผลของกระบวนการ (Enabling processes)
  - COBIT 5: การสัมฤทธิ์ผลของสารสนเทศ (Enabling Information)
  - แนวทางของปัจจัยเอื้อ (Enabler guide) อื่นๆ (ตรวจสอบได้ใน *www.isaca.org/cobit*)
- COBIT 5 แนวทางด้านวิชาชีพ(Professional guides) ประกอบด้วย
  - COBIT 5 การนำไปใช้งาน (implementation)
  - COBIT 5 สำหรับความมั่นคงปลอดภัยของสารสนเทศ (for information security)
  - COBIT 5 สำหรับการให้ความเชื่อมั่น (for Assurance)
  - COBIT 5 สำหรับความเสี่ยง (for Risk)
  - แนวทางด้านวิชาชีพอื่นๆ (ตรวจสอบได้ใน *www.isaca.org/cobit*)
- สภาพแวดล้อมที่เป็นความร่วมมือกันทางออนไลน์ ซึ่งจะจัดให้มีขึ้นในอนาคตเพื่อสนับสนุนการใช้ COBIT 5

หน้านี้เป็นหน้าว่าง

บทสรุปสำหรับผู้บริหาร

สารสนเทศเป็นทรัพยากรหลักสำหรับทุกองค์กร และเทคโนโลยีมีบทบาทอย่างเป็นนัยสำคัญตั้งแต่ได้จัดทำขึ้นจนถึงเวลาที่ทำลายทิ้ง เทคโนโลยีสารสนเทศก้าวหน้าขึ้นเรื่อยๆ และใช้กันอย่างแพร่หลายในองค์กร ตลอดจนในสภาพแวดล้อมทางสังคม สาธารณะ และธุรกิจ

ด้วยเหตุนี้ ในปัจจุบันจึงยิ่งทำให้องค์กรและผู้บริหารระดับสูงต่างๆ ต้องเรียกร้องให้มี
- การดูแลรักษาสารสนเทศให้ได้คุณภาพสูง เพื่อใช้สนับสนุนการตัดสินใจ
- สร้างคุณค่าทางธุรกิจจากการลงทุนโดยมีไอทีเป็นปัจจัยเอื้อ ได้แก่ การใช้งานไอทีอย่างประสิทธิผลและสร้างสรรค์เพื่อให้บรรลุเป้าหมายทางกลยุทธ์และก่อให้เกิดประโยชน์ทางธุรกิจ
- บรรลุการปฏิบัติงานที่เป็นเลิศ ผ่านการใช้งานเทคโนโลยีที่เชื่อถือได้และมีประสิทธิผล
- ดูแลความเสี่ยงที่เกี่ยวกับไอที ให้อยู่ในระดับที่ยอมรับได้
- ดูแลต้นทุนของการให้บริการทางไอทีและต้นทุนทางเทคโนโลยีให้เกิดประโยชน์สูงสุด
- ปฏิบัติตามกฎหมาย กฎระเบียบข้อบังคับ ข้อตกลงตามสัญญา และนโยบายที่เกี่ยวข้อง

ในทศวรรษที่ผ่านมา คำว่า 'การกำกับดูแล (Governance)' ได้กลายมาเป็นความคิดของธุรกิจในระดับแนวหน้า ที่แสดงให้เห็นถึงความสำคัญของการกำกับดูแลที่ดี และในทางกลับกันก็สะท้อนให้เห็นถึงความล้มเหลวของธุรกิจอันเกิดจากการละเลยการกำกับดูแล

องค์กรที่ประสบความสำเร็จได้ตระหนักดีว่าคณะกรรมการบริหารและผู้บริหารระดับสูงจำเป็นต้องยอมรับการนำไอทีมาใช้เสมือนกับส่วนอื่นๆ ที่มีนัยสำคัญในการดำเนินธุรกิจ ในการดำเนินธุรกิจ คณะกรรมการบริหารและผู้บริหาร—ทั้งหน้าที่งานทางด้านธุรกิจและไอที—จึงต้องร่วมมือและทำงานร่วมกันเพื่อให้ไอทีได้รวมอยู่ในวิธีปฏิบัติด้านการกำกับดูแลและการบริหารจัดการ นอกจากนี้ ยังมีการออกกฎหมายใหม่ๆ และกฎข้อบังคับที่นำมาใช้เพิ่มขึ้นอย่างต่อเนื่องเพื่อจัดการกับความจำเป็นดังกล่าว

COBIT 5 ให้กรอบการดำเนินงานที่ครอบคลุม เพื่อช่วยให้องค์กรบรรลุวัตถุประสงค์ในเรื่องการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร กล่าวง่ายๆ ก็คือ ช่วยองค์กรสร้างคุณค่าที่เกิดประโยชน์สูงสุดจากไอที โดยการรักษาความสมดุลระหว่างประโยชน์ที่จะได้รับ กับระดับความเสี่ยงและการใช้ทรัพยากรที่ทำให้เกิดประโยชน์สูงสุด COBIT 5 เอื้อให้ไอทีได้รับการกำกับดูแลและบริหารจัดการในแบบองค์รวมสำหรับทั่วทั้งองค์กร โดยครอบคลุมหน้าที่งานตามความรับผิดชอบทั้งทางด้านธุรกิจและไอทีอย่างครบวงจร พิจารณาถึงผลประโยชน์ที่เกี่ยวข้องกับไอทีของผู้มีส่วนได้เสียทั้งภายในและภายนอก COBIT 5 สามารถใช้ได้ทั่วไปและใช้ประโยชน์ได้สำหรับองค์กรทุกขนาด ไม่ว่าจะเป็นองค์กรการค้า องค์กรที่ไม่แสวงหากำไร หรือในภาคเอกชน

รูปภาพที่ 2—หลักการของ COBIT 5

COBIT 5 ตั้งอยู่บนพื้นฐานของหลักการสำคัญ 5 ประการ (ดูใน**รูปภาพที่ 2**) ในการกำกับดูแลและการบริหารจัดการไอที ระดับองค์กร:

- **หลักการที่ 1: ตอบสนองความต้องการของผู้มีส่วนได้เสีย**—องค์กรตั้งอยู่เพื่อที่สร้างคุณค่าสำหรับผู้มีส่วนได้เสีย โดยการรักษาความสมดุลระหว่างผลประโยชน์ที่จะได้รับกับความเสี่ยงและการใช้ทรัพยากรที่ทำให้เกิดประโยชน์สูงสุด COBIT 5 ให้กระบวนการที่จำเป็นทั้งหมดและปัจจัยเอื้ออื่นๆ ที่ใช้สนับสนุนการสร้างคุณค่าแก่ธุรกิจจากการใช้ไอที เพราะว่าทุกองค์กรมีวัตถุประสงค์ที่แตกต่างกัน องค์กรสามารถปรับแต่ง COBIT 5 ให้เหมาะกับบริบทของตนผ่านทางการส่งทอดเป้าหมาย (goal cascade) การแปลงเป้าหมายองค์กรในภาพรวมไปสู่เป้าหมายในระดับที่สามารถบริหารจัดการได้ มีความเฉพาะเจาะจง มีความเกี่ยวข้องกับไอที และการเชื่อมโยงหรือเทียบเป้าหมายนี้กับกระบวนการหรือแนวปฏิบัติหนึ่งๆ
- **หลักการที่ 2: ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร**—COBIT 5 บูรณาการการกำกับดูแลไอทีระดับองค์กรเข้าไปในการกำกับดูแลองค์กร:
  - ครอบคลุมทุกหน้าที่งานและกระบวนการภายในองค์กร COBIT 5 ไม่เน้นเพียงแค่ 'หน้าที่งานด้านไอที' เท่านั้น แต่จะถือว่าสารสนเทศและเทคโนโลยีที่เกี่ยวข้องเป็นสินทรัพย์ที่ทุกคนในองค์กรจำเป็นต้องดูแลเช่นเดียวกับสินทรัพย์อื่นๆ
  - **พิจารณาการกำกับดูแลและการบริหารจัดการปัจจัยเอื้อที่เกี่ยวข้องกับไอทีทั้งหมด เพื่อให้ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร ได้แก่การรวมทุกคนและทุกสิ่ง ทั้งภายในและภายนอก ที่เกี่ยวข้องกับการกำกับดูแลและการบริหารจัดการสารสนเทศและไอทีที่เกี่ยวข้อง**
- **หลักการที่ 3: ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว**—มีมาตรฐานและแนวปฏิบัติที่ดีที่เกี่ยวข้องกับไอทีจำนวนมาก ซึ่งแต่ละอย่างก็ให้แนวทางเกี่ยวกับกิจกรรมของไอทีในด้านใดด้านหนึ่ง COBIT 5 ได้นำมาตรฐานและกรอบการดำเนินงานที่เกี่ยวข้องอื่นๆ มาจัดให้สอดคล้องกันในภาพรวม จึงสามารถใช้เป็นกรอบการดำเนินงานที่ครอบอยู่เหนือกรอบการดำเนินงานอื่นๆ สำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร
- **หลักการที่ 4: เอื้อให้วิธีปฏิบัติแบบองค์รวมส่งผลทธิ์ผล** —การกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่มีประสิทธิภาพและประสิทธิผลต้องใช้วิธีปฏิบัติแบบองค์รวมที่ได้พิจารณาถึงองค์ประกอบหลายๆ อย่างซึ่งมีปฏิสัมพันธ์ต่อกัน COBIT 5 ระบุถึงกลุ่มของปัจจัยเอื้อที่ใช้สนับสนุนการนำระบบการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรไปใช้งานอย่างครอบคลุม ปัจจัยเอื้อนิยามได้อย่างกว้างๆ ว่าเป็นสิ่งที่สามารถช่วยในการบรรลุวัตถุประสงค์ขององค์กร กรอบการดำเนินงานของ COBIT 5 ระบุถึงปัจจัยเอื้อ 7 ประเภทดังนี้
  - หลักการ นโยบาย และกรอบการดำเนินงาน
  - กระบวนการ
  - โครงสร้างการจัดองค์กร
  - วัฒนธรรม จริยธรรม และพฤติกรรม
  - สารสนเทศ
  - บริการ โครงสร้างพื้นฐาน และระบบงาน
  - บุคลากร ทักษะ และศักยภาพ
- **หลักการที่ 5: แบ่งแยกการกำกับดูแลออกจากการบริหารจัดการ**—กรอบการดำเนินงานของ COBIT 5 ระบุความแตกต่างอย่างชัดเจนระหว่างการกำกับดูแลและการบริหารจัดการ หลักสองประการนี้ครอบคลุมถึงกิจกรรมที่ต่างกัน ต้องการโครงสร้างการจัดองค์กรที่แตกต่างกัน และใช้เพื่อจุดประสงค์ที่แตกต่างกัน ในมุมมองของ COBIT 5 ความแตกต่างหลักๆ ที่เห็นเด่นชัดระหว่างการกำกับดูแลและการบริหารจัดการคือ:

  – การกำกับดูแล (Governance)

  การกำกับดูแล ทำให้มั่นใจได้ว่า ความต้องการ เงื่อนไข และทางเลือกของผู้มีส่วนได้เสียได้รับการประเมินเพื่อกำหนดวัตถุประสงค์ที่องค์กรต้องการให้บรรลุซึ่งมีความสมดุลและเห็นชอบร่วมกัน; การกำหนดทิศทางผ่านการจัดลำดับความสำคัญและการตัดสินใจ; และการเฝ้าติดตามผลการดำเนินงานและการปฏิบัติตามเทียบกับทิศทางและวัตถุประสงค์ที่ได้ตกลงร่วมกัน

  ในองค์กรส่วนใหญ่ คณะกรรมการบริหารเป็นผู้รับผิดชอบการกำกับดูแลโดยรวมภายใต้การชี้นำของประธานกรรมการ ในองค์กรขนาดใหญ่และมีความซับซ้อน หน้าที่บางประการสำหรับการกำกับดูแลอาจมอบหมายให้กับหน่วยงานที่จัดตั้งขึ้นเป็นพิเศษในระดับที่เหมาะสม

  – การบริหารจัดการ (Management)

  ผู้บริหารวางแผน สร้าง ดำเนินงาน และเฝ้าติดตามกิจกรรมต่างๆ ให้สอดคล้องกับทิศทางที่กำหนดโดยหน่วยงานกำกับดูแล (governance body) เพื่อให้บรรลุวัตถุประสงค์ขององค์กร

  ในองค์กรส่วนใหญ่ การบริหารจัดการรับผิดชอบโดยผู้บริหารระดับสูงภายใต้การชี้นำของประธานเจ้าหน้าที่บริหาร (CEO)

เมื่อนำหลักการทั้ง 5 ประการนี้มารวมกันจะทำให้องค์กรสามารถสร้างกรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการที่มีประสิทธิผล ซึ่งส่งผลให้การใช้สารสนเทศและการลงทุนด้านเทคโนโลยีเกิดประโยชน์สูงสุด เพื่อยังประโยชน์ให้กับผู้มีส่วนได้เสีย

บทที่ 1
ภาพรวมของ COBIT 5

COBIT 5 ให้แนวทางสำหรับยุคถัดไปของสมาคม ISACA ในเรื่องการกำกับดูแลและการบริหารจัดการองค์กรทางด้านไอทีที่โดยจัดทำขึ้นจากประสบการณ์ที่มีการนำ COBIT ไปใช้งานจริงมากกว่า 15 ปี และมีการนำไปประยุกต์ใช้โดยองค์กรมากมาย รวมทั้งผู้ใช้ต่างๆ จากกลุ่มธุรกิจ กลุ่มไอที กลุ่มบริหารความเสี่ยง กลุ่มผู้รักษาความมั่นคงปลอดภัย และกลุ่มให้ความเชื่อมั่น (assurance) ปัจจัยขับเคลื่อนหลักในการพัฒนา COBIT 5 เกิดจากความต้องการที่จะ

- ให้ผู้มีส่วนได้เสียได้มีส่วนมากขึ้นในการกำหนดสิ่งที่คาดหวังจากสารสนเทศและเทคโนโลยีที่เกี่ยวข้อง (ประโยชน์ที่ได้รับ ณ ระดับความเสี่ยงที่ยอมรับได้ และด้วยต้นทุนที่จะเกิดขึ้น) และลำดับสำคัญของแต่ละสิ่งเหล่านั้น เพื่อให้มั่นใจว่า คุณค่าที่คาดหวังนั้นจะได้รับการส่งมอบจริง ผู้มีส่วนได้เสียบางคนอาจต้องการผลประโยชน์ในระยะสั้น บางคนต้องการความยั่งยืนในระยะยาว บางคนพร้อมที่จะรับความเสี่ยงสูง แต่บางคนอาจไม่สามารถยอมรับความเสียงได้เลย ความคาดหวังที่แตกต่างกันเหล่านี้ (ซึ่งบางครั้งก็ขัดแย้งกัน) ต้องได้รับการจัดการอย่างมีประสิทธิผล นอกจากนี้ผู้มีส่วนได้เสียเหล่านี้ยังไม่เพียงต้องการมีส่วนร่วมมากขึ้นเท่านั้น แต่พวกเขาต้องการความโปร่งใสด้วยว่า สิ่งเหล่านี้จะเกิดขึ้นได้อย่างไร และจะบรรลุผลลัพธ์จริงได้อย่างไร
- ระบุถึงความสำเร็จขององค์กรที่ต้องพึ่งพากลุ่มธุรกิจและองค์กรด้านไอทีจากภายนอกมากขึ้นเรื่อยๆ เช่น ผู้ให้บริการภายนอก ผู้ขาย ที่ปรึกษา ลูกค้า ผู้ให้บริการแบบกลุ่มเมฆ (Cloud) และอื่นๆ ตลอดจนวิธีการและกลไกต่างๆ ที่ใช้เป็นการภายในเพื่อส่งมอบคุณค่าตามที่คาดหวัง
- รับมือกับปริมาณสารสนเทศที่มีแนวโน้มเพิ่มขึ้นอย่างมีนัยสำคัญ องค์กรจะเลือกสารสนเทศที่มีความเกี่ยวข้องและน่าเชื่อถือซึ่งจะนำไปสู่การตัดสินใจที่มีประสิทธิภาพและประสิทธิผลได้อย่างไร สารสนเทศเองก็จำเป็นต้องได้รับการบริหารจัดการอย่างมีประสิทธิผลซึ่งการมีต้นแบบสารสนเทศที่มีประสิทธิผลสามารถช่วยได้
- รับมือกับไอทีที่กำลังแพร่หลายมากขึ้น ไอทีได้บูรณาการเป็นส่วนหนึ่งของธุรกิจมากขึ้นเรื่อยๆ บ่อยครั้งที่เกิดความไม่พอใจหากแยกไอทีออกมาต่างหากแม้ว่าไอทีจะยังสอดคล้องกับธุรกิจก็ตาม ไอทีจำเป็นต้องบูรณาการให้เป็นส่วนหนึ่งของโครงการทางธุรกิจ โครงสร้างการจัดองค์กร การบริหารความเสี่ยง นโยบาย ทักษะ กระบวนการ และอื่นๆ บทบาทของผู้บริหารสูงสุดด้านสารสนเทศ (CIO) และหน้าที่งานด้านไอทีกำลังค่อยๆ วิวัฒนาการไปจากเดิม บุคลากรในหน่วยงานธุรกิจมีทักษะด้านไอทีมากขึ้นและมีส่วนร่วมหรือกำลังจะมีส่วนร่วมในการตัดสินใจและการปฏิบัติการด้านไอทีมากขึ้น ไอทีจะต้องบูรณาการให้เข้ากับธุรกิจมากขึ้น
- ให้แนวทางเพิ่มเติมในเรื่องนวัตกรรมและเทคโนโลยีที่ออกมาใหม่ซึ่งเป็นเรื่องของความคิดสร้างสรรค์ การประดิษฐ์คิดค้นการพัฒนาผลิตภัณฑ์ใหม่ๆ การทำให้ผลิตภัณฑ์ที่มีอยู่ให้เป็นที่สนใจของลูกค้าและดึงดูดลูกค้าประเภทใหม่ๆ นวัตกรรมอาจหมายถึงการปรับปรุงกระบวนการให้มีประสิทธิภาพมากขึ้นทั้งในเรื่องของการพัฒนาผลิตภัณฑ์การผลิตและห่วงโซ่อุปทาน (supply chain) เพื่อนำสินค้าสู่ตลาดด้วยความมีประสิทธิภาพ รวดเร็ว และมีคุณภาพในระดับที่สูงขึ้น
- ครอบคลุมความรับผิดชอบในหน้าที่งานทั้งทางธุรกิจและด้านไอทีอย่างครบวงจรและครอบคลุมทุกแง่มุมที่จะนำไปสู่การกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรอย่างมีประสิทธิผล เช่น โครงสร้างการจัดองค์กร นโยบาย และวัฒนธรรมนอกเหนือจากกระบวนการ
- มีการควบคุมที่ดีขึ้นสำหรับกระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จด้านไอที (IT Solution) ที่ผู้ใช้เป็นผู้ริเริ่มหรือที่อยู่ในความควบคุมของผู้ใช้
- องค์กรบรรลุถึง:
  - การสร้างคุณค่าผ่านทางการใช้ไอทีระดับองค์กรอย่างมีประสิทธิผลและสร้างสรรค์
  - ความพึงพอใจของผู้ใช้ทางธุรกิจ กับการทำงานและบริการด้านไอที
  - ปฏิบัติตามกฎหมาย กฎระเบียบข้อบังคับ ข้อกำหนดตามสัญญา และนโยบายภายในที่เกี่ยวข้อง
  - ความเชื่อมโยงที่ดีขึ้นระหว่างความต้องการทางธุรกิจกับวัตถุประสงค์ด้านไอที
- เชื่อมโยงและหากเป็นไปได้ ทำให้เกิดความสอดคล้องกับกรอบการดำเนินงานและมาตรฐานอื่นๆ ที่มีใช้กันอยู่ เช่น Information Technology Infrastructure Library (ITIL®),The Open Group Architecture Forum (TOGAF®), Project Management Body of Knowledge (PMBOK®), PRojects IN Controlled Environments 2 (PRINCE2®), Committee of Sponsoring Organizations of the Treadway Commission (COSO) และ the International Organization for Standardization (ISO) ซึ่งจะช่วยให้ผู้มีส่วนได้เสียเข้าใจถึงกรอบการดำเนินงาน แนวปฏิบัติที่ดี และมาตรฐานต่างๆ เหล่านี้ว่าใช้สำหรับจุดใดและใช้ร่วมกันได้อย่างไร
- บูรณาการกรอบการดำเนินงานและแนวทางที่สำคัญของ ISACA ทั้งหมด โดยเน้นที่ COBIT Val IT และ Risk IT แต่ยังคงพิจารณาถึงต้นแบบทางธุรกิจสำหรับความมั่นคงปลอดภัยของสารสนเทศ (Business Model for Information Security - BMIS) กรอบการดำเนินงานสำหรับความเชื่อมั่นในไอที (IT Assurance Framework-ITAF) เอกสารชื่อว่า *บทสรุปสำหรับคณะกรรมการบริหารเพื่อการกำกับดูแลไอที (Board Briefing on IT Governance)* และเอกสารที่ชื่อว่า Taking governance forward (TGF) ดังนั้น COBIT 5 จึงครอบคลุมทั่วทั้งองค์กรและให้พื้นฐานในการบูรณาการกรอบการดำเนินงานมาตรฐานและแนวปฏิบัติอื่นๆ มารวมกันเป็นกรอบการดำเนินงานเพียงหนึ่งเดียว

ผลิตภัณฑ์และแนวทางอื่นๆ ที่ครอบคลุมความต้องการที่หลากหลายของผู้มีส่วนได้เสียต่างๆ จะสร้างขึ้นจากองค์ความรู้หลักของ COBIT 5 โดยจะค่อยๆ จัดทำเพิ่มเติมขึ้นอีกไปเรื่อยๆ ซึ่งจะทำให้สถาปัตยกรรมใน COBIT 5 มีการปรับปรุงเพิ่มเติมอยู่เสมอ ท่านสามารถหาข้อมูลล่าสุดเกี่ยวกับสถาปัตยกรรมของผลิตภัณฑ์ใน COBIT 5 ได้บน ISACA เว็บไซต์ (*www.isaca.org/cobit)*

ภาพรวมของเอกสารฉบับนี้

กรอบการดำเนินงานของ COBIT 5 บรรจุเนื้อหาไว้ในอีก 7 บทดังนี้:

- บทที่ 2 อธิบายหลักการที่ 1 คือ **การตอบสนองความต้องการของผู้มีส่วนได้เสีย** บทนี้จะเกริ่นนำถึงการส่งทอดเป้าหมาย (goals cascade) ของ COBIT 5 เป้าหมายระดับองค์กรด้านไอทีได้นำมาใช้เพื่อจัดระเบียบและโครงสร้างให้กับความต้องการของผู้มีส่วนได้เสีย เป้าหมายระดับองค์กรสามารถเชื่อมโยงไปสู่เป้าหมายที่เกี่ยวข้องกับไอที และเป้าหมายเกี่ยวข้องกับไอทีจะสามารถบรรลุได้โดยการนำปัจจัยเอื้อทั้งหมด ซึ่งรวมถึงกระบวนการต่างๆ ไปใช้และดำเนินการให้เกิดประโยชน์สูงสุดเป้าหมายต่างๆ ที่เชื่อมโยงกันเหล่านี้เรียกว่า การส่งทอดเป้าหมาย (goals cascade) ใน COBIT 5 ในบทนี้ยังให้ตัวอย่างของคำถามด้านการกำกับดูแลและการบริหารจัดการที่ผู้มีส่วนได้เสียมักมีข้อสงสัยเกี่ยวกับไอทีระดับองค์กร
- บทที่ 3 อธิบายหลักการที่ 2 คือ **ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร** บทนี้อธิบายว่า COBIT 5 บูรณาการการกำกับดูแลไอทีระดับองค์กรเข้ากับการกำกับดูแลองค์กร โดยครอบคลุมหน้าที่งานและกระบวนการทั้งหมดภายในองค์กรได้อย่างไร
- บทที่ 4 อธิบายหลักการที่ 3 **ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว** และอธิบายโดยสรุปเกี่ยวกับการบูรณาการภายใต้สถาปัตยกรรมของ COBIT 5
- บทที่ 5 อธิบายหลักการที่ 4 **เอื้อให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผล** การกำกับดูแลไอทีระดับองค์กรเป็นการทำงานอย่างเป็นระบบและสนับสนุนโดยปัจจัยเอื้อต่างๆ ในบทนี้ได้เกริ่นนำถึงปัจจัยเอื้อและนำเสนอวิธีที่มักใช้กันทั่วไปในการพิจารณาถึงปัจจัยเอื้อด้วยการใช้ต้นแบบปัจจัยเอื้อทั่วไป (generic enabler model)
- บทที่ 6 อธิบายหลักการที่ 5 **การแบ่งแยกการกำกับดูแลออกจากการบริหารจัดการ** และอธิบายถึงความแตกต่างระหว่างการบริหารจัดการและการกำกับดูแล และความสัมพันธ์ระหว่างกัน ภาพรวมของต้นแบบอ้างอิงของกระบวนการ (process reference model) ของ COBIT 5 ได้รวมไว้ในบทนี้เพื่อเป็นตัวอย่าง
- บทที่ 7 ได้เกริ่นนำถึง **แนวทางการนำไปใช้งาน** ซึ่งอธิบายว่า เราสามารถสร้างสภาพแวดล้อมที่เหมาะสมขึ้นมาได้อย่างไร อธิบายถึงปัจจัยเอื้อที่ต้องการ จุดที่มีปัญหา (pain point) และเหตุการณ์จุดชนวน (trigger event) สำหรับการนำไปใช้งาน วัฏจักรของการนำไปใช้งานและการปรับปรุงอย่างต่อเนื่อง ในบทนี้จะอิงกับเอกสารชื่อว่า*การนำ COBIT® 5 ไปใช้งาน (COBIT® 5 Implementation)* ที่มีรายละเอียดอย่างครบถ้วนเกี่ยวกับวิธีการนำการกำกับดูแลไอทีระดับองค์กรไปใช้โดยอิงกับ COBIT 5
- บทที่ 8 อธิบายถึง **ต้นแบบระดับความสามารถของกระบวนการ (process capability model) ของ COBIT 5** ที่มีอยู่ในแบบแผนวิธีปฏิบัติในการประเมินชุดโครงการ (assessment programe approach scheme) (*www.isaca.org/cobit-assessment-programme*) และชี้แจงถึงความแตกต่างจากการประเมินวุฒิภาวะของกระบวนการใน COBIT 4.1 (COBIT4.1 process maturity assessment) และผู้ใช้จะเปลี่ยนไปใช้วิธีปฏิบัติใหม่ได้อย่าง

ในภาคผนวกประกอบด้วยข้อมูลอ้างอิงการแสดงความสัมพันธ์และการเปรียบเทียบ และรายละเอียดเพิ่มเติมในบางหัวข้อ

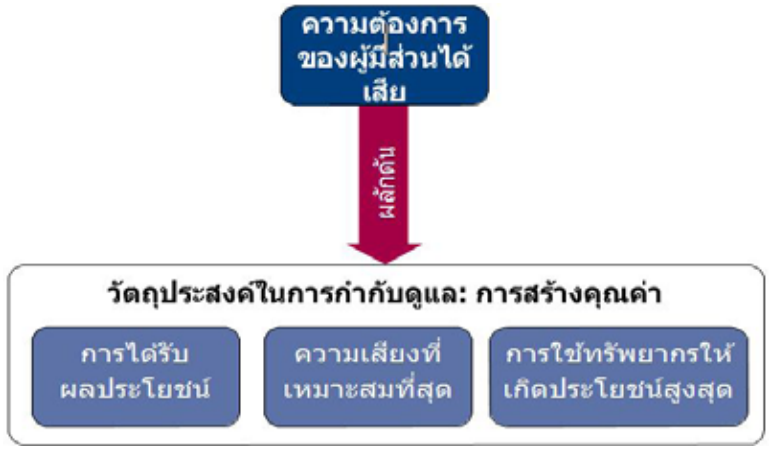
- ภาคผนวก A. **ข้อมูลอ้างอิง**ที่นำมาใช้ในระหว่างการจัดทำ COBIT 5 ได้นำมาแสดงไว้ในภาคผนวกนี้
- ภาคผนวก B. **รายละเอียดความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรกับเป้าหมายที่เกี่ยวข้องกับไอที** อธิบายว่าเป้าหมายระดับองค์กรในแต่ละข้อ สนับสนุนโดยเป้าหมายที่เกี่ยวข้องกับไอทีข้อใดบ้าง
- ภาคผนวก C**. รายละเอียดความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีและกระบวนการที่เกี่ยวข้องกับไอที** กับกระบวนการที่เกี่ยวข้องกับไอทีอธิบายว่ากระบวนการต่างๆ ใน COBIT สนับสนุนการบรรลุถึงเป้าหมายที่เกี่ยวข้องกับไอทีได้อย่างไร
- ภาคผนวก D. **ความต้องการของผู้มีส่วนได้เสียและเป้าหมายระดับองค์กร** อธิบายว่า ความต้องการของผู้มีส่วนได้เสียเกี่ยวข้องกับเป้าหมายระดับองค์กรใน COBIT 5 อย่างไร
- ภาคผนวก E. **การเทียบ COBIT 5 กับมาตรฐาน/กรอบการดำเนินงานอื่นที่เกี่ยวข้องและเกี่ยวเนื่องกันมากที่สุด**
- ภาคผนวก F. **การเปรียบเทียบระหว่างต้นแบบสารสนเทศใน COBIT 5 กับเกณฑ์คุณสมบัติของสารสนเทศใน COBIT 4.1**
- ภาคผนวก G. **คำอธิบายอย่างละเอียดของปัจจัยเอื้อใน COBIT 5** จากบทที่ 5 และรวมถึงรายละเอียดเพิ่มเติมของปัจจัยเอื้อต่างๆ รวมถึงรายละเอียดของต้นแบบปัจจัยเอื้อ (enabler model) ที่อธิบายถึงองค์ประกอบเฉพาะและแสดงตัวอย่างประกอบ
- ภาคผนวก H. **อภิธานศัพท์**

บทที่ 2
หลักการที่ 1: การตอบสนองต่อความต้องการของผู้มีส่วนได้เสีย

บทนำ

องค์กรตั้งขึ้นเพื่อที่สร้างคุณค่าให้กับผู้มีส่วนได้เสีย ดังนั้นองค์กรไม่ว่าจะเป็นองค์กรการค้าหรือไม่แสวงหาผลกำไรก็จะต้องมีการสร้างคุณค่าเป็นหนึ่งในวัตถุประสงค์ของการกำกับดูแล การสร้างคุณค่าหมายถึง การได้รับผลประโยชน์ด้วยต้นทุนทรัพยากรที่ให้ประโยชน์สูงสุดและความเสี่ยงที่เหมาะสมที่สุด (ดู**รูปภาพ**ที่ 3) ผลประโยชน์สามารถรับรู้ได้หลายรูปแบบ ยกตัวอย่างเช่น ด้านการเงินสำหรับองค์กรที่แสวงหาผลกำไร หรือการบริการสาธารณะสำหรับหน่วยงานภาครัฐ

รูปภาพที่ 3—วัตถุประสงค์ในการกำกับดูแล: การสร้างคุณค่า



องค์กรมีผู้มีส่วนได้เสียหลายคน และคำว่า "สร้างคุณค่า" ก็มีความหมายที่แตกต่างกันไปและบางครั้งก็ขัดแย้งกัน การกำกับดูแลจึงเป็นการเจรจาต่อรองและตัดสินใจท่ามกลางความแตกต่างในผลประโยชน์ที่ของผู้มีส่วนได้เสียทั้งหลาย ด้วยเหตุนี้ระบบการกำกับดูแลจึงควรพิจารณาถึงผู้มีส่วนได้เสียทั้งหมดเมื่อจะตัดสินใจในการประเมินผลประโยชน์ ความเสี่ยงและทรัพยากร คำถามที่ควรถามในการตัดสินใจแต่ละครั้งคือ ใครเป็นผู้ได้รับประโยชน์ ใครเป็นผู้รับความเสี่ยง และต้องใช้ทรัพยากรอะไรบ้าง

การส่งทอดเป้าหมายของ COBIT 5

ทุกองค์กรดำเนินงานภายใต้บริบทที่ต่างกัน ซึ่งบริบทนี้กำหนดโดยทั้งปัจจัยภายนอก (ด้านการตลาด ประเภทธุรกิจ ภูมิศาสตร์การเมือง และอื่นๆ) และปัจจัยภายใน (วัฒนธรรม การจัดองค์กร การยอมรับความเสี่ยง และอื่นๆ) และจำเป็นต้องมีระบบการกำกับดูแลและการบริหารจัดการที่ปรับแต่งให้เหมาะสมเฉพาะสำหรับองค์กร

ความต้องการของผู้มีส่วนได้เสีย จะต้องถูกแปลงมาเป็นกลยุทธ์ขององค์กรที่สามารถดำเนินการได้ การส่งทอดเป้าหมายของ COBIT 5 เป็นกลไกในการแปลงความต้องการของผู้มีส่วนได้เสียมาเป็นเป้าหมายขององค์กร เป้าหมายที่เกี่ยวข้องกับไอทีและเป้าหมายของปัจจัยเอื้อที่ปรับแต่งให้เป็นเฉพาะตัวและสามารถนำไปปฏิบัติได้ การแปลงนี้ช่วยให้มีการกำหนดเป้าหมายที่เฉพาะเจาะจงลงไปในแต่ละระดับและในทุกด้านขององค์กรเพื่อสนับสนุนเป้าหมายและความต้องการของผู้มีส่วนได้เสียในภาพรวม และสนับสนุนให้เกิดความสอดคล้องกันระหว่างความต้องการขององค์กรกับกระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จและการให้บริการด้านไอที

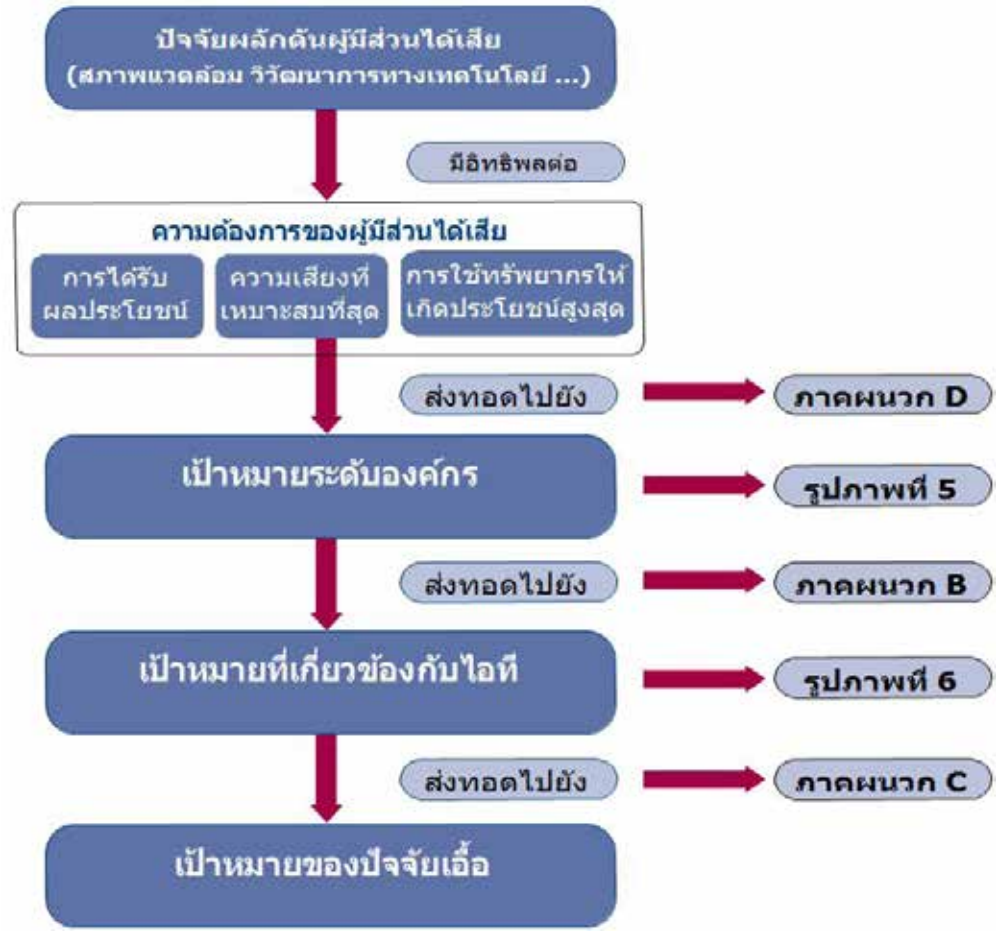
การส่งทอดเป้าหมายของ COBIT 5 แสดงไว้ใน **รูปภาพที่ 4**

ขั้นตอนที่ 1 ปัจจัยผลักดันผู้มีส่วนได้เสียมีอิทธิผลต่อความต้องการของผู้มีส่วนได้เสีย
ความต้องการของผู้มีส่วนได้เสียได้รับอิทธิพลจากปัจจัยผลักดันหลายอย่าง ยกตัวอย่างเช่น การเปลี่ยนแปลงกลยุทธ์ การเปลี่ยนแปลงสภาพแวดล้อมทางธุรกิจและกฎระเบียบในการควบคุม และเทคโนโลยีใหม่ๆ

ขั้นตอนที่ 2 ส่งทอดความต้องการของผู้มีส่วนได้เสียไปยังเป้าหมายระดับองค์กร
ความต้องการของผู้มีส่วนได้เสียสามารถเชื่อมโยงไปถึงเป้าหมายทั่วไปในระดับองค์กร (Generic enterprise goal) เป้าหมายระดับองค์กรเหล่านี้กำหนดขึ้นโดยใช้มิติต่างๆ ของการวัดผลแบบสมดุล (BSC)[1] และเป็นการแสดงรายการเป้าหมายที่มักใช้กันโดยทั่วไปซึ่งองค์กรสามารถนำมากำหนดใช้เป็นของตนได้ ถึงแม้ว่าเป้าหมายต่างๆ ที่มีอยู่ในรายการนี้จะไม่ใช้เป้าหมายทั้งหมด แต่เป้าหมายเฉพาะขององค์กรโดยส่วนใหญ่ก็สามารถเทียบได้ง่ายกับเป้าหมายทั่วไปในระดับองค์กรนี้ ตารางแสดงความสัมพันธ์ระหว่างความต้องการของผู้มีส่วนได้เสียกับเป้าหมายระดับองค์กรแสดงไว้ในภาคผนวก D

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

รูปภาพที่ 4—ภาพรวมของการส่งทอดเป้าหมายใน COBIT 5



COBIT 5 กำหนดเป้าหมายทั่วไปไว้ 17 ข้อ ดังที่แสดงไว้ใน**รูปภาพ**ที่ 5 ซึ่งประกอบด้วย
- มิติของการวัดผลแบบสมดุล (BSC) ที่เหมาะสมกับเป้าหมายระดับองค์กร
- เป้าหมายระดับองค์กร
- ความสัมพันธ์กับวัตถุประสงค์หลักของการกำกับดูแล 3 ประการ คือ การได้รับผลประโยชน์ ความเสี่ยงในระดับที่เหมาะสม และการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด (P หมายถึง ความสัมพันธ์หลัก และ S หมายถึง ความสัมพันธ์รอง หรือมีความสัมพันธ์กันน้อย)

ขั้นตอนที่ 3 เป้าหมายระดับองค์กรส่งทอดไปยังเป้าหมายที่เกี่ยวข้องกับไอที
การบรรลุซึ่งเป้าหมายระดับองค์กรจำเป็นต้องมีผลลัพธ์[2] ที่เกี่ยวข้องกับไอทีจำนวนหนึ่ง ซึ่งได้แก่เป้าหมายที่เกี่ยวข้องกับไอที นั่นเอง คำว่าเกี่ยวข้องกับไอทีหมายถึงสารสนเทศและเทคโนโลยีที่เกี่ยวข้อง และเป้าหมายที่เกี่ยวข้องกับไอทีนี้ได้กำหนดขึ้นตามมิติของการวัดผลแบบสมดุลด้านไอที (IT BSC) COBIT 5 ได้กำหนดเป้าหมายที่เกี่ยวข้องกับไอทีไว้ 17 ข้อ ตาม**รูปภาพที่ 6**

ตารางแสดงความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีกับเป้าหมายระดับองค์กรได้แสดงไว้ในภาคผนวก B และยังแสดงให้เห็นด้วยว่าเป้าหมายระดับองค์กรแต่ละข้อสนับสนุนด้วยเป้าหมายที่เกี่ยวข้องกับไอทีข้อใดบ้าง

ขั้นตอนที่ 4 เป้าหมายที่เกี่ยวข้องกับไอทีส่งทอดไปยังเป้าหมายของปัจจัยเอื้อ
การบรรลุเป้าหมายเกี่ยวข้องกับไอทีจำเป็นต้องมีระบบงานที่ทำงานได้ดีและใช้ปัจจัยเอื้อจำนวนหนึ่ง แนวคิดของปัจจัยเอื้อได้อธิบายรายละเอียดไว้ในบทที่ 5 ปัจจัยเอื้อรวมถึงกระบวนการ โครงสร้างการจัดองค์กร และสารสนเทศ และได้มีการกำหนดเป้าหมายสำหรับปัจจัยเอื้อแต่ละประเภทที่จะสนับสนุนเป้าหมายที่เกี่ยวข้องกับไอที

กระบวนการเป็นหนึ่งในปัจจัยเอื้อ ในภาคผนวก C ได้แสดงความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีและกับกระบวนการของ COBIT 5 ที่เกี่ยวข้อง ซึ่งรวมถึงเป้าหมายของกระบวนการเหล่านั้นด้วย

[2] ไอทีย่อมไม่ใช่สิ่งเดียวเท่านั้นที่จำเป็นในการบรรลุเป้าหมายระดับองค์กร หน้าที่งานในด้านอื่นๆ ทั้งหมดภายในองค์กร เช่น การเงินและการตลาด ย่อมมีส่วนช่วยให้บรรลุเป้าหมายระดับองค์กรเช่นกัน แต่ในบริบทของ COBIT 5 จะพิจารณาเฉพาะเป้าหมายที่เกี่ยวข้องกับไอทีเท่านั้น

รูปภาพที่ 5—เป้าหมายระดับองค์กรของ COBIT 5				
มิติการวัดผลแบบสมดุล	เป้าหมายระดับองค์กร	ความเชื่อมโยงกับวัตถุประสงค์ในการกำกับดูแล		
		การได้รับผลประโยชน์	ความเสี่ยงที่เหมาะสม	ทรัพยากรที่ให้ประโยชน์สูงสุด
ด้านการเงิน	1. คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	P		S
	2. กลุ่ม (Portfolio)ของผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน	P	P	S
	3. ความเสี่ยงทางธุรกิจที่ได้รับการจัดการ (การปกป้องคุ้มครองสินทรัพย์)		P	S
	4. การปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับจากภายนอก		P	
	5. ความโปร่งใสทางการเงิน	P	S	S
ด้านลูกค้า	6. วัฒนธรรมที่เน้นการบริการลูกค้า	P		S
	7. บริการของธุรกิจมีความต่อเนื่องและความพร้อมให้บริการ		P	
	8. การตอบสนองอย่างฉับไวต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	P		S
	9. การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	P	P	P
	10. ต้นทุนในการส่งมอบบริการที่ให้ประโยชน์สูงสุด	P		P
ด้านกระบวนการภายใน	11. หน้าที่งานในกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	P		P
	12. ต้นทุนของกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	P		P
	13. ชุดโครงการเพื่อการเปลี่ยนแปลงทางธุรกิจที่ได้รับการบริหารจัดการ	P	P	S
	14. การปฏิบัติงานและบุคคลากรที่มีประสิทธิภาพ	P		P
	15. การปฏิบัติตามนโยบายภายในองค์กร		P	
ด้านการเรียนรู้และเติบโต	16. บุคคลากรที่มีทักษะและแรงจูงใจ	S	P	P
	17. วัฒนธรรมที่ส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ	P		

รูปภาพที่ 6—เป้าหมายที่เกี่ยวข้องกับไอที		
มิติการวัดผลแบบสมดุลด้านไอที	เป้าหมายของสารสนเทศและเทคโนโลยีที่เกี่ยวข้อง	
ด้านการเงิน	01	กลยุทธ์ด้านไอทีสอดคล้องไปในแนวทางเดียวกันกับกลยุทธ์ด้านธุรกิจ
	02	ไอทีเอื้ออำนวยและสนับสนุนให้ธุรกิจสามารถปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับของหน่วยงานภายนอก
	03	ผู้บริหารระดับสูงให้คำมั่นในการตัดสินใจต่างๆ ที่เกี่ยวข้องกับไอที
	04	ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้
	05	ประโยชน์ที่ได้รับจริงจากกลุ่มของการลงทุนและการให้บริการในด้านต่างๆ ที่มีไอทีเป็นปัจจัยเอื้อ
	06	ต้นทุน ประโยชน์ และความเสี่ยงทางด้านไอทีมีความโปร่งใส
ด้านลูกค้า	07	การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ
	08	การใช้ระบบงาน สารสนเทศและเทคโนโลยีอย่างเหมาะสม
ด้านกระบวนการภายใน	09	ความคล่องตัวทางด้านไอที
	10	ความมั่นคงปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน
	11	การใช้สินทรัพย์ ทรัพยากร และสมรรถนะทางด้านไอทีให้ได้ประโยชน์สูงสุด
	12	การเอื้ออำนวยและสนับสนุนการทำงานของกระบวนการทางธุรกิจโดยบูรณาการระบบงานและเทคโนโลยีเข้าไปใช้ในกระบวนการทางธุรกิจ
	13	การส่งมอบชุดโครงการต่างๆ ก่อให้เกิดประโยชน์ ตรงเวลา ตามงบประมาณที่ตั้งไว้ และตามความต้องการและมาตรฐานด้านคุณภาพ
	14	ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้ และมีประโยชน์ในการตัดสินใจ
	15	ไอทีที่ปฏิบัติตามนโยบายภายในขององค์กร
ด้านการเรียนรู้และเติบโต	16	บุคลากรทั้งทางด้านไอทีและด้านธุรกิจที่มีความสามารถและมีแรงจูงใจ
	17	ความรู้ ความเชี่ยวชาญ และการริเริ่มดำเนินการเพื่อนวัตกรรมทางธุรกิจ

การใช้การส่งทอดเป้าหมายของ COBIT 5

ประโยชน์ของการส่งทอดเป้าหมายของ COBIT 5

การส่งทอดเป้าหมาย[3] เป็นสิ่งสำคัญที่จะช่วยจัดลำดับความสำคัญในการนำไปใช้งาน การปรับปรุงให้ดีขึ้น และการให้ความเชื่อมั่นในการกำกับดูแลไอทีระดับองค์กร บนพื้นฐานของวัตถุประสงค์ (เชิงกลยุทธ์) ขององค์กรและความเสี่ยงที่เกี่ยวข้อง ในทางปฏิบัติการส่งทอดเป้าหมายจะรวมถึง

- กำหนดเป้าหมายและวัตถุประสงค์ที่เกี่ยวข้องและจับต้องได้ สำหรับหน้าที่ความรับผิดชอบในระดับต่างๆ
- กรองฐานความรู้ (Knowledge base) ของ COBIT 5 เฉพาะที่เกี่ยวข้องกับเป้าหมายในระดับองค์กร เพื่อคัดเฉพาะแนวทางที่เกี่ยวข้องไปใช้ในโครงการหนึ่งๆ ไม่ว่าจะเป็นโครงการเพื่อการนำไปใช้งาน(ระบบงานใหม่) เพื่อการปรับปรุงให้ดีขึ้น หรือเพื่อให้ความเชื่อมั่น
- ระบุและสื่อสาร (ในบางครั้งอาจเป็นในระดับปฏิบัติการ) อย่างชัดเจนว่า ปัจจัยเอื้อมีความสำคัญต่อการบรรลุเป้าหมายในระดับองค์กรอย่างไร

การใช้การส่งทอดเป้าหมายของ COBIT 5 อย่างระมัดระวัง

การส่งทอดเป้าหมาย รวมทั้งตารางแสดงความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรกับเป้าหมายที่เกี่ยวข้องกับไอที และระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีกับปัจจัยเอื้อของ COBIT 5 (รวมถึงกระบวนการต่างๆ) ไม่ได้เป็นคำตอบที่ครอบจักรวาล และผู้ใช้ไม่ควรพยายามที่จะนำไปใช้โดยไม่คำนึงถึงปัจจัยแวดล้อมอื่นๆ แต่ควรใช้เป็นเพียงแนวทางหนึ่งด้วย เหตุผลหลายประการ ได้แก่

- ทุกองค์กรมีการจัดลำดับความสำคัญของเป้าหมายที่แตกต่างกัน และลำดับความสำคัญนี้อาจจะเปลี่ยนแปลงไปตามเวลา
- ตารางแสดงความสัมพันธ์ไม่ได้แยกแยะขนาด และ/หรือ ประเภทธุรกิจขององค์กร แต่เป็นการแสดงให้เห็นว่า โดยทั่วไปแล้วเป้าหมายในระดับต่างๆ มีความสัมพันธ์ต่อกันอย่างไร
- ค่าบ่งชี้ต่างๆ ที่ระบุไว้ในตารางแสดงถึงระดับของความสำคัญหรือความสัมพันธ์ที่แบ่งเป็น 2 ระดับ ซึ่งชี้นำว่าเราสามารถ "แยกแยะ" ระดับทั้งสองได้อย่างชัดเจน แต่ในความเป็นจริงแล้ว ระดับความสัมพันธ์อาจเป็นค่าใดค่าหนึ่งที่อยู่ระหว่างช่วงของ 2 ระดับดังกล่าวก็ได้

การใช้การส่งทอดเป้าหมายของ COBIT 5 ในทางปฏิบัติ

จากเหตุผลที่กล่าวมาข้างต้น เห็นได้ชัดว่าในขั้นแรกของการใช้การส่งทอดเป้าหมายนี้ องค์กรควรปรับแต่งตารางความสัมพันธ์ให้สอดคล้องกับสถานการณ์เฉพาะหนึ่งๆ หรืออีกนัยหนึ่ง แต่ละองค์กรควรจัดทำการส่งทอดเป้าหมายที่เป็นลักษณะเฉพาะของตัวเองก่อน จากนั้นจึงนำมาเปรียบเทียบกับของ COBIT เพื่อปรับให้มีความสมบูรณ์มากขึ้น

ยกตัวอย่าง องค์กรอาจปรารถนาที่จะ

- แปลงลำดับความสำคัญของกลยุทธ์มาเป็นการให้น้ำหนักหรือให้ความสำคัญอย่างใดอย่างหนึ่งสำหรับเป้าหมายในระดับองค์กรแต่ละข้อ
- ตรวจสอบความสมเหตุสมผลของความสัมพันธ์ในการส่งทอดเป้าหมาย โดยพิจารณาถึงสภาพแวดล้อมหรือประเภทธุรกิจที่เป็นเรื่องเฉพาะของตน เป็นต้น

[3] การส่งทอดเป้าหมายมาจากงานวิจัยโดยมหาวิทยาลัยอันทเวิบ (University of Antwerp) สาขาวิชา Management School IT Alignment and Governance Institute ในประเทศเบลเยียม

ตัวอย่างที่ 1—การส่งทอดเป้าหมาย

องค์กรได้กำหนดเป้าหมายกลยุทธ์ขึ้นมาจำนวนหนึ่ง ซึ่งการปรับปรุงความพึงพอใจของลูกค้าเป็นเป้าหมายที่สำคัญที่สุด จากจุดดังกล่าว องค์กรต้องการทราบถึงทุกจุดที่เกี่ยวข้องกับไอทีที่จะต้องปรับปรุง

องค์กรตัดสินใจกำหนดให้ความพึงพอใจของลูกค้ามีความสำคัญในลำดับต้น เท่ากับว่าได้ยกระดับความสำคัญให้กับเป้าหมายระดับองค์กรในข้อต่อไปนี้ (จาก**รูปภาพที่ 5**):
- 6. วัฒนธรรมที่เน้นการบริการลูกค้า
- 7. บริการของธุรกิจมีความต่อเนื่องและความพร้อมให้บริการ
- 8. การตอบสนองอย่างฉับไวต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ

จากนั้น องค์กรดำเนินการในลำดับถัดมาในการส่งทอดเป้าหมาย ได้แก่การวิเคราะห์ว่าเป้าหมายที่เกี่ยวข้องกับไอทีข้อใดที่มีความเชื่อมโยงกับเป้าหมายระดับองค์กรเหล่านี้ ความเชื่อมโยงที่ให้เป็นแนวทางไว้นี้ ได้แสดงไว้ในภาคผนวก B

จากนั้น เป้าหมายที่เกี่ยวข้องกับไอทีดังต่อไปนี้ถือว่ามีความสำคัญมากที่สุด (ระบุไว้ในตารางว่ามีความสัมพันธ์หลัก 'P'):
- 01 กลยุทธ์ด้านไอทีสอดคล้องไปในแนวทางเดียวกันกับกลยุทธ์ด้านธุรกิจ
- 04 ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้
- 07 การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ
- 09 ความคล่องตัวทางด้านไอที
- 10 ความมั่นคงปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน
- 14 ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้ และมีประโยชน์ในการตัดสินใจ
- 17 ความรู้ ความเชี่ยวชาญ และการริเริ่มดำเนินการเพื่อนวัตกรรมทางธุรกิจ

องค์กรตรวจสอบความสมเหตุสมผลของรายการ และตัดสินใจที่จะคงไว้ซึ่งเป้าหมาย 4 ข้อแรกให้มีความสำคัญในลำดับต้น

ในการส่งทอดในลำดับถัดไป โดยใช้แนวคิดของปัจจัยเอื้อ (ดูบทที่ 5) เป้าหมายที่เกี่ยวข้องกับไอทีเหล่านี้ขับเคลื่อนเป้าหมายของปัจจัยเอื้อจำนวนหนึ่งซึ่งรวมถึงเป้าหมายของกระบวนการ ในภาคผนวก C ได้แนะให้เห็นถึงความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีกับกระบวนการใน COBIT 5 ตารางที่นำเสนอช่วยให้สามารถระบุถึงกระบวนการที่เกี่ยวข้องกับไอทีที่มีความเกี่ยวเนื่องมากที่สุดในการสนับสนุนเป้าหมายที่เกี่ยวข้องกับไอที แต่กระบวนการอย่างเดียวยังไม่เพียงพอ ปัจจัยเอื้ออื่นๆ เช่น วัฒนธรรม พฤติกรรมและจริยธรรม โครงสร้างการจัดองค์กร หรือทักษะและความเชี่ยวชาญล้วนมีความสำคัญไม่ยิ่งหย่อนไปกว่ากันและจำเป็นต้องมีเป้าหมายที่ชัดเจน

เมื่อทำขั้นตอนดังกล่าวเสร็จแล้ว องค์กรก็จะได้ชุดของเป้าหมายที่สอดคล้องสำหรับปัจจัยเอื้อทั้งหมดที่ช่วยให้บรรลุถึงวัตถุประสงค์ด้านกลยุทธ์ที่ได้ประกาศไว้และชุดของมาตรวัดในการวัดผลการดำเนินงานที่เกี่ยวข้อง

ตัวอย่างที่ 2—ความต้องการของผู้มีส่วนได้เสีย: ความสามารถในการดำรงอยู่ได้

หลังจากดำเนินการวิเคราะห์ความต้องการของผู้มีส่วนได้เสียแล้ว องค์กรตัดสินใจว่า 'ความสามารถในการดำรงอยู่ได้' เป็นกลยุทธ์ที่มีความสำคัญในลำดับต้นๆ สำหรับความสามารถในการดำรงอยู่ได้นั้นไม่ได้มีเพียงแค่มุมมองด้านสภาพแวดล้อมเท่านั้น แต่ยังรวมถึงทุกสิ่งที่ส่งผลต่อความสำเร็จในระยะยาวขององค์กรด้วย

จากผลการวิเคราะห์ความต้องการของผู้มีส่วนได้เสีย องค์กรตัดสินใจที่จะมุ่งเน้นไปที่วัตถุประสงค์ 5 ข้อต่อไปนี้ โดยมีข้อมูลรายละเอียดเพิ่มเติมสำหรับเป้าหมายบางประการ
1. คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย โดยเฉพาะในสังคมของผู้มีส่วนได้เสีย
4. การปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับจากภายนอก เน้นที่กฎหมายด้านสิ่งแวดล้อมและกฎหมายที่เกี่ยวข้องกับกฎระเบียบข้อบังคับด้านแรงงานในข้อตกลงบริการจากหน่วยงานภายนอก
8. การตอบสนองอย่างฉับไวต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ
16. บุคคลกรที่มีทักษะและแรงจูงใจ ตระหนักว่าความสำเร็จขององค์กรขึ้นอยู่กับบุคลากรในองค์กร
17. วัฒนธรรมที่ส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ โดนเน้นที่นวัตกรรมในระยะยาว

จากลำดับความสำคัญนี้ สามารถนำการส่งทอดเป้าหมายมาประยุกต์ใช้ดังที่ได้อธิบายไว้แล้ว

คำถามเกี่ยวกับการกำกับดูแลและการบริหารจัดการด้านไอที

ในการตอบสนองความต้องการของผู้มีส่วนได้เสียในองค์กรที่พึ่งพาไอทีเป็นอย่างมาก จะเกิดคำถามมากมายเกี่ยวกับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร (**รูปภาพที่ 7**)

รูปภาพที่ 7—คำถามเกี่ยวกับการกำกับดูแลและการบริหารจัดการไอที	
ผู้มีส่วนได้เสียภายใน	**คำถามของผู้มีส่วนได้เสียภายใน**
• คณะกรรมการบริหาร • ประธานเจ้าหน้าที่บริหาร (CEO) • ผู้บริหารสูงสุดด้านการเงิน (CFO) • ผู้บริหารสูงสุดด้านสารสนเทศ (CIO) • ผู้บริหารสูงสุดด้านความเสี่ยง(CRO) • ผู้บริหารด้านธุรกิจ • เจ้าของกระบวนการทางธุรกิจ • ผู้จัดการด้านธุรกิจ • ผู้จัดการด้านความเสี่ยง • ผู้จัดการด้านความมั่นคงปลอดภัย • ผู้จัดการด้านบริการ • ผู้จัดการด้านทรัพยากรบุคคล • ผู้ตรวจสอบภายใน • เจ้าหน้าที่ด้านการรักษาความเป็นส่วนบุคคล • ผู้ใช้งานไอที • ผู้จัดการด้านไอที • อื่นๆ	• เราจะได้รับคุณค่าจากการใช้ไอทีได้อย่างไร ผู้ใช้งานมีความพอใจกับคุณภาพของบริการด้านไอทีหรือไม่ • เราจะจัดการกับประสิทธิภาพด้านไอทีได้อย่างไร • เราจะนำเทคโนโลยีใหม่ๆ มาใช้ให้ดีที่สุดเพื่อเปิดช่องทางกลยุทธ์ได้อย่างไร • เราจะจัดตั้งและจัดโครงสร้างหน่วยงานด้านไอทีให้ดีที่สุดได้อย่างไร • เราต้องพึ่งพาผู้ให้บริการภายนอกมากน้อยเพียงใด มีการจัดการกับสัญญาบริการด้านไอทีกับบุคคลภายนอกได้ดีเพียงใด เราจะได้รับความเชื่อมั่นจากผู้ให้บริการภายนอกได้อย่างไร • มีข้อกำหนด (ด้านการควบคุม) อะไรบ้างเกี่ยวกับสารสนเทศ • เราได้ระบุถึงความเสี่ยงที่เกี่ยวข้องทั้งหมดแล้วหรือยัง • เรามีการดำเนินงานด้านไอทีที่มีประสิทธิภาพ และต้านทานภัยต่างๆ ได้หรือไม่ • เราจะควบคุมต้นทุนด้านไอทีได้อย่างไร เราจะใช้ทรัพยากรด้านไอทีให้มีประสิทธิภาพและประสิทธิผลได้อย่างไร ทางเลือกใดที่มีประสิทธิภาพและประสิทธิผลมากที่สุดในการจ้างหน่วยงานภายนอก • เรามีบุคลากรที่เพียงพอสำหรับงานด้านไอทีหรือไม่ เราจะพัฒนาและรักษาทักษะของบุคลากรได้อย่างไร และจะจัดการประสิทธิภาพในการทำงานได้อย่างไร • เราจะได้รับความเชื่อมั่นในเรื่องของไอทีได้อย่างไร • ข้อมูลที่ได้รับการประมวลผลมีความปลอดภัยหรือไม่ • เราจะเพิ่มความคล่องตัวให้กับธุรกิจด้วยการมีสภาพแวดล้อมด้านไอทีที่มีความยืดหยุ่นได้อย่างไร • โครงการด้านไอทีประสบความล้มเหลวที่จะส่งมอบงานตามที่กำหนดหรือไม่ ถ้าใช่เป็นด้วยสาเหตุใด ไอทีเป็นอุปสรรคในการดำเนินกลยุทธ์ทางธุรกิจหรือไม่ • ไอทีมีความสำคัญเพียงใดต่อความอยู่รอดขององค์กร จะทำอย่างไรหากไอทีไม่พร้อมใช้ • กระบวนการทางธุรกิจที่เป็นหลักสำคัญในการดำเนินธุรกิจใดที่ต้องพึ่งพาไอที และกระบวนการเหล่านั้นต้องการอะไรบ้าง • มีการใช้จ่ายเกินงบประมาณสำหรับการปฏิบัติงานด้านไอทีโดยเฉลี่ยเท่าไร โครงการด้านไอทีมีการใช้จ่ายเงินเกินงบประมาณบ่อยครั้งหรือไม่และเป็นจำนวนเงินมากน้อยเพียงใด • มีการใช้ความพยายามไปในการแก้ปัญหาเฉพาะหน้ามากกว่าการปรับปรุงทางธุรกิจมากน้อยเพียงใด • มีทรัพยากรทางไอทีที่เพียงพอและมีโครงสร้างพื้นฐานที่พร้อมใช้ในการบรรลุถึงวัตถุประสงค์ด้านกลยุทธ์ขององค์กรหรือไม่ • การตัดสินใจในเรื่องสำคัญๆ ทางด้านไอทีใช้เวลานานมากน้อยเพียงใด • การใช้กำลังคนและการลงทุนทางด้านไอทีมีความโปร่งใสหรือไม่ • ไอทีใช้ในการสนับสนุนองค์กรในการปฏิบัติตามกฎระเบียบข้อบังคับต่างๆ และระดับของการให้บริการหรือไม่ จะทราบได้อย่างไรว่าเราได้ปฏิบัติตามกฎระเบียบข้อบังคับต่างๆ ที่ใช้บังคับทั้งหมดแล้ว
ผู้มีส่วนได้เสียภายนอก	**คำถามของผู้มีส่วนได้เสียภายนอก**
• พันธมิตรทางธุรกิจ • ผู้ขายหรือผู้ให้บริการ • ผู้ถือหุ้น • หน่วยงานกำกับดูแล / รัฐบาล • ผู้ใช้ภายนอก • ลูกค้า • องค์กรที่กำหนดมาตรฐาน • ผู้ตรวจสอบภายนอก • ที่ปรึกษา • อื่นๆ	• จะทราบได้อย่างไรว่าการดำเนินงานของพันธมิตรทางธุรกิจมีความปลอดภัยและเชื่อถือได้ • จะทราบได้อย่างไรว่าองค์กรปฏิบัติตามกฎและกฎระเบียบข้อบังคับที่เกี่ยวข้อง • จะทราบได้อย่างไรว่าองค์กรรักษาระบบการควบคุมภายในให้มีประสิทธิภาพหรือไม่ • พันธมิตรทางธุรกิจสามารถจัดการให้สารสนเทศที่เชื่อมโยงระหว่างกันอยู่ภายใต้การควบคุมหรือไม่

เราจะหาคำตอบสำหรับคำถามเหล่านี้ได้อย่างไร

คำถามทั้งหมดที่ระบุไว้ใน **รูปภาพที่ 7** สามารถเชื่อมโยงไปถึงเป้าหมายระดับองค์กร และใช้เป็นข้อมูลเพื่อการส่งทอดเป้าหมายเพื่อให้คำถามเหล่านั้นได้รับการตอบสนองอย่างมีประสิทธิภาพ ในภาคผนวก D จะมีตัวอย่างของความสัมพันธ์ระหว่างคำถามของผู้มีส่วนได้เสียภายที่ระบุไว้ใน **รูปภาพที่ 7** กับเป้าหมายระดับองค์กร

บทที่ 3
หลักการที่ 2: ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร

COBIT 5 กล่าวถึงการกำกับดูแลและการบริหารจัดการสารสนเทศและเทคโนโลยีที่เกี่ยวข้องในมุมมองที่ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร ซึ่งหมายความว่า COBIT 5:

- บูรณาการการควบคุมกำกับดูแลไอทีระดับองค์กรเข้าไปในการควบคุมกำกับดูแลขององค์กร กล่าวคือระบบการกำกับดูและของไอทีระดับองค์กรที่นำเสนอใน COBIT 5 สามารถบูรณาการอย่างไร้รอยต่อเข้ากับระบบการกำกับดูแลใดๆ ก็ตาม COBIT 5 ยังสอดคล้องกับมุมมองล่าสุดของการกำกับดูแล
- ครอบคลุมหน้าที่งานและกระบวนการทั้งหมดที่จำเป็นต้องกำกับดูแลและบริหารจัดการสารสนเทศขององค์กร และเทคโนโลยีที่เกี่ยวข้องไม่ว่าสารสนเทศจะได้รับการประมวลผลที่ใดก็ตาม โดยการขยายขอบเขตให้ครอบคลุมทั่วทั้งองค์กรนี้จึงทำให้ COBIT 5 มีการระบุถึงบริการด้านไอทีทั้งภายในและภายนอกทั้งหมดที่เกี่ยวข้องพร้อมกับกระบวนการทางธุรกิจทั้งภายในและภายนอก

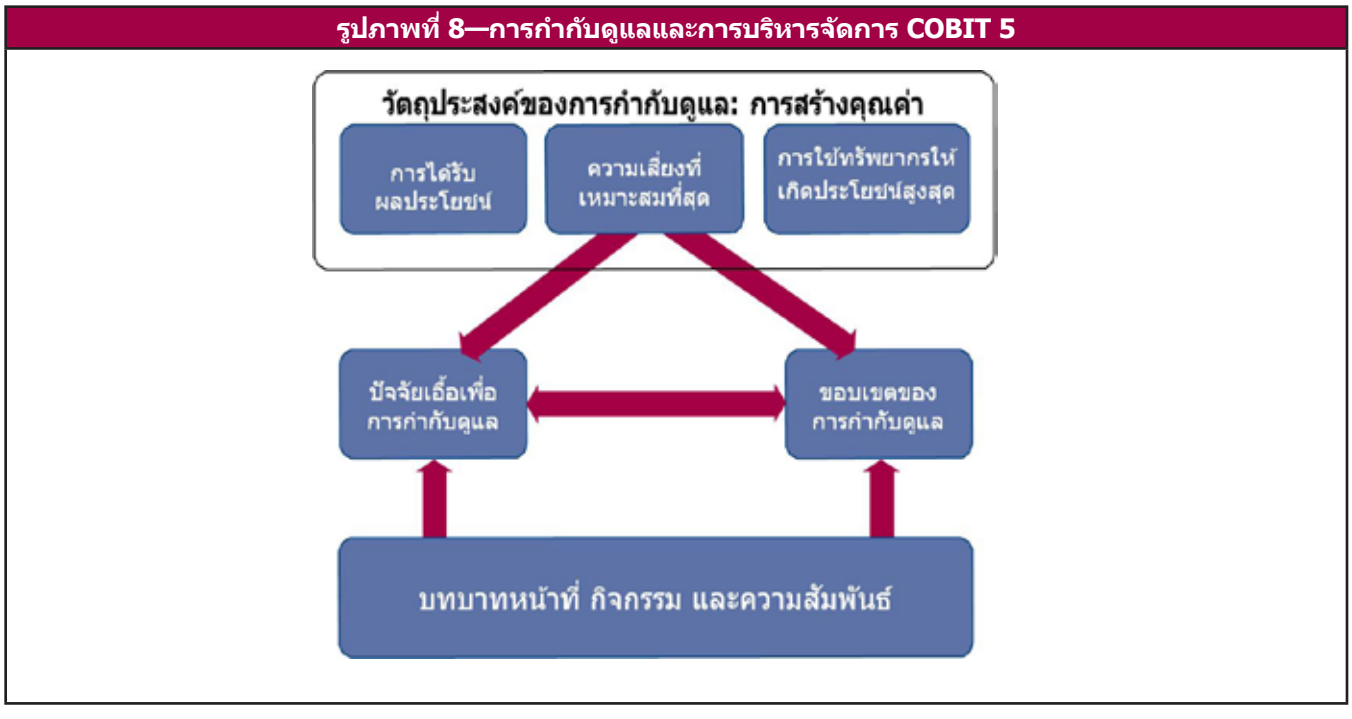
COBIT 5 ให้ภาพของการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรอย่างเป็นองค์รวมและเป็นระบบ (ดูหลักการที่ 4) โดยอิงกับปัจจัยเอื้อจำนวนหนึ่ง ปัจจัยเอื้อเหล่านี้อาจพบอยู่ตรงไหนก็ได้ทั่วทั้งองค์กรและตั้งแต่เริ่มต้นจนจบ ได้แก่การรวมเอาทุกสิ่งและทุกคน ทั้งภายในและภายนอก ที่เกี่ยวเนื่องกับการกำกับดูแลและการบริหารจัดการสารสนเทศขององค์กรและไอทีที่เกี่ยวข้อง รวมทั้งกิจกรรมและความรับผิดชอบของทั้งด้านไอทีและด้านธุรกิจที่ไม่ใช่ไอที

สารสนเทศเป็นปัจจัยเอื้อประเภทหนึ่งของ COBIT รูปแบบที่ COBIT ได้ระบุถึงปัจจัยเอื้อช่วยให้ผู้มีส่วนได้เสียทุกคนสามารถระบุถึงความต้องการสารสนเทศและวัฏจักรการประมวลผลของสารสนเทศของตนได้อย่างครอบคลุมและสมบูรณ์ จึงช่วยให้สามารถเชื่อมต่อกับธุรกิจและความต้องการของธุรกิจที่จำเป็นต้องมีสารสนเทศและหน้าที่งานด้านไอทีที่เหมาะสม รวมทั้งสนับสนุนธุรกิจและบริบทที่มีความสำคัญ

วิธีปฏิบัติสำหรับการกำกับดูแล

วิธีปฏิบัติสำหรับการกำกับดูแลอย่างครบวงจรเป็นเรื่องขั้นพื้นฐานของ COBIT 5 ดังที่แสดงใน**รูปภาพที่ 8** ซึ่งแสดงให้เห็นถึงส่วนประกอบหลักของระบบการกำกับดูแล[4]

รูปภาพที่ 8—การกำกับดูแลและการบริหารจัดการ COBIT 5



นอกจากวัตถุประสงค์ด้านการกำกับดูแลแล้วองค์ประกอบที่สำคัญอื่นๆ ของวิธีปฏิบัติสำหรับการกำกับดูแลยังรวมถึง ปัจจัยเอื้อ ได้แก่ขอบเขตบทบาทหน้าที่ กิจกรรมต่างๆ และความสัมพันธ์

[4] ระบบการกำกับดูแลได้แสดงไว้ในการริเริ่มดำเนินงาน ISACA' s Taking Governance Forward (TGF) รายละเอียดเพิ่มเติมสามารถหาได้จาก www.takinggovernanceforward.org.

ปัจจัยเอื้อเพื่อการกำกับดูแล
ปัจจัยเอื้อเพื่อการกำกับดูแล ได้แก่ทรัพยากรที่ใช้สำหรับจัดระบบในการกำกับดูแล เช่น กรอบการดำเนินงาน หลักการ โครงสร้าง กระบวนการ และแนวปฏิบัติ ซึ่งกำหนดทิศทางของการกระทำและช่วยให้บรรลุวัตถุประสงค์ ปัจจัยเอื้อยังรวมถึงทรัพยากรขององค์กรเช่น ความสามารถในการบริการ (โครงสร้างพื้นฐานด้านไอที ระบบงาน และอื่นๆ) บุคลากร และสารสนเทศ การขาดแคลนทรัพยากรหรือปัจจัยเอื้ออาจจะส่งผลต่อความสามารถขององค์กรในการสร้างคุณค่า

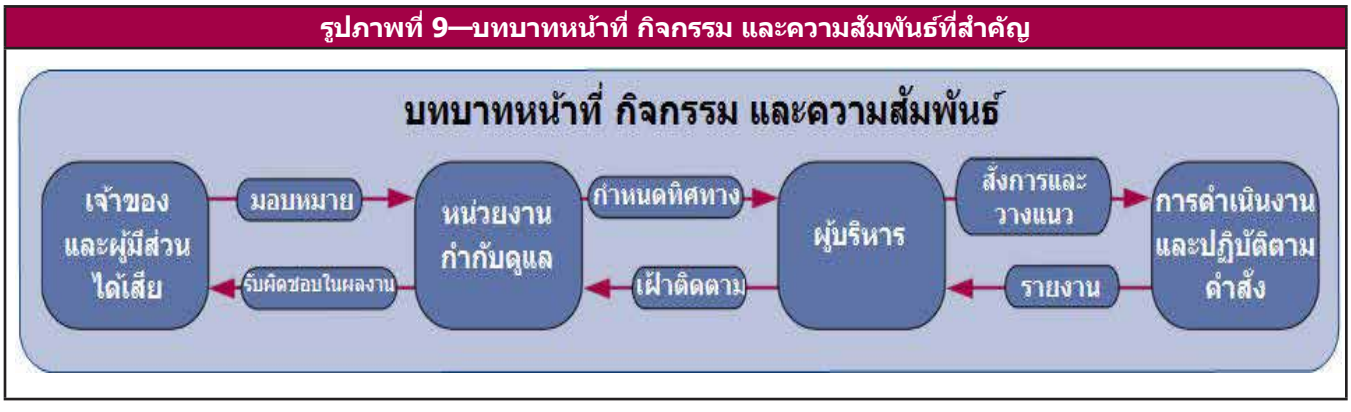
ด้วยความสำคัญของปัจจัยเอื้อเพื่อการกำกับดูแล COBIT 5 จึงมีเพียงหนทางเดียวที่จะพิจารณาและจัดการกับปัจจัยเอื้อ (ดูบทที่ 5).

ขอบเขตของการกำกับดูแล
การกำกับดูแลสามารถประยุกต์ใช้กับทั่วทั้งองค์กรกับหน่วยงานใดหน่วยงานหนึ่ง กับสินทรัพย์ทั้งที่จับต้องได้และจับต้องไม่ได้ และอื่นๆ กล่าวคือ เราสามารถกำหนดการนำการกำกับดูแลไปประยุกต์ใช้ในมุมมองที่แตกต่างกันไปของแต่ละองค์กร และเป็นสิ่งจำเป็นที่จะต้องระบุขอบเขตของระบบการกำกับดูแลนี้ให้ดี ขอบเขตของ COBIT 5 คือ ระดับองค์กร แต่เนื้อหาสาระของ COBIT 5 สามารถนำไปประยุกต์ใช้ได้ในมุมมองใดๆ ที่แตกต่างออกไปก็ได้

บทบาท กิจกรรม และความสัมพันธ์
องค์ประกอบสุดท้าย คือ บทบาท กิจกรรมและความสัมพันธ์ของการกำกับดูแลซึ่งระบุว่าใครมีส่วนร่วมในการกำกับดูแล มีส่วนร่วมอย่างไร และบุคคลเหล่านั้นทำอะไร และจะมีปฏิสัมพันธ์ระหว่างกันอย่างไร ภายใต้ขอบเขตของระบบการกำกับดูแล ใน COBIT 5 จะแบ่งแยกกิจกรรมการกำกับดูแลออกจากกิจกรรมการบริหารจัดการอย่างชัดเจน พร้อมกับระบุถึงความสัมพันธ์ระหว่างกันและผู้ที่มีบทบาทหน้าที่จะเข้ามามีส่วนร่วม **รูปภาพที่ 9** แสดงถึงรายละเอียดของส่วนล่างของ**รูปภาพที่ 8** ซึ่งแสดงรายการปฏิสัมพันธ์ระหว่างบทบาทหน้าที่ต่างๆ

สำหรับข้อมูลเพิ่มเติมในมุมมองทั่วไปสำหรับการกำกับดูแล กรุณาดู "taking governance Forward" ที่ *www.takinggovernanceforward.org*

รูปภาพที่ 9—บทบาทหน้าที่ กิจกรรม และความสัมพันธ์ที่สำคัญ



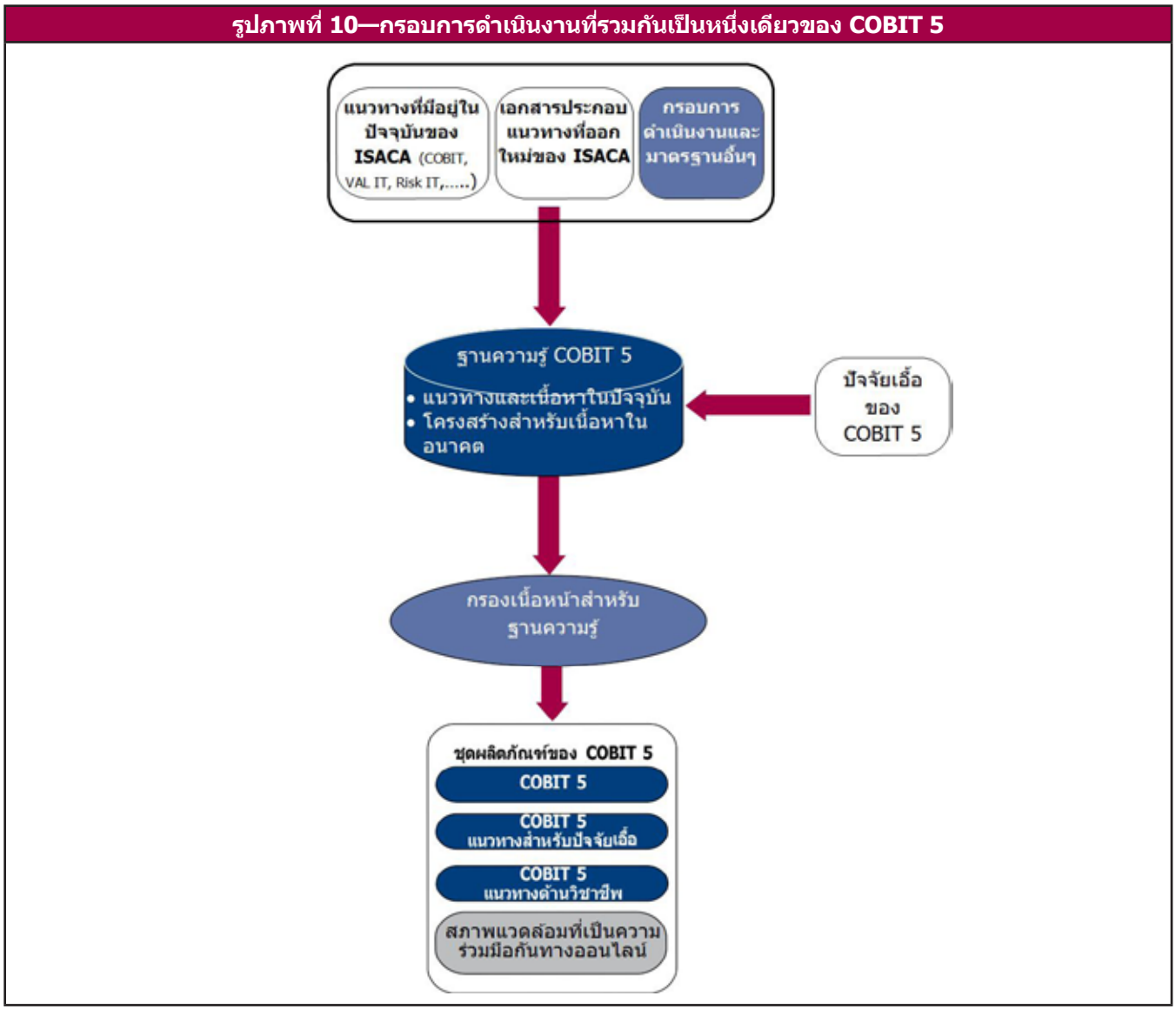
บทที่ 4
หลักการที่ 3: ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว

COBIT 5 เป็นกรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว เนื่องจาก:
- สอดคล้องกับมาตรฐานและกรอบการดำเนินงานอื่นๆ ที่เกี่ยวข้อง ซึ่งช่วยให้องค์กรสามารถใช้ COBIT 5 เสมือนเป็นกรอบการดำเนินงานที่ครอบอยู่เหนือการบูรณาการกำกับดูแลและการบริหารจัดการ
- ครอบคลุมทั่วทั้งองค์กรอย่างสมบูรณ์ ซึ่งให้หลักในการบูรณาการ การใช้กรอบการดำเนินงาน มาตรฐาน และแนวปฏิบัติอื่นๆ อย่างมีประสิทธิผล กรอบการดำเนินงานที่ครอบเป็นหนึ่งเดียวนี้ทำให้การนำแนวทางจากแหล่งต่างๆ มาใช้สอดคล้องและบูรณาการเข้าด้วยกัน โดยไม่ใช้ภาษาเชิงเทคนิคหรือภาษาด้านเทคโนโลยี
- ให้สถาปัตยกรรมที่เรียบง่ายสำหรับจัดโครงสร้างของเอกสารประกอบแนวทางและการจัดทำชุดผลิตภัณฑ์ที่สอดคล้องกัน
- บูรณาการองค์ความรู้ต่างๆ ที่กระจัดกระจายอยู่ตามกรอบการดำเนินงานต่างๆ ของ ISACA ทั้งหมด ISACA ได้วิจัยประเด็นที่สำคัญๆ เกี่ยวกับการกำกับดูแลระดับองค์กรมาหลายปี และจัดทำกรอบการดำเนินงานออกมาใช้มากมาย ไม่ว่าจะเป็น COBIT, Val IT, Risk IT, BMIS, เอกสารที่ชื่อว่าบทสรุปการกำกับดูแลไอทีสำหรับกรรมการบริหาร (Board briefing on IT Governance), และ ITAF ซึ่งให้แนวทางและการสนับสนุนแก่องค์กร COBIT 5 ได้บูรณาการองค์ความรู้ทั้งหมดนี้เข้าไว้ด้วยกัน

COBIT 5 เป็นที่รวบรวมกรอบการดำเนินงานต่างๆ

รูปภาพที่ 10 ให้คำอธิบายด้วยภาพว่า COBIT 5 เป็นกรอบการดำเนินงานที่บูรณาการและมีความสอดคล้องไปในแนวทางเดียวกันได้อย่างไร

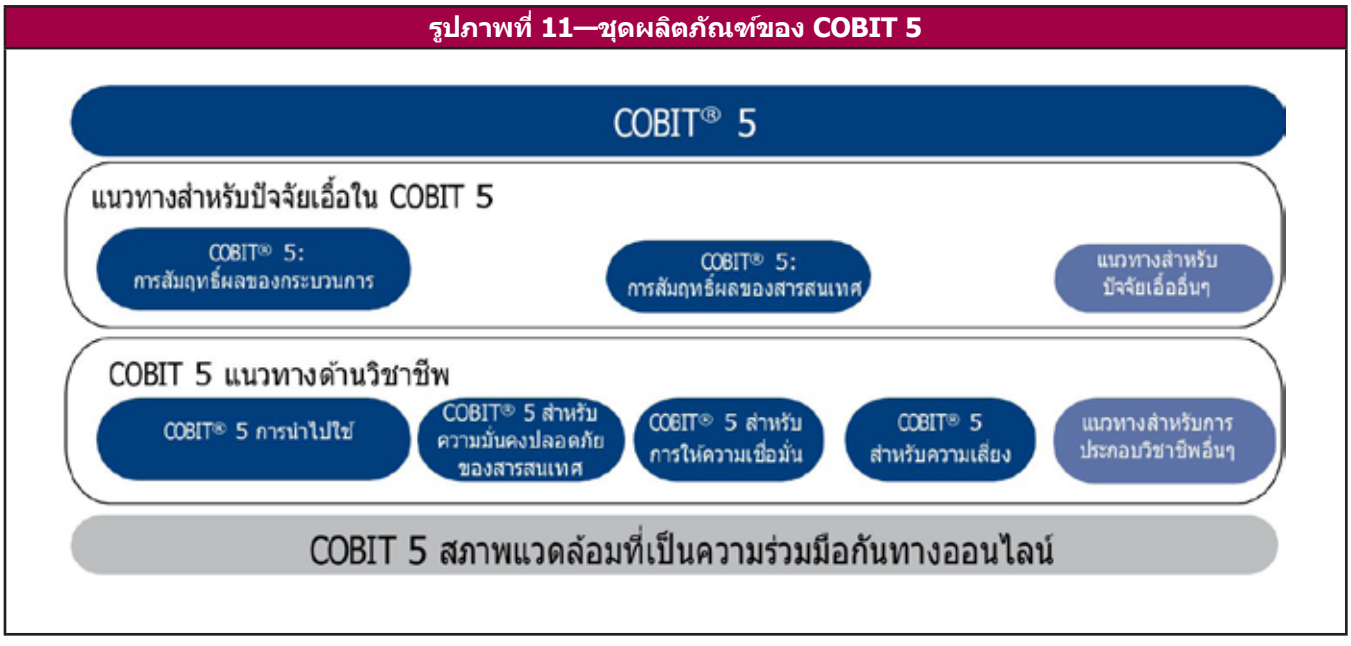
รูปภาพที่ 10—กรอบการดำเนินงานที่รวมกันเป็นหนึ่งเดียวของ COBIT 5



กรอบการดำเนินงานของ COBIT 5 ได้ให้แนวทางที่สมบูรณ์และเป็นปัจจุบันมากที่สุดแก่ผู้มีส่วนได้เสียต่างๆ (**ดูรูปภาพที่ 11**) ในด้านการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร โดย

- การทำวิจัยและใช้แหล่งข้อมูลต่างๆ ที่ผลักดันให้เกิดการพัฒนาเนื้อหาใหม่ๆ ซึ่งประกอบด้วย
  - การนำแนวทางของ ISACA ที่มีอยู่ (COBIT4.1, ValIT2.0, RiskIT, BMIS) มารวมกันเป็นกรอบการดำเนินงานเพียงหนึ่งเดียว
  - การเสริมเนื้อหาในส่วนที่จำเป็นต้องมีคำอธิบายเพิ่มเติมและต้องปรับปรุงให้เป็นปัจจุบัน
  - การจัดแนวให้สอดคล้องกับมาตรฐานและกรอบการดำเนินงานอื่นๆ ที่เกี่ยวข้อง เช่น ITIL ,TOGAF และมาตรฐาน ISO รายการอ้างอิงทั้งหมดสามารถดูได้ในภาคผนวก A
- การระบุถึงกลุ่มของปัจจัยเอื้อเพื่อการกำกับดูแลและการบริหารจัดการ ซึ่งใช้เป็นโครงสร้างสำหรับเอกสารประกอบแนวทางทั้งหมด
- การเพิ่มข้อมูลเข้าสู่ฐานความรู้ของ COBIT 5 ให้จัดเก็บแนวทางและเนื้อหาทั้งหมดในปัจจุบันและให้โครงสร้างสำหรับเนื้อหาที่จะเพิ่มเติมในอนาคต
- การใช้อ้างอิงสำหรับแนวปฏิบัติที่ดีที่เหมาะสมและครอบคลุม

รูปภาพที่ 11—ชุดผลิตภัณฑ์ของ COBIT 5



บทที่ 5
หลักการที่ 4: เอื้อให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผล

ปัจจัยเอื้อใน COBIT 5

ปัจจัยเอื้อ อาจเป็นหนึ่งปัจจัยหรือหลายปัจจัยมารวมกัน ที่มีอิทธิพลต่อความสำเร็จของงาน ซึ่งในที่นี้ก็คือการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร ปัจจัยเอื้อขับเคลื่อนโดยการส่งทอดเป้าหมาย (goals cascade) กล่าวคือเป้าหมายที่เกี่ยวข้องกับไอทีในภาพรวมจะระบุว่าจะต้องมีปัจจัยเอื้ออะไรบ้าง

กรอบการดำเนินงาน COBIT 5 อธิบายถึงปัจจัยเอื้อ 7 ประเภท ประกอบด้วย (**รูปภาพที่ 12**)
- **หลักการ นโยบาย และกรอบการดำเนินงาน** ซึ่งเป็นสิ่งที่นำไปสู่การแปลงพฤติกรรมที่คาดหวังให้เป็นแนวทางที่ปฏิบัติได้จริงสำหรับการบริหารจัดการประจำวัน
- **กระบวนการ** อธิบายถึงกลุ่มของแนวปฏิบัติและกิจกรรมที่ใช้บรรลุวัตถุประสงค์บางประการ และให้ผลลัพธ์เพื่อสนับสนุนการบรรลุวัตถุประสงค์ที่เกี่ยวข้องกับไอทีโดยรวม
- **โครงสร้างการจัดองค์กร** ระบุถึงหน่วยงานที่เป็นหลักในการตัดสินใจในองค์กร
- **วัฒนธรรม จริยธรรม และพฤติกรรม** ทั้งของแต่ละบุคคลและขององค์กร ซึ่งมักจะได้รับการประเมินค่าน้อยกว่าจริงในการเป็นปัจจัยสู่ความสำเร็จของกิจกรรมการกำกับดูแลและการบริหารจัดการ
- **สารสนเทศ** ที่ใช้กันอย่างกว้างขวางทั่วทั้งองค์กร ซึ่งรวมสารสนเทศทั้งที่เกิดจากและที่ใช้โดยองค์กร สารสนเทศเป็นสิ่งจำเป็นที่องค์กรจะต้องใช้เพื่อดำเนินกิจกรรมและเพื่อการกำกับดูแลที่ดี แต่สำหรับในระดับปฏิบัติการเท่านั้น สารสนเทศมักมองว่าเป็นผลผลิตหลักขององค์กร
- **บริการ โครงสร้างพื้นฐาน และระบบงาน** รวมถึงโครงสร้างพื้นฐาน เทคโนโลยี และระบบงานที่ใช้สำหรับการประมวลผลและบริการอื่นๆ ด้านเทคโนโลยีแก่องค์กร
- **บุคลากร ทักษะ และศักยภาพ** เชื่อมโยงกับเข้ากับตัวบุคคลและเป็นสิ่งจำเป็นที่จะช่วยให้กิจกรรมทั้งหมดสำเร็จลุล่วงไปด้วยดี และช่วยให้ตัดสินใจได้อย่างถูกต้องพร้อมทั้งดำเนินการแก้ไข

รูปภาพที่ 12—ปัจจัยเอื้อขององค์กรใน COBIT 5

ปัจจัยเอื้อบางประการที่ระบุไว้ก่อนหน้านี้ ก็เป็นทรัพยากรขององค์กรที่จำเป็นต้องจัดการและกำกับดูแลเช่นกัน ซึ่งรวมถึง
- สารสนเทศ ซึ่งจำเป็นต้องได้รับการบริหารจัดการเช่นเดียวกับทรัพยากรอื่นๆ สารสนเทศบางอย่างเช่น รายงานสำหรับผู้บริหาร และข้อมูลเพื่อการวิเคราะห์ธุรกิจ (business intelligence information) เป็นปัจจัยเอื้อที่สำคัญสำหรับการกำกับดูแลและการบริหารจัดการองค์กร
- บริการ โครงสร้างพื้นฐาน และระบบงาน
- บุคคลากร ทักษะ และศักยภาพ

การกำกับดูแลและการบริหารจัดการอย่างเป็นระบบด้วยปัจจัยเอื้อที่เชื่อมต่อถึงกัน

รูปภาพที่ 12 ยังได้แสดงถึงแนวคิดที่ควรนำไปประยุกต์ใช้กับการกำกับดูแลในระดับองค์กรเพื่อให้บรรลุวัตถุประสงค์หลักขององค์กร ซึ่งย่อมรวมถึงการกำกับดูแลทางด้านไอทีด้วย องค์กรใดๆ ก็ตามจะต้องคำนึงถึงการเชื่อมโยงกันของปัจจัยเอื้อต่างๆ นี้ กล่าวคือ แต่ละปัจจัยเอื้อ
- ต้องการข้อมูลจากปัจจัยเอื้ออื่นๆ เพื่อให้สามารถทำงานได้อย่างมีประสิทธิผล ยกตัวอย่างเช่น กระบวนการต้องการสารสนเทศ โครงสร้างขององค์กรต้องการทักษะและพฤติกรรม เป็นต้น
- ส่งมอบผลลัพธ์ที่เป็นประโยชน์แก่ปัจจัยเอื้ออื่นๆ ยกตัวอย่างเช่น กระบวนการส่งมอบสารสนเทศ ทักษะและพฤติกรรมช่วยให้กระบวนการมีประสิทธิผล

ดังนั้น เมื่อต้องรับมือกับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร การตัดสินใจที่ดีจะเกิดขึ้นได้ก็ต่อเมื่อมีการกำกับดูแลและการบริหารจัดการอย่างเป็นระบบ ซึ่งย่อมหมายความว่า เมื่อต้องรับมือกับความต้องการของผู้มีส่วนได้เสีย

ปัจจัยเอื้อต่างๆ ที่มีความสัมพันธ์กันนี้ต้องได้รับการวิเคราะห์ในเรื่องความเชื่อมโยงถึงกันและได้รับการจัดการเมื่อเกิดปัญหา ผู้บริหารระดับสูงขององค์กรจะต้องผลักดันแนวคิดนี้ ดังที่จะแสดงให้เป็นตัวอย่างต่อไปนี้

ตัวอย่างที่ 3—การกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

การให้บริการด้านไอทีแก่ผู้ใช้ทุกคนจำเป็นต้องมีความสามารถในการให้บริการ (โครงสร้างพื้นฐาน ระบบงาน) และบุคลากรที่มีทักษะและพฤติกรรมที่เหมาะสม ทั้งยังต้องมีกระบวนการทำงานเพื่อส่งมอบบริการต่างๆ ที่สนับสนุนด้วยโครงสร้างการจัดองค์กรที่เหมาะสม ซึ่งแสดงให้เห็นว่าปัจจัยเอื้อต่างๆ เหล่านี้มีความจำเป็นต่อความสำเร็จในการส่งมอบบริการ

ตัวอย่างที่ 4—การกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

ความจำเป็นที่จะต้องรักษาความมั่นคงปลอดภัยด้านสารสนเทศทำให้องค์กรต้องออกนโยบายและขั้นตอนการปฏิบัติงานต่างๆ มาบังคับใช้ อย่างไรก็ตาม หากวัฒนธรรมและจริยธรรมของบุคคลและองค์กรไม่เหมาะสม กระบวนการและขั้นตอนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศก็จะไร้ประสิทธิผล

มิติต่างๆ ของปัจจัยเอื้อใน COBIT 5

ทุกปัจจัยเอื้อมีมิติที่เหมือนกันอยู่ชุดหนึ่ง (**ดูรูปภาพที่ 13**) มิติเหล่านี้
- ช่วยให้มีวิธีที่เหมือนกัน เรียบง่าย และเป็นระบบในการจัดการกับปัจจัยเอื้อ
- ช่วยให้แต่ละหน่วยงานสามารถบริหารจัดการปฏิสัมพันธ์ที่ซับซ้อนของตนได้
- ช่วยให้ปัจจัยเอื้อทำงานได้ผลสำเร็จ

รูปภาพที่ 13—ปัจจัยเอื้อทั่วไปใน COBIT 5

มิติต่างๆ ของปัจจัยเอื้อ

ปัจจัยเอื้อต่างมีมิติที่เหมือนกันอยู่ 4 ด้าน ได้แก่
- **ผู้มีส่วนได้เสีย**—แต่ละปัจจัยเอื้อมีผู้มีส่วนได้เสีย (ผู้ที่มีบทบาทสำคัญหรือมีผลประโยชน์ในปัจจัยเอื้อนั้น) ยกตัวอย่าง เช่น กระบวนการมีหน่วยงานต่างๆ ที่ดำเนินกิจกรรมของกระบวนการ และ/หรือที่ได้รับประโยชน์จากผลลัพธ์ของกระบวนการนั้นๆ โครงสร้างองค์กรมีผู้ที่มีส่วนได้เสียซึ่งแต่ละคนก็มีบทบาทหน้าที่และผลประโยชน์อันเป็นส่วนหนึ่งของโครงสร้าง ผู้มีส่วนได้เสียอาจจะอยู่ภายในหรืออยู่ภายนอกองค์กรก็ได้ ผู้มีส่วนได้เสียต่างก็มีผลประโยชน์และความต้องการของตน ซึ่งในบางครั้งอาจจะขัดแย้งกันเอง ความต้องการของผู้มีส่วนได้เสียแปลงมาเป็นเป้าหมายขององค์กร ซึ่งเป้าหมายนี้ก็จะถูกแปลงมาเป็นเป้าหมายที่เกี่ยวข้องกับไอทีสำหรับองค์กร รายละเอียดของผู้มีส่วนได้เสียแสดงอยู่ใน **รูปภาพที่ 7**
- **เป้าหมาย**—แต่ละปัจจัยเอื้อมีเป้าหมายจำนวนหนึ่งและปัจจัยเอื้อให้คุณค่าโดยการบรรลุเป้าหมายเหล่านั้น เป้าหมายเหล่านี้อาจระบุเป็นลักษณะของ
  – ผลลัพธ์ที่คาดหวังจากปัจจัยเอื้อ
  – ระบบงานหรือปฏิบัติการของปัจจัยเอื้อเอง

เป้าหมายของปัจจัยเอื้อเป็นขั้นตอนสุดท้ายของการส่งทอดเป้าหมายใน COBIT 5 เป้าหมายสามารถแยกออกเป็นกลุ่มต่างๆ ได้ดังนี้
– **คุณภาพในตัวเอง** (intrinsic quality) ครอบคลุมถึงการที่ปัจจัยเอื้อทำงานอย่างถูกต้อง เที่ยงตรง และให้ผลลัพธ์ที่

แม่นยำ เที่ยงตรง และเชื่อถือได้
  - **คุณภาพเชิงบริบท** (contextual quality) ครอบคลุมถึงการที่ปัจจัยเอื้อและผลลัพธ์เป็นไปตามจุดประสงค์ในบริบทที่ปัจจัยเอื้อนั้นดำเนินงานอยู่ ยกตัวอย่างเช่น ผลลัพธ์ควรจะเกี่ยวเนื่อง สมบูรณ์ เป็นปัจจุบัน เหมาะสม สม่ำเสมอ เข้าใจได้ง่าย และใช้งานง่าย
  - **การเข้าถึงและการรักษาความมั่นคงปลอดภัย** ครอบคลุมถึงการที่ปัจจัยเอื้อและผลลัพธ์สามารถเข้าถึงได้และมีความปลอดภัย ยกตัวอย่างเช่น
    - ปัจจัยเอื้อมีความพร้อมใช้เมื่อต้องการ
    - มีการรักษาความปลอดภัยให้กับผลลัพธ์ ได้แก่การเข้าถึงผลลัพธ์จำกัดให้เฉพาะผู้ที่ได้รับอนุมัติและจำเป็นต้องใช้เท่านั้น
- **วัฏจักร**—แต่ละปัจจัยเอื้อมีวัฏจักรจากจุดเริ่มต้นผ่านช่วงเวลาของการดำเนินงาน/การใช้ประโยชน์จนถึงการจำหน่ายออก วัฏจักรนี้ประยุกต์ใช้กับสารสนเทศ โครงสร้าง กระบวนการ นโยบาย และอื่นๆ วัฏจักรประกอบด้วยระยะต่างๆ ของการดำเนินงานดังนี้
  - การวางแผน (รวมถึง การพัฒนาและการคัดเลือกแนวคิด)
  - การออแบบ
  - การสร้าง/การจัดซื้อจัดหา/การจัดทำ/การนำไปใช้
  - ใช้/ดำเนินการ
  - ประเมิน/เฝ้าติดตาม
  - ปรับให้เป็นปัจจุบัน/จำหน่ายออก
- **แนวปฏิบัติที่ดี**—เราสามารถกำหนดแนวปฏิบัติที่ดีสำหรับปัจจัยเอื้อแต่ละรายการได้ แนวปฏิบัติที่ดีสนับสนุนปัจจัยเอื้อให้บรรลุถึงเป้าหมาย แนวปฏิบัติที่ดีให้ตัวอย่างหรือข้อแนะนำว่าจะนำปัจจัยเอื้อไปใช้งานอย่างไรให้ได้ดีที่สุด และชิ้นงานหรือข้อมูลรับเข้าและผลลัพธ์อะไรบ้างที่ต้องการ COBIT 5 ได้ให้ตัวอย่างของแนวปฏิบัติที่ดีสำหรับปัจจัยเอื้อใน COBIT 5 เฉพาะบางรายการ (เช่น กระบวนการ) ส่วนปัจจัยเอื้ออื่นๆ ที่เหลือสามารถใช้แนวทางจากมาตรฐาน และกรอบการดำเนินงานอื่นๆ ได้

การบริหารจัดการประสิทธิภาพของปัจจัยเอื้อ
องค์กรคาดหวังที่จะได้ผลลัพธ์ในด้านดีจากระบบงานและการใช้ปัจจัยเอื้อต่างๆ ในการบริหารจัดการประสิทธิภาพของปัจจัยเอื้อจะต้องเฝ้าติดตามคำถามเหล่านี้และหาคำตอบจากมาตรวัดอย่างสม่ำเสมอ
- มีการระบุความต้องการของผู้มีส่วนได้เสียหรือไม่
- บรรลุเป้าหมายของปัจจัยเอื้อหรือไม่
- วัฏจักรของปัจจัยเอื้อได้รับการจัดการหรือไม่
- มีการประยุกต์ใช้แนวปฏิบัติที่ดีหรือไม่

คำถามสองข้อแรกเป็นคำถามเกี่ยวกับผลที่เกิดขึ้นจริงจากปัจจัยเอื้อ มาตรวัดที่ใช้วัดว่าได้บรรลุถึงเป้าหมายเพียงใดนั้น เรียกว่า 'ดัชนีตาม' (lag indicators)

คำถามสองข้อหลังเป็นคำถามเกี่ยวกับการทำงานจริงของปัจจัยเอื้อ และมาตรวัดที่ใช้จะเรียกว่า 'ดัชนีชี้นำ' (lead indicators)

ตัวอย่างของปัจจัยเอื้อในทางปฏิบัติ

ตัวอย่างที่ 5 แสดงถึงปัจจัยเอื้อ การเชื่อมต่อระหว่างกัน และมิติต่างๆ ของปัจจัยเอื้อ และการใช้สิ่งเหล่านี้ให้เกิดประโยชน์ในทางปฏิบัติ

ตัวอย่างที่ 5—ปัจจัยเอื้อ

องค์กรได้แต่งตั้ง "ผู้จัดการกระบวนการ" สำหรับกระบวนการที่เกี่ยวข้องกับไอทีเพื่อรับผิดชอบในการจัดวางและดำเนินกระบวนการต่างๆ ที่เกี่ยวข้องกับไอทีให้มีประสิทธิภาพและประสิทธิผล ภายใต้บริบทของการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

เริ่มต้น ผู้จัดการกระบวนการจะมุ่งไปที่ปัจจัยเอื้อด้านกระบวนการ โดยพิจารณาถึงมิติต่างๆของปัจจัยเอื้อดังนี้

- **ผู้มีส่วนได้เสีย**: ผู้มีส่วนได้เสียในกระบวนการ รวมถึงผู้ปฏิบัติงานทั้งหมดในกระบวนการ ได้แก่ ทุกฝ่ายที่รับผิดชอบตามหน้าที่ (Responsible) รับผิดชอบในผลงาน (Accountable) ให้คำปรึกษา (Consulted) หรือได้รับแจ้งให้ทราบ(Informed) (ตาราง RACI) สำหรับหรือระหว่างการดำเนินกิจกรรมของกระบวนการ เราสามารถนำตาราง RACI ที่ได้อธิบายไว้ใน *COBIT 5 : การสัมฤทธิ์ผลของกระบวนการ (COBIT 5: Enabling Processes)* มาใช้งานได้
- **เป้าหมาย:** แต่ละกระบวนการต้องมีการกำหนดเป้าหมายและมาตรวัดที่เหมาะสม ยกตัวอย่างเช่น กระบวนการบริหารจัดการความสัมพันธ์ (กระบวนการ APO08 ใน *COBIT 5 : การสัมฤทธิ์ผลของกระบวนการ (COBIT 5: Enabling Processes)*) เราสามารถอ้างถึงชุดของเป้าหมายและมาตรวัดดังนี้
  - **เป้าหมาย**: ทำความเข้าใจถึงกลยุทธ์ทางธุรกิจ แผนงาน และความต้องการ เป็นอย่างดี จัดทำเป็นลายลักษณ์อักษร และได้รับอนุมัติ
    - ***มาตรวัด:*** ร้อยละของชุดโครงการ (programme) ที่สอดคล้องกับความต้องการทางธุรกิจหรือลำดับความสำคัญขององค์กร
  - **เป้าหมาย:** มีความสัมพันธ์ที่ดีระหว่างองค์กรกับหน่วยงานด้านไอที
    - ***มาตรวัด:*** คะแนนจากผลการสำรวจความพึงพอใจของผู้ใช้งานและบุคลากรด้านไอที
- **วัฏจักร**: แต่ละกระบวนการมีวัฏจักรในการดำเนินงาน ได้แก่ กระบวนการได้รับการสร้างขึ้น ดำเนินการและเฝ้าติดตาม และปรับปรุงแก้ไขเมื่อจำเป็น แต่ในที่สุดกระบวนการนั้นก็จะถูกยกเลิกไป ด้วยวัฏจักรนี้ ผู้จัดการกระบวนการจะต้องออกแบบและกำหนดให้มีกระบวนการขึ้นมาเป็นอย่างแรก โดยสามารถใช้องค์ประกอบต่างๆ ที่มีระบุไว้ใน *COBIT 5 : การสัมฤทธิ์ผลของกระบวนการ (COBIT 5: Enabling Processes)* เพื่อใช้ในการออกแบบกระบวนการ ได้แก่ เพื่อกำหนดหน้าที่ความรับผิดชอบ และเพื่อแตกกระบวนการให้ย่อยลงมาเป็นแนวปฏิบัติและกิจกรรมต่างๆ พร้อมทั้งระบุชิ้นงานของกระบวนการ (ข้อมูลรับเข้าและผลลัพธ์) ในขั้นต่อมา จะต้องทำให้กระบวนการมีความทนทานและมีประสิทธิภาพ และด้วยจุดประสงค์นี้ ผู้จัดการกระบวนการสามารถเพิ่มระดับขีดความสามารถของกระบวนการ โดยการนำต้นแบบการวัดระดับความสามารถของกระบวนการ (Process Capability Model) และคุณลักษณะความสามารถของกระบวนการใน COBIT 5 ซึ่งได้แรงบันดาลใจจาก ISO/IEC 15504 มาใช้เพื่อการนี้

- **แนวปฏิบัติที่ดี**: COBIT 5 อธิบายถึงรายละเอียดของแนวปฏิบัติที่ดีสำหรับกระบวนการไว้ใน *COBIT 5 : การสัมฤทธิ์ผลของกระบวนการ (COBIT 5: Enabling Processes)* ดังที่ได้กล่าวไว้แล้วในหัวข้อก่อนหน้านี้ โดยที่มาและตัวอย่างของกระบวนการสามารถหาดูได้จากเอกสารดังกล่าว ซึ่งครอบคลุมถึงกิจกรรมที่หลากหลายอย่างครบถ้วนที่จำเป็นสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่ดี

นอกจากแนวทางของปัจจัยเอื้อด้านกระบวนการแล้ว ผู้จัดการกระบวนการยังสามารถพิจารณาปัจจัยเอื้ออื่นๆ ได้อีกด้วย อาทิเช่น

- ตาราง RACI ซึ่งอธิบายถึงบทบาทหน้าที่และความรับผิดชอบ ปัจจัยเอื้ออื่นๆ ช่วยให้เราสามารถลงไปในรายละเอียดของมิตินี้ได้ เช่น
  - ในปัจจัยเอื้อด้านทักษะและความสามารถ เราสามารถกำหนดทักษะและความสามารถสำหรับแต่ละบทบาทหน้าที่ พร้อมทั้งกำหนดเป้าหมายที่เหมาะสม (เช่น ระดับของทักษะด้านเทคนิคและด้านพฤติกรรม) และมาตรวัดที่เกี่ยวข้อง
  - ตาราง RACI ยังได้แสดงถึงโครงสร้างองค์จำนวนหนึ่ง ซึ่งปัจจัยเอื้อด้านโครงสร้างการจัดองค์กรสามารถอธิบายรายละเอียดเพิ่มเติมเกี่ยวกับโครงสร้างเหล่านี้ ไม่ว่าจะเป็นคำอธิบายในรายละเอียด ผลลัพธ์ที่คาดหวัง และมาตรวัดที่เกี่ยวข้อง (เช่น การตัดสินใจ) ตลอดจนการสามารถกำหนดแนวปฏิบัติที่ดี (เช่น ช่วงการควบคุม (span of control) หลักการปฏิบัติงานของโครงสร้าง ระดับของอำนาจหน้าที่)
- หลักการและนโยบาย จะทำให้กระบวนการมีลักษณะที่เป็นทางการและใช้อธิบายว่าทำไมถึงต้องมีกระบวนการนี้ ใช้กับใครและใช้อย่างไร สิ่งเหล่านี้เป็นจุดที่ปัจจัยเอื้อด้านหลักการและนโยบายจะเน้นถึง

ในภาคผนวก G ได้กล่าวถึงปัจจัยเอื้อ 7 ประเภทไว้อย่างละเอียด จึงควรอ่านภาคผนวก G เพื่อทำความเข้าใจปัจจัยเอื้อให้ดีขึ้น และเข้าใจถึงประโยชน์ว่ามีมากน้อยเพียงใดต่อการกำกับดูแลและบริหารจัดการไอทีระดับองค์กร

บทที่ 6
หลักการที่ 5: ความแตกต่างระหว่างการกำกับดูแลและการบริหารจัดการ

การกำกับดูแลและการบริหารจัดการ

กรอบการดำเนินงาน COBIT 5 ชี้ให้เห็นถึงความแตกต่างอย่างชัดเจนระหว่าง การกำกับดูแลและการบริหารจัดการ หลักการทั้งสองนี้นำไปสู่ประเภทของกิจกรรมที่แตกต่างกัน มีความต้องการการจัดโครงสร้างองค์กรที่แตกต่างกัน และใช้สำหรับจุดประสงค์ที่แตกต่างกัน ความแตกต่างที่สำคัญระหว่างการกำกับดูแลและการบริหารจัดการตามมุมมองของ COBIT 5 คือ

- **การกำกับดูแล (Governance)**

การกำกับดูแล มีเพื่อให้มั่นใจได้ว่า มีการประเมินความต้องการ เงื่อนไข และทางเลือกของผู้มีส่วนได้เสีย เพื่อกำหนดความสมดุลและความเห็นชอบร่วมกันในวัตถุประสงค์ระดับองค์กรที่ต้องการบรรลุ เพื่อกำหนดทิศทางผ่านการจัดลำดับความสำคัญและการตัดสินใจ และเพื่อการเฝ้าติดตามประสิทธิภาพในการทำงานและการปฏิบัติตามกฎระเบียบข้อบังคับให้เป็นไปตามทิศทางและวัตถุประสงค์ที่มีการตกลงร่วมกัน

ในองค์กรส่วนใหญ่ คณะกรรมการบริหารเป็นผู้รับผิดชอบในการกำกับดูแล โดยมีประธานบริษัทเป็นผู้นำ

- **การบริหารจัดการ**

ผู้บริหารวางแผน สร้าง ดำเนินงาน และเฝ้าติดตามกิจกรรมต่างๆ ให้สอดคล้องกับทิศทางที่กำหนดโดยหน่วยงานกำกับดูแล (governance body) เพื่อให้บรรลุวัตถุประสงค์ขององค์กร

ในองค์กรส่วนใหญ่ ผู้บริหารระดับสูงเป็นผู้รับผิดชอบในการบริหารจัดการ โดยมีประธานเจ้าหน้าที่บริหารเป็นผู้นำ

ความสัมพันธ์ระหว่างการกำกับดูแลและการบริหารจัดการ

จากคำนิยามของการกำกับดูแลและการบริหารจัดการ เห็นได้ชัดเจนว่าทั้งสองอย่างนี้ประกอบด้วยประเภทของกิจกรรมที่แตกต่างกัน มีหน้าที่ความรับผิดชอบที่ต่างกัน อย่างไรก็ตาม ในบทบาทของการกำกับดูแล–เพื่อการประเมิน สั่งการ และเฝ้าติดตาม–จำเป็นต้องมีปฏิสัมพันธ์กันระหว่างการกำกับดูแลและการบริหารจัดการ เพื่อให้เกิดประสิทธิภาพและประสิทธิผลในระบบการกำกับดูแล ภาพรวมของปฏิสัมพันธ์ตามโครงสร้างของปัจจัยเอื้อแสดงไว้ใน**รูปภาพที่ 14**

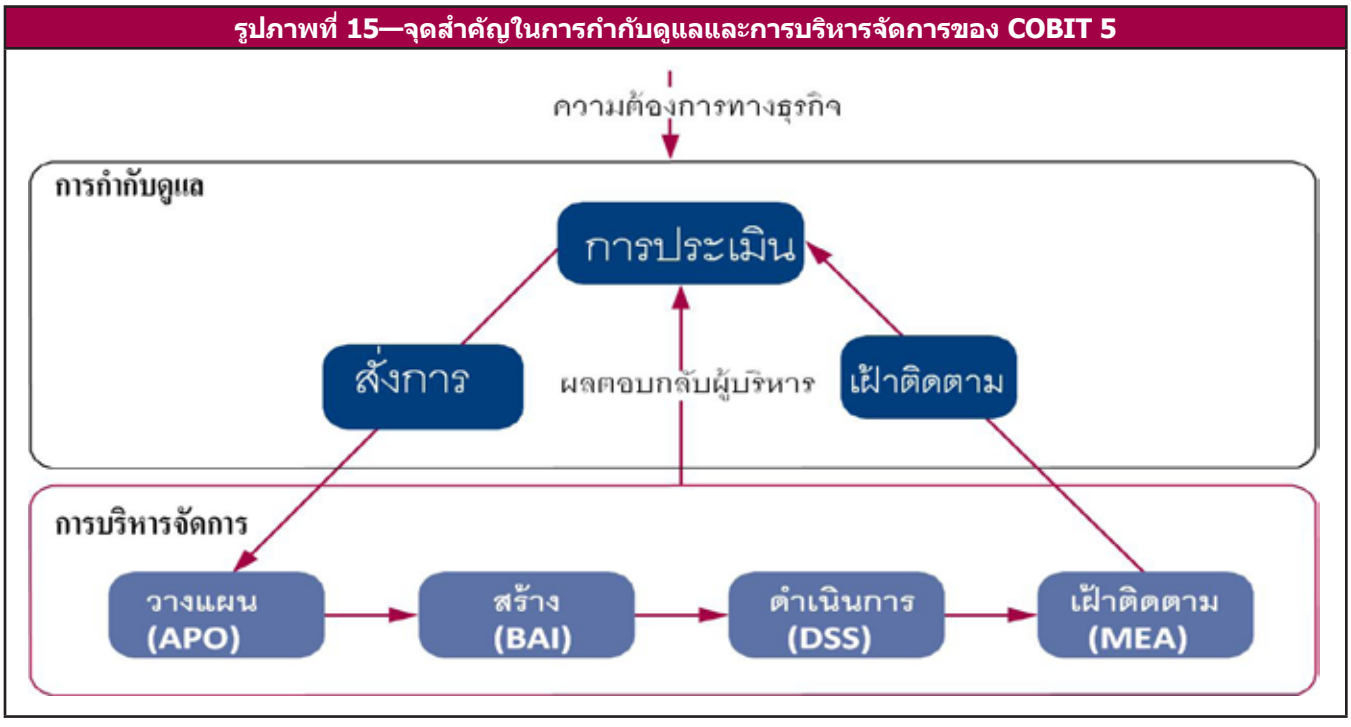
รูปภาพที่ 14—COBIT 5 ความสัมพันธ์ระหว่างการกำกับดูแลและการบริหารจัดการ

ปัจจัยเอื้อ	ปฏิสัมพันธ์ระหว่างการกำกับดูแลและการบริหารจัดการ
กระบวนการ	ในการแสดงถึงต้นแบบของกระบวนการใน COBIT 5 *(COBIT 5 : การสัมฤทธิ์ผลของกระบวนการ)* มีความแตกต่างระหว่างกระบวนการสำหรับการกำกับดูแลและกระบวนการบริหารจัดการ ซึ่งรวมถึงแนวปฏิบัติและกิจกรรมต่างๆ สำหรับแต่ละกระบวนการ ต้นแบบของกระบวนการนี้ ยังได้รวมเอาตาราง RACI ซึ่งอธิบายถึงความรับผิดชอบสำหรับตำแหน่งงานและบทบาทหน้าที่ต่างๆ ภายในองค์กร
สารสนเทศ	ต้นแบบของกระบวนการอธิบายถึง การรับข้อมูลและการส่งผลลัพธ์จากแนวปฏิบัติของกระบวนการหนึ่งไปยังกระบวนการอื่นๆ ซึ่งรวมถึงการแลกเปลี่ยนสารสนเทศกันระหว่างกระบวนการของการกำกับดูแลและการบริหารจัดการด้วย สารสนเทศที่ใช้สำหรับการประเมิน การสั่งการ และการเฝ้าติดตามไอทีระดับองค์กร ได้มีการแลกเปลี่ยนกันระหว่างการกำกับดูแลและการบริหารจัดการ ดังที่อธิบายไว้ในการรับข้อมูลและการส่งผลลัพธ์ที่อยู่ภายใต้ต้นแบบของกระบวนการ
โครงสร้างองค์กร	โครงสร้างองค์กรต่างๆ ได้ถูกกำหนดขึ้นสำหรับแต่ละองค์กร โครงสร้างองค์กรหนึ่งๆ อาจอยู่ในส่วนของการกำกับดูแลหรือของของการบริหารจัดการก็ได้ ขึ้นอยู่กับองค์ประกอบและขอบเขตในการตัดสินใจนั้นๆ เนื่องจากการกำกับดูแลเป็นเรื่องเกี่ยวกับการกำหนดทิศทาง ปฏิสัมพันธ์จึงเกิดขึ้นระหว่างการตัดสินใจที่เกิดขึ้นจากโครงสร้างในส่วนของการกำกับดูแล (ยกตัวอย่างเช่น การตัดสินใจเกี่ยวกับกลุ่มของการลงทุน (investment portfolio) การกำหนดความเสี่ยงที่ยอมรับได้) และ การนำผลการตัดสินใจไปปฏิบัติ
หลักการ นโยบาย และกรอบการดำเนินงาน	หลักการ นโยบาย และกรอบการดำเนินงาน เป็นสิ่งที่นำไปสู่การตัดสินใจด้านการกำกับดูแลให้เกิดขึ้นภายในองค์กร และด้วยเหตุผลนี้จึงเกิดปฏิสัมพันธ์ระหว่างการตัดสินใจด้านการกำกับดูแล (การกำหนดทิศทาง) และการบริหารจัดการ (การปฏิบัติตามการตัดสินใจ)
วัฒนธรรม จริยธรรม และพฤติกรรม	พฤติกรรม เป็นหนึ่งในปัจจัยเอื้อหลักสำหรับการบริหารจัดการและการกำกับดูแลที่ดีขององค์กร ซึ่งกำหนดขึ้นโดยผู้บริหารระดับสูงด้วยการปฏิบัติให้เห็นเป็นตัวอย่าง ดังนั้นพฤติกรรมจึงเป็นปฏิสัมพันธ์ที่สัมพันธ์ระหว่างการกำกับดูแลและการบริหารจัดการ
บุคลากร ทักษะ และความสามารถ	กิจกรรมต่างๆ ในการกำกับดูแลและการบริหารจัดการต้องการกลุ่มของทักษะต่างๆ ที่แตกต่างกัน แต่ทักษะที่จำเป็นสำหรับสมาชิกในหน่วยงานกำกับดูแลและผู้บริหาร คือการเข้าใจภารกิจของทั้งสองด้านและเข้าใจถึงความแตกต่างระหว่างกัน
บริการ โครงสร้างพื้นฐาน และ ระบบงาน	เราต้องการบริการซึ่งสนับสนุนโดยระบบงานและโครงสร้างพื้นฐาน เพื่อให้สารสนเทศที่เหมาะสมกับหน่วยงานกำกับดูแล และเพื่อสนับสนุนกิจกรรมการกำกับดูแลที่รวมถึงการประเมิน การกำหนดทิศทาง และการเฝ้าติดตาม

ต้นแบบอ้างอิงของกระบวนการใน COBIT 5

COBIT 5 ไม่ได้เป็นกฎตายตัว แต่สนับสนุนให้องค์กรนำกระบวนการทางด้านการกำกับดูแลและการบริหารจัดการไปใช้งานให้ครอบคลุมถึงจุดต่างๆ ที่สำคัญตามที่แสดงไว้ใน**รูปภาพที่ 15**

รูปภาพที่ 15—จุดสำคัญในการกำกับดูแลและการบริหารจัดการของ COBIT 5



องค์กรสามารถจัดให้มีกระบวนการต่างๆ ที่เห็นว่าเหมาะสม ตราบใดที่ครอบคลุมถึงวัตถุประสงค์ที่จำเป็นสำหรับการกำกับดูแลและการบริหารจัดการ ทั้งนี้ การบรรลุถึงวัตถุประสงค์เดียวกัน องค์กรขนาดเล็กอาจใช้เพียงไม่กี่กระบวนการ แต่ในองค์กรขนาดใหญ่และมีความซับซ้อนอาจจำเป็นต้องมีกระบวนการที่มากกว่า

COBIT 5 ประกอบด้วย ต้นแบบอ้างอิงของกระบวนการที่ระบุและอธิบายถึงรายละเอียดของกระบวนการสำหรับการกำกับดูแลและการบริหารจัดการ โดยแสดงถึงกระบวนการทั้งหมดซึ่งปกติมักจะพบได้ในองค์กรหนึ่งๆ ในส่วนที่เกี่ยวกับกิจกรรมทางไอที และให้ต้นแบบอ้างอิงที่สามารถใช้ร่วมกันได้ ในลักษณะที่เข้าใจง่ายสำหรับผู้จัดการทั้งด้านปฏิบัติการไอทีและด้านธุรกิจ ต้นแบบของกระบวนการที่นำเสนอนี้เป็นต้นแบบที่มีความสมบูรณ์และครอบคลุม แต่ก็ไม่ได้เป็นต้นแบบของกระบวนการเพียงอันเดียวที่ใช้ได้ องค์กรแต่ละแห่งจะต้องกำหนดกลุ่มของกระบวนการของตนขึ้นมาใช้ให้เหมาะสมกับในแต่ละสถานการณ์

การผนวกรวมรูปแบบในการดำเนินธุรกิจ (Operational model) และการใช้ภาษาสามัญเข้าไปไว้ในทุกภาคส่วนในองค์กรที่มีส่วนร่วมในกิจกรรมทางด้านไอทีเป็นก้าวสำคัญและจำเป็นที่จะนำไปสู่การกำกับดูแลที่ดี โดยให้กรอบการดำเนินงานสำหรับการวัดผลและการเฝ้าติดตามประสิทธภาพในการทำงานด้านไอที การให้ความเชื่อมั่นทางด้านไอที การสื่อสารกับผู้ให้บริการ และการบูรณาการแนวปฏิบัติที่ดีด้านการบริหารจัดการ

ต้นแบบอ้างอิงของกระบวนการใน COBIT 5 แยกการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรออกเป็นสองส่วนที่สำคัญ

- **การกำกับดูแล** ประกอบด้วย กระบวนการกำกับดูแล 5 กระบวนการ ในแต่ละกระบวนการได้มีการระบุแนวปฏิบัติสำหรับประเมิน (Evaluate) การสั่งการ (Direct) และการเฝ้าติดตาม (Monitor) (EDM)[5] เอาไว้
- **การบริหารจัดการ** ประกอบด้วย 4 โดเมนที่สอดคล้องกับความรับผิดชอบในการวางแผน (Plan) สร้าง (Build) ดำเนินการ (Run) และเฝ้าติดตาม (Monitor) (PBRM) และครอบคลุมไอทีอย่างครบวงจร โดเมนเหล่านี้มีวิวัฒนาการมาจากโดเมนและโครงสร้างของกระบวนการใน COBIT 4.1 ชื่อของโดเมนได้ตั้งให้สอดคล้องกับงานหลักที่เกี่ยวข้อง ซึ่งได้มีการเพิ่มคำกิริยาเข้าไปเป็นคำอธิบายเพิ่มเติม ดังนี้
  - จัดวางแนว (Align) จัดทำแผน (Plan) และจัดระบบ (Organise) (APO)
  - จัดสร้าง (Build) จัดหา (Acquire) และนำไปใช้ (Implement) (BAI)
  - ส่งมอบ (Deliver) ให้บริการ (Service) และสนับสนุน (Support) (DSS))
  - เฝ้าติดตาม (Monitor) วัดผล (Evaluate) และประเมิน (Assess) (MEA)

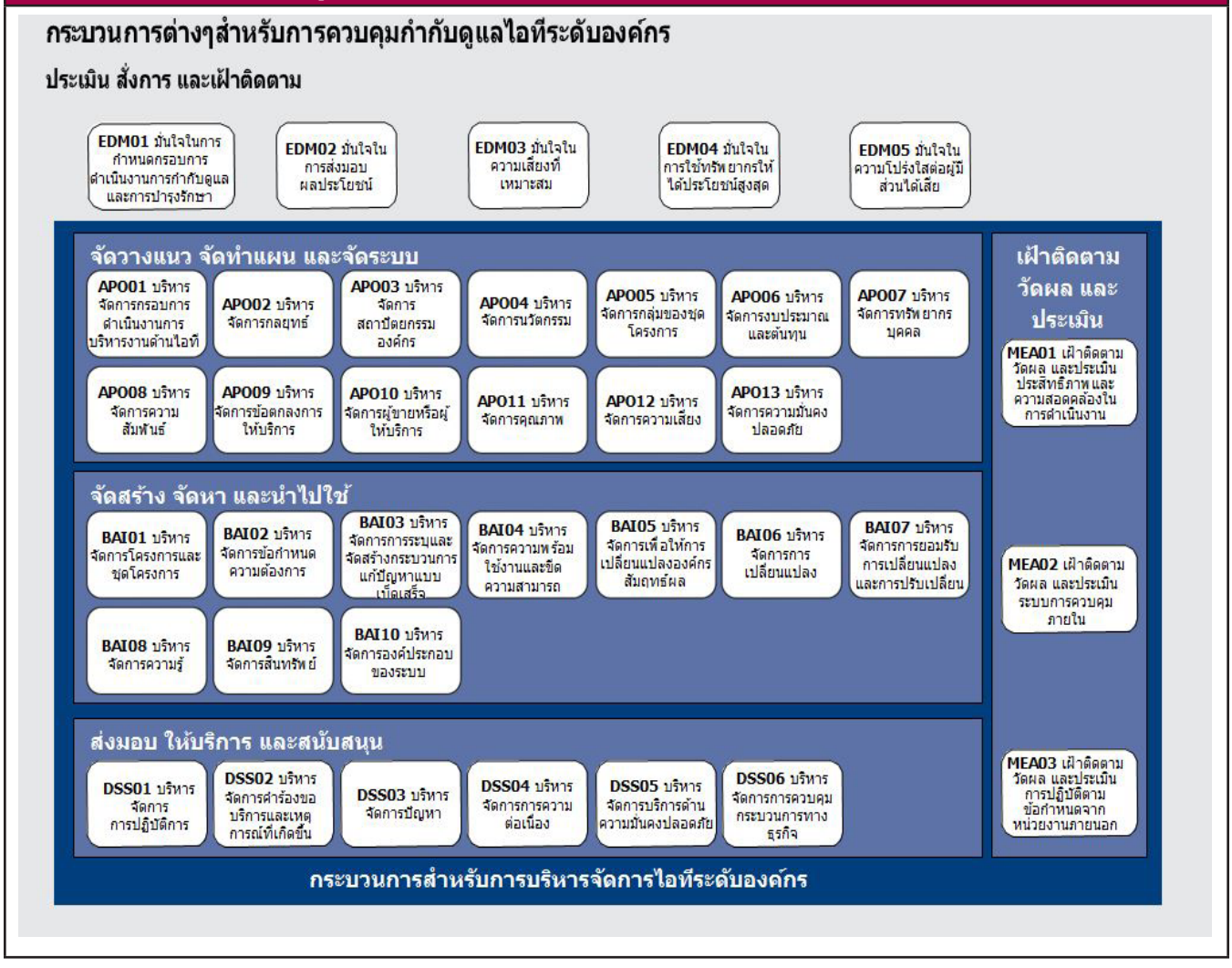
[5] ในบริบทของโดเมนการกำกับดูแล คำว่า "เฝ้าติดตาม" หมายถึง กิจกรรมต่างๆ ที่ทำให้หน่วยงานกำกับดูแลทราบได้ว่าผู้บริหารได้ดำเนินงานไปจริงตามทิศทางที่ได้กำหนดไว้ให้มากน้อยเพียงใด

แต่ละโดเมนประกอบด้วยกระบวนการต่างๆ ทั้งนี้ ตามที่ได้อธิบายไปแล้วก่อนหน้านี้ แม้ว่ากระบวนการส่วนใหญ่ต่างก็มีกิจกรรมในการ 'วางแผน' 'นำไปใช้' 'ปฏิบัติการ' และ 'เฝ้าติดตาม' ภายในกระบวนการนั้นๆ หรือภายใต้ประเด็นปัญหาเฉพาะทางที่ได้รับการหยิบยกขึ้นมา (อาทิเช่น ด้านคุณภาพ ด้านความมั่นคงปลอดภัย เป็นต้น) แต่กิจกรรมต่างๆ เหล่านั้นถูกจัดเข้าไปไว้ในแต่ละโดเมนตามความเกี่ยวเนื่องโดยส่วนใหญ่ของกิจกรรมในแต่ละด้าน ตามมุมมองของไอทีในระดับองค์กร

ต้นแบบอ้างอิงของกระบวนการใน COBIT 5 พัฒนาต่อจากต้นแบบของกระบวนการใน COBIT 4.1 และได้บูรณาการเอาต้นแบบกระบวนการใน Risk IT และ Val IT เข้าไปไว้ด้วย

รูปภาพที่ 16 แสดงภาพที่ครบชุดของกระบวนการสำหรับการกำกับดูแลและการบริหารจัดการ 37 กระบวนการใน COBIT 5 รายละเอียดของกระบวนการทั้งหมดตามที่กล่าวไว้ข้างต้นจะได้รวบรวมไว้ในเอกสาร *COBIT 5: การสัมฤทธิ์ผลของกระบวนการ*.

รูปภาพที่ 16—ต้นแบบอ้างอิงของกระบวนการใน COBIT 5



หน้านี้เป็นหน้าว่าง

บทที่ 7
แนวทางในการนำไปใช้งาน

บทนำ

คุณค่าที่เหมาะสมที่สุดจะสามารถเกิดขึ้นได้ด้วยการใช้ประโยชน์จาก COBIT โดยจะต้องรับมาและปรับใช้อย่างมีประสิทธิผลให้เหมาะสมกับสภาพแวดล้อมที่แตกต่างกันของแต่ละองค์กรเท่านั้น วิธีปฏิบัติสำหรับการนำไปใช้งานแต่ละวิธีจำเป็นต้องสามารถจัดการกับเรื่องท้าทาย และรวมถึงการบริหารการเปลี่ยนแปลงด้านวัฒนธรรมและพฤติกรรมอีกด้วย

ISACA ได้ให้แนวทางสำหรับการนำไปใช้งาน (implementation guideline) ที่ครอบคลุมและสามารถนำไปปฏิบัติได้จริงในเอกสารฉบับที่ชื่อว่า *การนำ COBIT 5 ไปใช้งาน (COBIT 5 Implementation)*[6] ซึ่งตั้งอยู่บนพื้นฐานของวัฏจักรการปรับปรุงอย่างต่อเนื่อง ทั้งนี้ เอกสารฉบับนี้ไม่ได้จัดทำขึ้นเพื่อเป็นวิธีปฏิบัติที่ตายตัวหรือเป็นกระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จที่สมบูรณ์ แต่ออกแบบมาเพื่อเป็นแนวทางในการหลีกเลี่ยงการเผชิญกับอันตรายแอบแฝงที่มักจะพบอยู่เป็นปกติ เพื่อใช้ประโยชน์จากแนวปฏิบัติที่ดี และเพื่อช่วยให้เกิดผลสำเร็จ แนวทางเหล่านี้ได้รับการสนับสนุนจากชุดคู่มือพร้อมใช้สำหรับการนำไปใช้งาน (implementation tool kit) อันประกอบด้วยทรัพยากรต่างๆ ที่จะได้รับการพัฒนาให้ดีขึ้นอย่างต่อเนื่อง ประกอบด้วย
- การประเมินตนเอง การวัดผล และเครื่องมือในการวิเคราะห์
- การนำเสนอที่พุ่งเป้าไปถึงผู้รับสารที่หลากหลาย
- บทความต่างๆ ที่เกี่ยวข้อง และคำอธิบายเพิ่มเติม

วัตถุประสงค์ของบทนี้ ได้แก่การแนะนำภาพรวมสำหรับวัฏจักรของการนำไปใช้และการปรับปรุงอย่างต่อเนื่อง และเน้นหัวข้อที่สำคัญจำนวนหนึ่งจากเอกสาร*การนำ COBIT 5 ไปใช้งาน* เช่น
- การจัดทำเหตุผลทางธุรกิจเพื่อสนับสนุนการนำการกำกับดูแลและการบริหารจัดการด้านไอทีไปใช้และการปรับปรุงให้ดีขึ้น
- การรับรู้ถึงจุดที่มีปัญหา (pain point) และเหตุการณ์จุดชนวน (trigger events)
- การสร้างสภาพแวดล้อมที่เหมาะสมสำหรับการนำไปใช้งาน
- ใช้ประโยชน์จาก COBIT ในการระบุถึงช่องว่างและแนวทางการพัฒนาปัจจัยเอื้อ อาทิเช่น นโยบาย กระบวนการหลักการ โครงสร้างองค์กร บทบาทและหน้าที่ความรับผิดชอบ

ข้อควรพิจารณาในบริบทขององค์กร

การกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรไม่ได้เกิดขึ้นจากสุญญากาศ ทุกองค์กรต้องออกแบบแผนการนำไปใช้หรือแผนการทำงานเพื่อให้บรรลุเป้าหมาย (Road map) ที่สอดคล้องกับปัจจัยที่เป็นสภาพแวดล้อมเฉพาะขององค์กรทั้งภายในและภายนอก ยกตัวอย่างเช่น
- จริยธรรมและวัฒนธรรม
- กฎหมายที่เกี่ยวข้อง ระเบียบข้อบังคับ และนโยบาย
- ภารกิจ วิสัยทัศน์ และคุณค่า
- นโยบายและแนวปฏิบัติด้านการกำกับดูแล
- แผนธุรกิจและกลยุทธ์ที่ตั้งไว้
- ต้นแบบสำหรับปฏิบัติงานและระดับวุฒิภาวะ
- รูปแบบ (Style) ในการบริหารจัดการ
- ความเสี่ยงที่ยอมรับได้
- ความสามารถและความพร้อมของทรัพยากร
- แนวปฏิบัติเฉพาะประเภทธุรกิจ

สิ่งที่สำคัญไม่ยิ่งหย่อนกว่ากันคือ การใช้ประโยชน์จากปัจจัยเอื้อและสร้างปัจจัยเอื้อเพิ่มจากที่มีอยู่แล้วสำหรับการกำกับดูแลในระดับองค์กร

วิธีปฏิบัติที่เหมาะสมอาจแตกต่างกันไปในแต่ละองค์กรสำหรับการกำกับดูแลและบริหารจัดการไอทีระดับองค์กร ซึ่งจะต้องทำความเข้าใจและพิจารณาถึงสภาพแวดล้อมก่อนที่จะรับ COBIT มาปรับใช้ให้มีประสิทธิผลในการนำปัจจัยเอื้อมาไปใช้งานสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร COBIT มักอ้างถึงกรอบการดำเนินงาน แนวปฏิบัติที่ดี และมาตรฐานอื่นๆ ด้วย สิ่งเหล่านี้ก็จะต้องนำมาประยุกต์ให้เข้ากับความต้องการเฉพาะองค์กรเช่นกัน

ปัจจัยหลักสู่ความสำเร็จที่จะช่วยให้การนำไปใช้งานประสบผลสำเร็จประกอบด้วย
- ผู้บริหารระดับสูงเป็นผู้ให้ทิศทางและสั่งการสำหรับการริเริ่มดำเนินงาน (initiatives) พร้อมกับให้คำมั่นและการสนับสนุนที่ต่อเนื่องอย่างชัดเจน
- ทุกภาคส่วนที่สนับสนุนกระบวนการกำกับดูแลและบริหารจัดการ มีความเข้าใจในวัตถุประสงค์ทั้งทางด้านธุรกิจและด้านไอที

[6] www.isaca.org/cobit

- ทำให้แน่ใจได้ว่ามีการสื่อสารที่มีประสิทธิผลและสามารถทำให้เกิดการเปลี่ยนแปลงที่จำเป็น
- ปรับใช้ COBIT และแนวปฏิบัติที่ดีและมาตรฐานที่สนับสนุนอื่นๆ ให้เหมาะสมกับบริบทเฉพาะขององค์กร
- มุ่งเน้นการแก้ปัญหาที่ทำได้เร็ว (Quick win) และให้ความสำคัญในลำดับต้นสำหรับการปรับปรุงที่ให้ประโยชน์สูงสุดซึ่งสามารถนำไปใช้งานจริงได้ง่าย

การสร้างสภาพแวดล้อมที่เหมาะสม

เป็นสิ่งสำคัญสำหรับการริเริ่มดำเนินการเพื่อการนำไปใช้โดยใช้ประโยชน์จาก COBIT ที่จะต้องมีการกำกับดูแลอย่างถูกต้องและบริหารจัดการอย่างเหมาะสม การริเริ่มดำเนินการ (initiatives) ที่เกี่ยวข้องกับไอทีที่สำคัญ มักประสบความล้มเหลวเนื่องจากไม่ได้กำหนดทิศทางที่เหมาะสม ขาดการสนับสนุนและดูแลจากผู้มีส่วนได้เสียต่างๆ การจัดให้มีการกำกับดูแลและการบริหารจัดการสำหรับปัจจัยเอื้อทางด้านไอทีโดยใช้ประโยชน์จาก COBIT ก็เช่นเดียวกัน การสนับสนุนและการให้ทิศทางจากผู้มีส่วนได้เสียหลักเป็นเรื่องจำเป็นเพื่อให้การปรับปรุงได้รับมาใช้อย่างยั่งยืน ยิ่งในสภาพแวดล้อมขององค์กรที่อ่อนแอ (เช่น รูปแบบการดำเนินงานไม่ชัดเจน หรือขาดปัจจัยเอื้อด้านการกำกับดูแลระดับองค์กรที่ชัดเจน) การสนับสนับสนุนและการมีส่วนร่วมจากผู้มีส่วนได้เสียก็ยิ่งมีความสำคัญมากขึ้น

ปัจจัยเอื้อที่ใช้ประโยชน์จาก COBIT ควรจะให้กระบวนการแก้ปัญหาแบบเบ็ดเสร็จ (solution) ที่สามารถจะจัดการกับความต้องการและประเด็นปัญหาของธุรกิจได้อย่างแท้จริงมากกว่าที่จะใช้ COBIT เป็นผลลัพธ์สุดท้าย ควรมีการระบุถึงความต้องการที่มาจากจุดที่มีปัญหา(pain point) และปัจจัยขับเคลื่อน (driver) ซึ่งฝ่ายบริหารยอมรับว่าเป็นจุดที่จำเป็นต้องจัดการ การตรวจสอบสถานะในภาพรวม (high level health check) การวินิจฉัย หรือการประเมินความสามารถตาม COBIT เป็นเครื่องมือที่ดีในการสร้างความตระหนัก นำไปสู่ความเห็นชอบร่วมกัน และก่อให้เกิดการให้คำมั่นที่จะดำเนินการ ผู้มีส่วนได้เสียที่เกี่ยวข้องควรให้คำมั่นและความเห็นชอบตั้งแต่เริ่มต้น ซึ่งในการที่จะบรรลุถึงสิ่งเหล่านี้ จะต้องกำหนดวัตถุประสงค์ของการนำไปใช้งานและผลประโยชน์ที่ต้องการอย่างชัดเจนในมุมมองทางธุรกิจ และสรุปไว้เป็นหัวข้อหนึ่งในเหตุผลทางธุรกิจ

เมื่อได้รับคำมั่นแล้ว ควรจัดสรรทรัพยากรที่จำเป็นเพื่อสนับสนุนชุดโครงการต่างๆ (programme) และควรกำหนดและมอบหมายบทบาทหน้าที่และความรับผิดชอบที่เป็นหลักสำหรับชุดโครงการ ควรให้ความใส่ใจอย่างต่อเนื่องที่จะรักษาคำมั่นจากผู้มีส่วนได้เสียที่ได้รับผลกระทบ

ควรจัดทำและดูแลรักษาโครงสร้างและกระบวนการที่เหมาะสมในการควบคุมดูแลและกำหนดทิศทาง โครงสร้างและกระบวนการเหล่านี้ควรจะให้ความมั่นใจได้ว่า วิธีปฏิบัติในการกำกับดูแลและการบริหารจัดการความเสี่ยงทั่วทั้งองค์กรเป็นไปในทิศทางที่สอดคล้องกันอยู่เสมอ

ผู้มีส่วนได้เสียหลัก เช่น คณะกรรมการบริหาร และผู้บริหารระดับสูง จะต้องให้การสนับสนุนและให้คำมั่นที่เห็นได้อย่างชัดเจน เพื่อกำหนดเป็นแนวทางจากผู้บริหารระดับสูง และเพื่อให้มั่นใจว่าจะได้รับคำมั่นจากเจ้าหน้าที่ในทุกระดับสำหรับการดำเนินงานตามชุดโครงการต่างๆ

การรับรู้จุดที่มีปัญหาและเหตุการณ์จุดชนวน

มีปัจจัยจำนวนมากที่อาจจะชี้ให้เห็นถึงความจำเป็นที่จะต้องปรับปรุงการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

จากการใช้จุดที่มีปัญหาและเหตุการณ์จุดชนวนให้เป็นจุดเริ่มต้นในการริเริ่มดำเนินการเพื่อการนำไปใช้ จะทำให้เหตุผลทางธุรกิจที่ใช้สนับสนุนการปรับปรุงการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรสามารถเชื่อมโยงได้กับประเด็นปัญหาที่ประสบอยู่จริงในการปฏิบัติงานประจำวัน โดยจะช่วยให้เกิดการยอมรับได้ดีขึ้นและทำให้คนในองค์กรรู้สึกถึงความจำเป็นที่จะต้องเร่งรีบเริ่มต้นการนำไปใช้ นอกจากนี้ ยังช่วยให้สามารถระบุได้ถึงการแก้ปัญหาที่ทำได้เร็วและสามารถแสดงถึงมูลค่าเพิ่มในจุดเหล่านั้นให้เห็นและรับรู้ได้อย่างชัดเจนที่สุดในองค์กร สิ่งเหล่านี้จะเป็นพื้นฐานในการนำเสนอการเปลี่ยนแปลงเพิ่มเติมต่อไป และสามารถช่วยให้ได้รับคำมั่นและการสนับสนุนจากผู้บริหารอาวุโสในวงกว้าง

ตัวอย่างของจุดที่มีปัญหาที่มักเกิดขึ้น ที่การสร้างหรือปรับปรุงการกำกับดูแลและการบริหารจัดการปัจจัยเอื้อด้านไอทีอาจสามารถใช้เป็นกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ (หรือบางส่วน) สำหรับจุดที่มีปัญหาดังกล่าวได้ ตามที่ระบุไว้ใน *การนำ COBIT 5 ไปใช้งาน* ได้แก่

- ความไม่พอใจต่อการริเริ่มดำเนินการที่ล้มเหลว ต้นทุนด้านไอทีที่สูงขึ้น และความรู้สึกว่าคุณค่าของธุรกิจลดลง
- เหตุการณ์ที่มีนัยสำคัญเกี่ยวกับความเสี่ยงด้านไอที เช่น ข้อมูลสูญหาย หรือ โครงการล้มเหลว
- ปัญหาการส่งมอบผลงานจากผู้ให้บริการภายนอก เช่น ความล้มเหลวในการให้บริการตามระดับที่ตกลงกันไว้อย่างต่อเนื่อง
- ความล้มเหลวที่จะปฏิบัติตามข้อกำหนดของกฎระเบียบข้อบังคับและสัญญา
- ไอทีจำกัดความคิดสร้างสรรค์และความคล่องตัวในการดำเนินธุรกิจขององค์กร
- มีประเด็นที่พบจากการตรวจสอบอยู่เป็นประจำ เกี่ยวกับปัญหาประสิทธิภาพด้านไอที หรือ รายงานเกี่ยวกับปัญหาคุณภาพของการให้บริการด้านไอที
- มีค่าใช้การจ่ายด้านไอทีที่ปิดบังไว้ หรือใช้ในทางที่ไม่ถูกต้อง
- มีการทับซ้อนหรือซ้ำซ้อนกันระหว่างการริเริ่มดำเนินการกับการสูญเสียทรัพยากร เช่น การยกเลิกโครงการก่อนกำหนด ทรัพยากรด้านไอทีไม่เพียงพอ บุคลากรขาดทักษะที่เหมาะสม หรือบุคลากรเหนื่อยล้า/ไม่พอใจ

- การเปลี่ยนแปลงที่มีไอทีเป็นปัจจัยเอื้อ ไม่สามารถบรรลุถึงความต้องการทางธุรกิจ และส่งมอบล่าช้าหรือเกินงบประมาณ
- กรรมการบริหาร ผู้บริหารระดับสูง หรือผู้จัดการอาวุโสไม่เต็มใจที่จะมีส่วนร่วมในไอทีหรือขาดผู้ให้การสนับสนุนจากภาคธุรกิจที่จะให้คำมั่น (Commitment) และมีความพอใจกับบริการ
- ต้นแบบสำหรับการปฏิบัติงานด้านไอทีมีความซับซ้อน

นอกจากจุดที่มีปัญหาข้างต้นแล้ว เหตุการณ์อื่นๆ ในสภาพแวดล้อมทั้งภายในและภายนอกองค์กรก็สามารถส่งสัญญาณ หรือกระตุ้นให้องค์กรหันมาให้ความสนใจกับการกำกับดูแลและการบริหารจัดการด้านไอทีได้ ตัวอย่างจากบทที่ 3 ของเอกสาร *การนำ COBIT 5 ไปใช้งาน (COBIT 5 implementation)* ประกอบด้วย

- การควบรวมกิจการ การซื้อกิจการ และการขายกิจการ
- การเปลี่ยนแปลงในการตลาด เศรษฐกิจ และการแข่งขัน
- การเปลี่ยนแปลงในต้นแบบการปฏิบัติงานทางธุรกิจเป็น รูปแบบการดำเนินธุรกิจตลอดจนวิธีหรือแหล่งที่ใช้ในการจัดซื้อจัดหา (sourcing arrangement)
- กฎระเบียบข้อบังคับหรือข้อกำหนดที่ต้องปฏิบัติตามที่ออกมาใหม่
- การเปลี่ยนแปลงด้านไอทีที่มีนัยสำคัญ หรือการปรับเปลี่ยนกระบวนทัศน์ (Paradigm Shift)
- การให้ความสนใจเป็นพิเศษกับการกำกับดูแลทั่วทั้งองค์กรหรือโครงการด้านการกำกับดูแลทั่วทั้งองค์กร
- การเปลี่ยนประธานเจ้าหน้าที่บริหาร (CEO) ผู้บริหารสูงสุดด้านการเงิน (CFO) ผู้บริหารสูงสุดด้านสารสนเทศ (CIO) หรือผู้บริหารคนอื่นๆ
- การประเมินจากผู้ตรวจสอบภายนอก หรือที่ปรึกษา
- แผนกลยุทธ์หรือการจัดลำดับความสำคัญใหม่ของธุรกิจ

การเอื้อให้เกิดการเปลี่ยนแปลง

การนำไปใช้จะประสบความสำเร็จได้ก็ขึ้นอยู่กับการทำให้เกิดการเปลี่ยนแปลงที่เหมาะสมอย่างถูกวิธี (ปัจจัยเอื้อด้านการกำกับดูแลและการบริหารจัดการที่เหมาะสม) ในหลายองค์กรได้มุ่งเน้นไปที่มุมมองแรก—แก่นของการกำกับดูแลและการบริหารจัดการด้านไอที—เป็นสำคัญ แต่กลับละเลยมุมมองของการบริหารจัดการบุคคลากร พฤติกรรม และวัฒนธรรมสำหรับการเปลี่ยนแปลง และการจูงใจให้ผู้มีส่วนได้เสียยอมรับการเปลี่ยนแปลง

เราไม่ควรที่จะอุปมานว่า ผู้มีส่วนได้ส่วนเสียต่างๆ ที่มีส่วนร่วมหรือได้รับผลกระทบจากปัจจัยเอื้อที่เกิดขึ้นใหม่หรือที่ได้รับการปรับปรุงจะพร้อมยอมรับกับการเปลี่ยนแปลงและรับมาใช้ โอกาสที่จะละเลย และ/หรือต่อต้านการเปลี่ยนแปลง จะต้องได้รับการจัดการด้วยวิธีปฏิบัติที่เป็นแบบแผนและเชิงรุก (proactive) นอกจากนี้ การรับรู้ถึงความเป็นไปต่างๆ ในชุดโครงการสำหรับการนำไปใช้ในระดับที่เหมาะสมสามารถเกิดขึ้นได้จากแผนการสื่อสารที่ระบุถึงสิ่งที่จะต้องสื่อสาร วิธีการสื่อสาร และผู้ที่จะได้รับการสื่อสาร ตลอดระยะต่างๆ ของชุดโครงการ

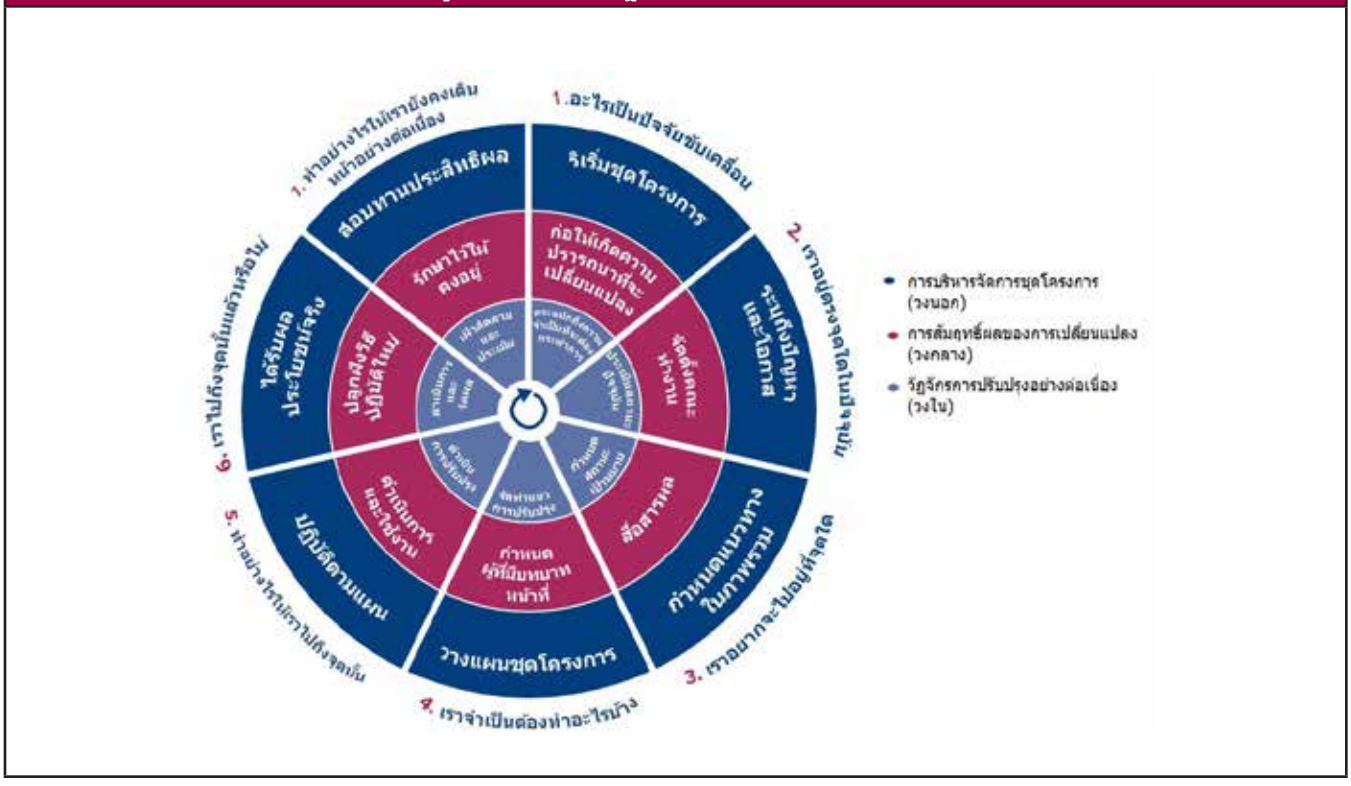
การปรับปรุงอย่างยั่งยืนสามารถบรรลุได้ 2 ทาง ทางหนึ่งคือการได้มาซึ่งคำมั่นจากผู้มีส่วนได้เสีย (ความพยายามในการที่จะชนะใจ ในการได้เวลาจากผู้นำ และในการสื่อสารและตอบสนองต่อผู้ปฏิบัติงาน) หรืออีกทางหนึ่งหากยังจำเป็น คือการบังคับให้ปฏิบัติตาม (ความพยายามในกระบวนการที่จะบริหารจัดการ เฝ้าติดตาม และบังคับใช้) พูดอีกนัยหนึ่งคือ ต้องเอาชนะอุปสรรคด้านบุคคลากร พฤติกรรม และวัฒนธรรม เพื่อให้เกิดความเห็นพ้องต้องกันในการรับการเปลี่ยนแปลงมาใช้อย่างเหมาะสม ปลูกฝังความพยายามที่จะรับการเปลี่ยนแปลงมาใช้ และให้แน่ใจถึงความสามารถในการรับการเปลี่ยนแปลงมาใช้

วิธีปฏิบัติแบบวัฏจักร (a life cycle approach)

วัฏจักรของการนำไปใช้งาน ให้แนวทางสำหรับองค์กรในการใช้ COBIT ที่จะจัดการกับความซับซ้อนและความท้ายทายที่จะเผชิญในระหว่างการนำไปใช้งาน มีองค์ประกอบของวงจรชีวิตที่สัมพันธ์กัน 3 ส่วนคือ
1. แก่นของวัฏจักรที่ปรับปรุงให้ดีขึ้นอย่างต่อเนื่อง – ไม่ใช่แค่โครงการที่เกิดขึ้นแล้วจบ
2. เอื้อให้เกิดการเปลี่ยนแปลง – เน้นที่มุมมองด้านพฤติกรรมและวัฒนธรรม
3. การบริหารจัดการชุดโครงการ (programme)

ดังที่ได้อธิบายไปแล้ว การมีสภาพแวดล้อมที่เหมาะสมจะช่วยให้มั่นใจว่า การริเริ่มดำเนินการเพื่อการนำไปใช้หรือเพื่อการปรับปรุงจะประสบความสำเร็จ วัฏจักรที่แบ่งออกเป็น 7 ระยะได้แสดงไว้ใน**รูปภาพที่ 17**

รูปภาพที่ 17—วัฏจักรการนำไปใช้ 7 ระยะ



ระยะที่ 1 เริ่มต้นจากการตระหนักและเห็นพ้องต้องกันถึงความจำเป็นของการริเริ่มดำเนินการเพื่อการนำไปใช้หรือเพื่อการปรับปรุง ซึ่งระบุถึงจุดที่มีปัญหาและตัวจุดชนวน (trigger) ในปัจจุบัน และการสร้างความปรารถนาที่จะทำให้เกิดการเปลี่ยนแปลงในกลุ่มผู้บริหารระดับสูง

ระยะที่ 2 มุ่งไปที่การระบุถึงขอบเขตของการริเริ่มดำเนินการเพื่อการนำไปใช้หรือเพื่อการปรับปรุงจะประสบความสำเร็จ โดยใช้การเทียบเป้าหมายในระดับองค์กร กับเป้าหมายที่เกี่ยวข้องกับไอที และกับกระบวนการทางไอทีที่เกี่ยวข้องของ COBIT 5 และพิจารณาว่าความเสี่ยงในสถานการณ์ต่างๆ (risk scenarios) จะช่วยให้สามารถระบุถึงกระบวนการหลักที่ควรให้ความสนใจ การวินิจฉัยในภาพรวมยังมีประโยชน์ในการกำหนดขอบเขตและเข้าใจถึงเรื่องที่มีความสำคัญเร่งด่วนที่จะต้องให้ความสนใจ จากนั้นจะประเมินภาวะปัจจุบันและระบุถึงประเด็นปัญหาหรือข้อบกพร่องโดยกระบวนการประเมินความสามารถ การริเริ่มดำเนินการที่มีขนาดใหญ่ควรจัดเป็นโครงสร้างที่แบ่งออกเป็นการดำเนินตามวัฏจักรหลายๆ รอบ เช่น การริเริ่มดำเนินการที่นานเกินกว่า 6 เดือนซึ่งมีความเสี่ยงที่จะสูญเสียแรงกระตุ้น ความสนใจ และการยอมรับจากผู้มีส่วนได้เสียได้

ระยะที่ 3 มีการกำหนดเป้าหมายในการปรับปรุง ตามมาด้วย การวิเคราะห์ในรายละเอียดที่ใช้แนวทางของ COBIT ในการระบุช่องว่างและกระบวนการแก้ปัญหาแบบเบ็ดเสร็จที่อาจเป็นไปได้ กระบวนการแก้ปัญหาแบบเบ็ดเสร็จบางอย่างอาจเป็นการแก้ปัญหาได้อย่างรวดเร็ว แต่บางอย่างก็อาจมีความท้าทายมากกว่าและดำเนินกิจกรรมที่ยาวนานกว่า เราควรให้ความสำคัญกับการริเริ่มดำเนินการที่สำเร็จได้ง่ายและน่าจะให้ผลที่เป็นประโยชน์สูงสุดก่อน

ระยะที่ 4 วางแผนกระบวนการแก้ปัญหาแบบเบ็ดเสร็จที่นำไปปฏิบัติได้จริง โดยกำหนดโครงการที่มีเหตุผลทางธุรกิจที่สมเหตุสมผลรองรับขึ้นมาดำเนินการ มีการจัดทำแผนรองรับการเปลี่ยนแปลงสำหรับการนำไปใช้ เหตุผลทางธุรกิจที่จัดทำขึ้นมาอย่างดีจะช่วยให้มั่นใจว่า มีการระบุถึงและเฝ้าติดตามผลประโยชน์ที่ต้องการได้รับจากโครงการ

ระยะที่ 5 กระบวนการแก้ปัญหาแบบเบ็ดเสร็จที่นำเสนอจะได้รับการนำไปใช้ในการดำเนินงานประจำวัน กำหนดให้มีการวัดผลและจัดให้มีการเฝ้าติดตามโดยใช้เป้าหมายและมาตรวัดของ COBIT เพื่อให้มั่นใจถึงการมีและการรักษาไว้ซึ่งความสอดคล้องกันทางธุรกิจ และสามารถวัดประสิทธิภาพในการทำงานได้ ความสำเร็จต้องการการมีส่วนร่วมและการแสดงถึงคำมั่นจากผู้บริหารระดับสูง พร้อมทั้งจิตสำนึกในความเป็นเจ้าของจากผู้มีส่วนได้เสียทั้งทางธุรกิจและด้านไอที

ระยะที่ 6 มุ่งไปที่การดำเนินงานอย่างยั่งยืนของปัจจัยเอื้อ ทั้งปัจจัยเอื้อที่เกิดขึ้นใหม่หรือที่ได้รับการปรับปรุง และการเฝ้าติดตามการบรรลุถึงผลประโยชน์ที่คาดหวัง

ระยะที่ 7 สอบทานความสำเร็จของการริเริ่มดำเนินการในภาพรวม ระบุถึงการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่ควรมีเพิ่มเติม และสนับสนุนให้มีการพัฒนาอย่างต่อเนื่อง

เมื่อเวลาผ่านไป วัฏจักรนี้จะเกิดขึ้นหลายๆ รอบ ซึ่งในขณะเดียวกันก็ช่วยสร้างวิธีปฏิบัติที่ยั่งยืนให้กับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

เริ่มต้น: สร้างเหตุผลทางธุรกิจ

เพื่อให้แน่ใจได้ว่า การริเริ่มดำเนินการเพื่อการนำไปใช้โดยใช้ประโยชน์จาก COBIT จะประสบความสำเร็จ ทุกคนในองค์กรจะต้องตระหนักและได้รับการสื่อสารให้ทราบถึงสิ่งที่จำเป็นต้องทำ โดยอาจจะอยู่ในรูปแบบของการกระตุ้นเตือน (ในจุดที่เคยมีปัญหามาก่อน ตามที่กล่าวไว้ข้างต้น) หรือการแสดงให้เห็นถึงโอกาสในการปรับปรุง และที่สำคัญมากคือผลประโยชน์ที่จะได้รับ ปลูกฝังให้สำนึกถึงระดับของความเร่งด่วนที่เหมาะสม (ที่จะต้องดำเนินการ) และผู้มีส่วนได้เสียหลักควรตระหนักถึงความเสี่ยงหากไม่มีการดำเนินการใดๆ และประโยชน์ที่จะได้รับจากการดำเนินชุดโครงการ

การริเริ่มดำเนินการควรมีผู้สนับสนุนเป็นเจ้าของ ให้ผู้มีส่วนได้เสียหลักทั้งหมดมีส่วนร่วม และมีเหตุผลทางธุรกิจรองรับ ในขั้นต้นอาจเริ่มที่ภาพรวมจากมุมมองด้านกลยุทธ์ – จากผู้บริหารลงมา – เริ่มจากการทำความเข้าใจให้ชัดเจนถึงผลลัพธ์ทางธุรกิจที่ต้องการ แล้วค่อยๆ เพิ่มคำอธิบายรายละเอียดเข้าไปงานที่มีความสำคัญ พร้อมทั้งกำหนดจุดชี้วัดความก้าวหน้าในแต่ระยะและบทบาทหน้าที่ความรับผิดชอบ เหตุผลทางธุรกิจเป็นเครื่องมือที่มีประโยชน์สำหรับผู้บริหารในการให้แนวทางเพื่อสร้างคุณค่าทางธุรกิจ อย่างน้อยเหตุผลทางธุรกิจควรรวมถึงเรื่องต่อไปนี้

- ผลประโยชน์ทางธุรกิจที่ตั้งเป้าไว้ ความสอดคล้องกับกลยุทธ์ทางธุรกิจ และผู้เป็นเจ้าของผลประโยชน์ที่เกี่ยวข้อง (หรืออีกนัยหนึ่งคือบุคคลที่จะต้องรับผิดชอบในการรักษาผลประโยชน์) ซึ่งอาจมาจากจุดที่มีปัญหาและเหตุการณ์จุดชนวนต่างๆ
- การเปลี่ยนแปลงทางธุรกิจต้องสร้างคุณค่าที่มองเห็นได้ โดยอาจมาจากการตรวจสอบสถานะ (health check) การวิเคราะห์ช่องว่างในความสามารถ (capability gap analyses) และควรระบุได้อย่างชัดเจนว่า อะไรที่อยู่ในขอบเขต และอะไรที่ไม่อยู่ในขอบเขตของการเปลี่ยนแปลงนี้
- การลงทุนที่จำเป็นเพื่อให้เกิดการเปลี่ยนแปลงในการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร (ประมาณจากความจำเป็นที่ต้องมีโครงการต่างๆ)
- ต้นทุนการดำเนินงานทั้งด้านไอทีและธุรกิจ
- ผลประโยชน์ที่คาดหวังจากการดำเนินงานหลังจากการเปลี่ยนแปลง
- ความเสี่ยงที่สืบเนื่องมาจากหัวข้อต่างๆ ข้างต้น ซึ่งรวมถึงข้อจำกัดหรือภาวะที่ต้องขึ้นอยู่กับปัจจัยอื่น (dependencies) (บนพื้นฐานของความท้าทายและปัจจัยแห่งความสำเร็จ)
- บทบาทหน้าที่ ความรับผิดชอบ และความรับผิดชอบในผลงาน (accountability) ที่เกี่ยวข้องกับการริเริ่มดำเนินการนั้น
- จะเฝ้าติดตามการลงทุนและการสร้างคุณค่าตลอดอายุการใช้งานเชิงเศรษฐกิจได้อย่างไร และจะใช้อะไรเป็นมาตรวัด (บนพื้นฐานของเป้าหมายและมาตรวัด)

เหตุผลทางธุรกิจไม่ใช่เอกสารที่ทำครั้งเดียวจบ แต่เป็นเครื่องมือในการปฏิบัติงานที่ต้องได้รับการปรับปรุงให้เป็นปัจจุบันอย่างต่อเนื่อง เพื่อสะท้อนถึงภาพในอนาคตณ ปัจจุบัน ให้เห็นได้ว่าชุดโครงการสามารถดำเนินต่อไปได้

อาจเป็นเรื่องยากที่จะวัดผลประโยชน์ในเชิงปริมาณจากการริเริ่มดำเนินการเพื่อการนำไปใช้หรือเพื่อการปรับปรุง และควรระวังที่จะตกลงเฉพาะสำหรับผลประโยชน์ที่สมเหตุสมผลและสามารถเกิดขึ้นได้จริง ข้อมูลที่องค์กรต่างๆ ได้ศึกษาจัดทำขึ้นสามารถให้สารสนเทศอันเป็นประโยชน์ในเรื่องของผลประโยชน์ที่เกิดขึ้นได้จริง

ตัวอย่างที่ 6—สถิติของการกำกับดูแลด้านไอที

ITGI มอบหมายให้ PWC ดำเนินโครงการวิจัยด้านการตลาดในเรื่องการกำกับดูแลด้านไอที[7] จากผู้ตอบแบบสอบถามซึ่งอยู่ทั้งทางด้านไอทีและด้านธุรกิจกว่า 800 รายจาก 21 ประเทศ พบว่าร้อยละ 38 ของผู้ตอบแบบสอบถาม ระบุว่ามีต้นทุนด้านไอทีลดลงจากผลการกำกับดูแลด้านไอที ร้อยละ 28.1 เห็นว่ามีการพัฒนาด้านศักยภาพในการแข่งขันทางธุรกิจ
ร้อยละ 27.1 ระบุว่าผลตอบแทนจากการลงทุนด้านไอทีเพิ่มขึ้น นอกจากนี้ ยังมีการรายงานถึงผลประโยชน์อื่นๆ ที่อาจไม่สามารถประเมินเป็นตัวเงินได้ เช่น การบริหารความเสี่ยงที่เกี่ยวข้องกับไอทีได้ดีขึ้น (ร้อยละ 42.2 ของผู้ตอบแบบสอบถาม) การสื่อสารและความสัมพันธ์ที่ดีขึ้นระหว่างธุรกิจและไอที (ร้อยละ 39.6 ของผู้ตอบแบบสอบถาม) และไอทีที่ให้ผลต่อวัตถุประสงค์ของธุรกิจได้ดีขึ้น (ร้อยละ 37.3 ของผู้ตอบแบบสอบถาม)

ISACA ได้ทำการวิจัยอีกอันหนึ่ง[8] เพื่อสำรวจและแสดงให้เห็นถึงคุณค่าทางธุรกิจของ COBIT ผลลัพธ์จากการวิจัยได้เปิดโอกาสให้มีการวิเคราะห์เพิ่มเติมอีกมาก และทำให้เห็นภาพของความสัมพันธ์ระหว่างการกำกับดูแลขององค์กรและประสิทธิภาพในดำเนินงานของธุรกิจที่ชัดเจน

การวิจัยอีกอันหนึ่งได้สำรวจองค์กร 250 แห่งทั่วโลก พบว่าด้วยวัตถุประสงค์เดียวกัน[9] องค์กรที่มีการกำกับดูแลด้านไอทีที่ดีจะมีกำไรมากกว่าองค์กรที่ขาดการกำกับดูแลอย่างน้อยร้อยละ 20 อาจกล่าวอีกนัยหนึ่งได้ว่า คุณค่าทางธุรกิจของไอที เป็นผลโดยตรงจากการกำกับดูแลด้านไอทีที่มีประสิทธิผล

ท้ายสุดนี้ กรณีศึกษาวิจัยในอุตสาหกรรมเครื่องบิน ได้ข้อสรุปว่า การนำการกำกับดูแลด้านไอทีไปใช้ และการให้ความเชื่อมั่นอย่างต่อเนื่อง จะช่วยฟื้นฟูความเชื่อมั่นระหว่างธุรกิจและไอทีให้กลับมา และช่วยให้การลงทุนสอดคล้องกับเป้าหมายทางกลยุทธ์มากยิ่งขึ้น นอกจากนี้ ยังมีการรายงานถึงผลประโยชน์ที่จับต้องได้มากขึ้น รวมทั้งการลดลงของต้นทุนด้านไอทีต่อหน่วยผลิตทางการค้า (business production unit) อย่างต่อเนื่อง และช่วยให้มีงบประมาณเหลือมาใช้สำหรับนวัตรกรรมใหม่ๆ ด้วย กรณีศึกษาอีกอันหนึ่งในภาคธุรกิจการเงิน แสดงให้เห็นว่า องค์กรที่มีวิธีปฏิบัติสำหรับการกำกับดูแลด้านไอทีที่ดี จะได้รับคะแนนวุฒิภาวะของความสอดคล้องกันระหว่างธุรกิจ/ไอทีในระดับสูง[10]

[7] ITITGI, 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

บทที่ 8
ต้นแบบความสามารถของกระบวนการใน COBIT 5

บทนำ

ผู้ใช้ COBIT 4.1 Risk IT และ Val IT จะคุ้นเคยกับต้นแบบระดับวุฒิภาวะของกระบวนการ (process maturity model) ที่มีอยู่ในกรอบการดำเนินงานเหล่านั้น ต้นแบบนี้ใช้สำหรับวัดระดับวุฒิภาวะของกระบวนการที่เกี่ยวกับไอทีขององค์กรในปัจจุบันหรือที่กำลังใช้อยู่ ใช้ระบุถึงระดับวุฒิภาวะที่ต้องการให้เป็นในอนาคต ใช้ระบุช่องว่างระหว่างกัน และใช้ระบุว่าจะพัฒนากระบวนการเพื่อบรรลุถึงระดับวุฒิภาวะที่ต้องการได้อย่างไร

ในชุดผลิตภัณฑ์ของ COBIT 5 ได้รวมถึงต้นแบบความสามารถของกระบวนการ ที่อิงกับ ISO/IEC 15504 วิศกรรมซอฟแวร์ - มาตรฐานการประเมินกระบวนการ (Software engineering - Process assessment standard) ซึ่งเป็นที่ยอมรับในระดับสากล ต้นแบบดังกล่าวนี้ใช้เพื่อวัตถุประสงค์เช่นเดียวกับการประเมินกระบวนการและการสนับสนุนการปรับปรุงกระบวนการ กล่าวคือให้วิธีในการวัดผลประสิทธิภาพในการดำเนินงานของกระบวนการการกำกับดูแล (EDM based) หรือกระบวนการบริหารจัดการ (PBRM base) และช่วยให้สามารถระบุถึงจุดที่ควรต้องได้รับการปรับปรุง

อย่างไรก็ตาม ต้นแบบใหม่นี้ต่างจากต้นแบบระดับวุฒิภาวะ (maturity model) เดิมของ COBIT 4.1 ทั้งในแง่ของการออกแบบและการใช้งาน ด้วยเหตุนี้ ในบทนี้จะได้กล่าวถึง 4 หัวข้อดังต่อไปนี้
- ความแตกต่างระหว่างต้นแบบของ COBIT 5 และ COBIT 4.1
- ประโยชน์ของต้นแบบของ COBIT 5
- บทสรุปความแตกต่างที่ผู้ใช้งาน COBIT 5 จะพบในทางปฏิบัติ
- การประเมินความสามารถโดยใช้ COBIT 5

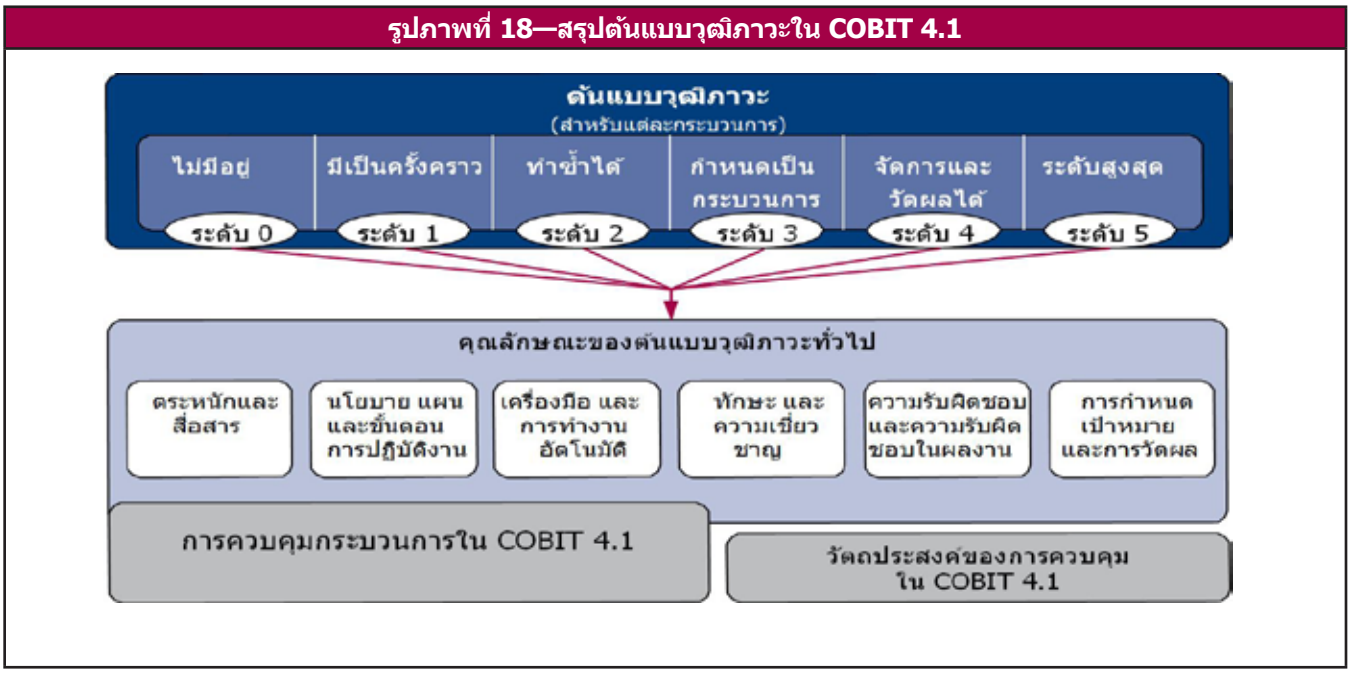
รายละเอียดของวิธีปฏิบัติของ COBIT 5 สำหรับการประเมินความสามารถ มีแสดงไว้ในเอกสารของ ISACA ชื่อ *COBIT® Process Assessment Model (PAM): Using COBIT® 4.1* [11]

ถึงแม้ว่าวิธีปฏิบัตินี้จะให้ข้อมูลที่เป็นประโยชน์เกี่ยวกับสถานะของกระบวนการต่างๆ แต่กระบวนการก็เป็นเพียงหนึ่งในปัจจัยเอื้อ 7 ประเภทสำหรับการกำกับดูแลและการบริหารจัดการ ดังนั้นการประเมินกระบวนการเพียงอย่างเดียวจะไม่ได้ให้ภาพทั้งหมดสำหรับสถานะของการกำกับดูแลในองค์กร จึงมีความจำเป็นต้องมีการประเมินปัจจัยเอื้ออื่นๆ ร่วมด้วย

ความแตกต่างระหว่างต้นแบบวุฒิภาวะใน COBIT4.1 และต้นแบบวุฒิภาวะของกระบวนการใน COBIT 5

องค์ประกอบของต้นแบบระดับวุฒิภาวะ(maturity model) ใน COBIT 4.1 ได้แสดงใน**รูปภาพที่ 18**

รูปภาพที่ 18—สรุปต้นแบบวุฒิภาวะใน COBIT 4.1



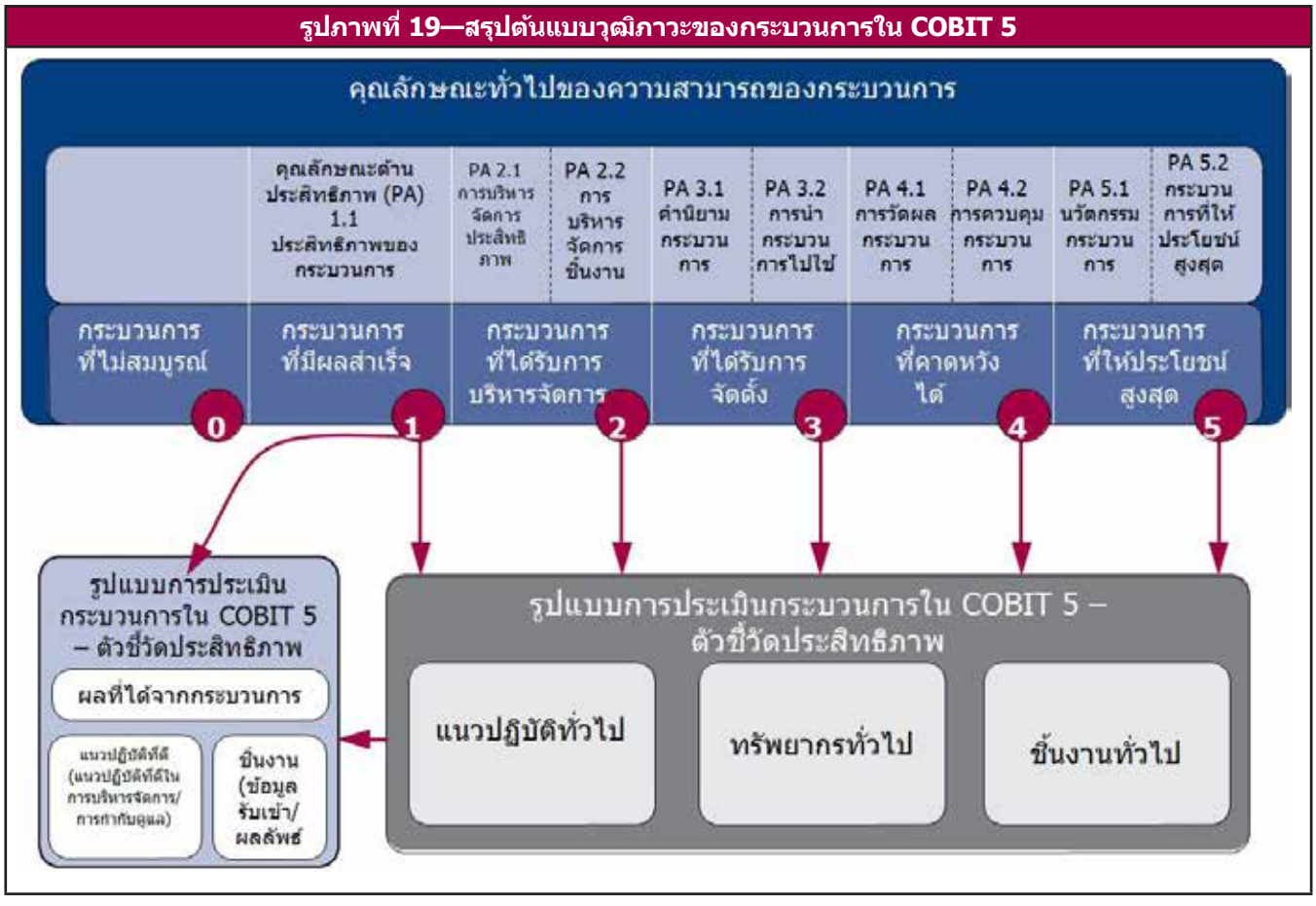
[11] www.isaca.org/cobit-pam

การใช้ต้นแบบวุฒิภาวะใน COBIT 4.1 สำหรับวัตถุประสงค์ในการปรับปรุงกระบวนการ ไม่ว่าจะเป็นการประเมินระดับวุฒิภาวะของกระบวนการ การระบุระดับวุฒิภาวะเป้าหมาย หรือการระบุช่องว่างที่เป็นความต่าง จำเป็นต้องใช้องค์ประกอบของ COBIT 4.1 ดังนี้

- เริ่มแรก จะต้องประเมินเพื่อให้ทราบว่า มีการดำเนินงานให้เป็นไปตามวัตถุประสงค์ของการควบคุมสำหรับกระบวนการหรือไม่
- ถัดมา ต้นแบบวุฒิภาวะที่แสดงไว้ในแนวทางการบริหารจัดการสำหรับแต่ละกระบวนการ อาจนำมาใช้ในการหาข้อมูลรายละเอียด (profile) เกี่ยวกับระดับวุฒิภาวะของกระบวนการ
- นอกจากนี้ ต้นแบบระดับวุฒิภาวะทั่วไป (generic maturity model) ใน COBIT 4.1 ยังได้กำหนดคุณลักษณะที่แตกต่างกัน 6 ประการสำหรับแต่ละกระบวนการ ซึ่งช่วยทำให้เห็นถึงรายละเอียดของระดับวุฒิภาวะของกระบวนการ
- การควบคุมกระบวนการ (Process Control) เป็นวัตถุประสงค์ของการควบคุมทั่วไป ซึ่งจำเป็นต้องได้รับการสอบทานเมื่อมีการประเมินกระบวนการ การควบคุมกระบวนการบางส่วนทับซ้อนกับคุณลักษณะของต้นแบบวุฒิภาวะทั่วไป

ต้นแบบความสามารถของกระบวนการ ใน COBIT 5 สามารถสรุปได้ตาม**รูปภาพที่ 19**

รูปภาพที่ 19—สรุปต้นแบบวุฒิภาวะของกระบวนการใน COBIT 5



กระบวนการหนึ่งๆ มีความสามารถได้อยู่ 6 ระดับ ซึ่งรวมถึง "กระบวนการที่ไม่สมบูรณ์" หากแนวปฏิบัติภายใต้กระบวนการไม่สามารถบรรลุถึงวัตถุประสงค์ที่ตั้งไว้

- **0 กระบวนการที่ไม่สมบูรณ์** (incomplete process) — กระบวนการไม่ถูกนำไปใช้ หรือไม่สามารถบรรลุวัตถุประสงค์ของกระบวนการนั้นๆ ได้ ในระดับนี้มีหลักฐานเพียงเล็กน้อยหรือไม่มีหลักฐานเลยที่จะแสดงถึงการบรรลุวัตถุประสงค์ของกระบวนการ
- **1 กระบวนการที่มีผลสำเร็จ** (Performed process (1 คุณลักษณะ)) — กระบวนการที่ได้รับการนำไปใช้งานประสบความสำเร็จตามวัตถุประสงค์ของกระบวนการ
- **2 กระบวนการที่ได้รับการบริหารจัดการ** (Managed process (2 คุณลักษณะ)) — กระบวนการที่มีผลสำเร็จดังที่กล่าวไว้ในข้อก่อน ได้รับการบริหารจัดการ (วางแผน เฝ้าติดตาม และแก้ไข) และชิ้นงานได้รับการกำหนด ควบคุม และเก็บรักษาอย่างเหมาะสม
- **3 กระบวนการที่ได้รับการจัดตั้ง** (Established process (2 คุณลักษณะ)) — กระบวนการที่กล่าวไว้ใน กระบวนการที่ได้รับการบริหารจัดการก่อนหน้านี้ ที่ได้รับการนำไปใช้โดยเป็นไปตามกระบวนการที่กำหนดไว้เพื่อให้สามารถได้มาซึ่งผลลัพธ์ของกระบวนการ
- **4 กระบวนการที่คาดหวังได้** (Predictable process (2 คุณลักษณะ)) — กระบวนการที่กล่าวไว้ใน กระบวนการที่ได้รับการจัดตั้งก่อนหน้านี้ ที่มีการดำเนินงานภายใต้ข้อจำกัดที่กำหนดไว้ เพื่อให้ได้มาซึ่งผลลัพธ์ของกระบวนการ
- **5 กระบวนการที่ให้ประโยชน์สูงสุด** (Optimising process (2 คุณลักษณะ)) กระบวนการที่กล่าวไว้ในกระบวนการที่คาดหวังได้ก่อนหน้านี้ ได้รับการปรับปรุงอย่างต่อเนื่องเพื่อให้บรรลุเป้าหมายทางธุรกิจที่เกี่ยวข้องทั้งในปัจจุบันและที่ประมาณการไว้

ในการที่จะบรรลุถึงความสามารถในแต่ละระดับได้นั้นเราต้องบรรลุถึงความสามารถในระดับต่ำกว่าอย่างสมบูรณ์ให้ได้ก่อน ตัวอย่างเช่น ความสามารถของกระบวนการที่ระดับ 3 (กระบวนการที่ได้รับการจัดตั้ง) กำหนดให้กระบวนการต้องมีความสามารถที่เป็นไปตามคำนิยามของกระบวนการและมีคุณลักษณะของการนำกระบวนการไปใช้งาน (Process deployment attribute) เป็นส่วนใหญ่ โดยจะต้องมีคุณลักษณะของความสามารถที่ระดับ 2 (กระบวนการที่ได้รับการบริหารจัดการ) อย่างสมบูรณ์ก่อน

มีความแตกต่างอย่างเป็นนัยสำคัญระหว่างความสามารถของกระบวนการในระดับที่ 1 กับระดับที่สูงกว่า ความสามารถของกระบวนการระดับที่ 1 จะต้องบรรลุคุณลักษณะของประสิทธิภาพในการดำเนินงานของกระบวนการ (process performance attribute) เป็นส่วนใหญ่ ซึ่งจริงๆ แล้วหมายถึงการได้ดำเนินกระบวนการอย่างเสร็จสิ้นสมบูรณ์และองค์กรได้ผลลัพธ์ตามที่ต้องการ ความสามารถของกระบวนการในระดับที่สูงกว่าจะต้องมีคุณลักษณะอื่นๆที่เพิ่มเติมเข้าไป การประเมินในลักษณะนี้แม้ว่ามาตรวัดจะมีสูงสุดถึงระดับ 5 แต่การบรรลุความสามารถในระดับ 1 ก็ถือว่าเป็นความสำเร็จก้าวสำคัญขององค์กรแล้ว มีข้อสังเกตว่าแม้ว่าแต่ละองค์กรอาจเลือกระดับความสามารถเป้าหมายหรือระดับที่ต้องการระดับใดก็ได้ (ตามการวิเคราะห์ต้นทุน-ประโยชน์ และการศึกษาความเป็นไปได้) แต่แทบจะไม่พบว่ามีองค์กรที่เลือกระดับสูงสุด

ความแตกต่างที่สำคัญระหว่าง การประเมินความสามารถของกระบวนการ ตาม ISO/IEC 15504 (ISO/IEC 15504-process capability assessment) กับต้นแบบระดับวุฒิภาวะ (maturity model) ใน COBIT 4.1 (และเช่นเดียวกับต้นแบบระดับวุฒิภาวะของแต่ละโดเมนใน Val IT และ Risk IT) สามารถสรุปได้ดังนี้
- ชื่อและความหมายของระดับของความสามารถที่กำหนดใน ISO/IEC 15504 ค่อนข้างแตกต่างจากระดับวุฒิภาวะของกระบวนการใน COBIT 4.1
- ใน ISO/IEC 15504 ระดับความสามารถถูกกำหนดโดยคุณลักษณะของกระบวนการ 9 ข้อ ซึ่งคุณลักษณะเหล่านี้ครอบคลุมเฉพาะบางคุณลักษณะของระดับวุฒิภาวะใน COBIT 4.1 (COBIT 4.1 maturity attribute) และ/หรือการควบคุมกระบวนการปัจจุบันเพียงในระดับหนึ่งเท่านั้นและเป็นไปในทางที่แตกต่างกัน

การปฏิบัติตามต้นแบบอ้างอิงของกระบวนการใน ISO/IEC 15504:2 กำหนดไว้ว่า ในคำอธิบายของกระบวนการใดๆ ที่จะได้รับประเมิน ได้แก่ กระบวนการสำหรับการกำกับดูแลและ/หรือการบริหารจัดการของ COBIT5 ใดๆ จะต้องระบุถึง :
- คำบรรยายที่กล่าวถึงวัตถุประสงค์และผลลัพธ์
- คำอธิบายกระบวนการไม่ควรกำหนดมุมมองใดๆ สำหรับการวัดผลตามกรอบดำเนินงานที่นอกเหนือไปกว่าระดับที่ 1 ซึ่งหมายความว่า ไม่ว่าจะเป็นลักษณะใดๆ ของคุณลักษณะของกระบวนการที่เหนือกว่าระดับที่ 1 จะต้องไม่ปรากฏในคำอธิบายกระบวนการหรือในแนวปฏิบัติในการบริหารจัดการใดๆ /กิจกรรมใดภายใต้กระบวนการนั้นๆ ดังนั้น คำอธิบายกระบวนการที่แสดงไว้ใน *COBIT 5: การสัมฤทธิ์ผลของกระบวนการ (COBIT 5: Enabling Process)* จะมีเพียงขั้นตอนที่จำเป็นเพื่อที่จะบรรลุวัตถุประสงค์และเป้าหมายของกระบวนการเท่านั้น
- จากหัวข้อข้างต้น คุณลักษณะทั่วไปที่ใช้ได้กับกระบวนการทั้งหมดขององค์กรซึ่งช่วยให้บรรลุถึงวัตถุประสงค์การควบคุมที่อาจแสดงไว้ซ้ำซ้อนกันในเอกสาร *COBIT® 3rd Edition* ได้รับการนำมาจัดกลุ่มเป็นวัตถุประสงค์การควบคุมกระบวนการ (PC) ใน COBIT 4.1 และปัจจุบันได้ถูกกำหนดเป็นระดับ 2 ถึงระดับ 5 ในรูปแบบการประเมิน (assessment model)

แนวปฏิบัติที่แตกต่างกัน[12]

จากที่ได้อธิบายไปข้างต้น เป็นที่ชัดเจนว่ามีแนวปฏิบัติที่แตกต่างกันบางประการที่เกี่ยวข้องกับการเปลี่ยนแปลงรูปแบบการประเมิน (Assessment model) ผู้ใช้งานต้องตระหนักถึงการเปลี่ยนแปลงนี้ และเตรียมพร้อมที่จะนำมาพิจารณาในแผนดำเนินการ

การเปลี่ยนแปลงสำคัญที่ควรพิจารณาประกอบด้วย
- ถึงแม้ว่าน่าจะมีการเปรียบเทียบผลการประเมินระหว่าง COBIT 4.1 และ COBIT 5 เนื่องจากความคล้ายคลึงกันในระดับของการวัดและคำที่ใช้ในการอธิบาย แต่การเปรียบเทียบนี้ยากมากเนื่องจากความแตกต่างกันในขอบเขต จุดสนใจ และเจตนารมณ์ ดังที่ได้แสดงใน**รูปภาพที่ 20**
- โดยทั่วไปแล้ว คะแนนที่ได้จากต้นแบบความสามารถของกระบวนการใน COBIT 5 (COBIT 5 process capability model) จะต่ำกว่า ตามที่แสดงใน**รูปภาพที่ 20** ด้วยต้นแบบระดับวุฒิภาวะ (maturity model) ใน COBIT 4.1 กระบวนการจะบรรลุระดับที่ 1 หรือ 2 ได้โดยไม่จำเป็นต้องบรรลุวัตถุประสงค์ทั้งหมดของกระบวนการอย่างสมบูรณ์ แต่ถ้าวัดตามระดับความสามารถของกระบวนการ (process capability level) ใน COBIT 5 แล้วจะได้แค่เพียงระดับ 0 หรือ 1 เท่านั้น

การวัดระดับของความสามารถ (capability scale) ใน COBIT 4.1 และ COBIT 5 สามารถเทียบกันได้คร่าวๆ ตาม**รูปภาพที่ 20**
- ไม่มีต้นแบบระดับวุฒิภาวะ (maturity model) สำหรับแต่ละกระบวนการในเนื้อหารายละเอียดของกระบวนการใน COBIT 5 อีกต่อไป เพราะว่าวิธีปฏิบัติสำหรับการประเมินความสามารถของกระบวนการใน ISO /IEC 15504 ไม่มีกำหนดไว้และถึงขนาดห้ามไม่ให้ใช้วิธีปฏิบัตินี้ แต่วิธีปฏิบัตินี้กำหนดสารสนเทศที่ต้องการสำหรับ 'ต้นแบบอ้างอิงของกระบวนการ' แทน (ต้นแบบกระบวนการที่จะใช้ในการประเมินนี้) ดังนี้
  - คำอธิบายกระบวนการ พร้อมกับคำแถลงจุดประสงค์
  - แนวปฏิบัติพื้นฐาน ซึ่งเทียบได้กับแนวปฏิบัติสำหรับกระบวนการกำกับดูแลและบริหารจัดการในความหมายของ COBIT 5

[12] ข้อมูลเพิ่มเติมเกี่ยวกับโปรแกรมการประเมิน COBIT ที่อิงกับมาตรฐาน ISO/IEC 15504 ใหม่ๆ สามารถหาได้จาก *www.isaca.org/cobit-assessment-programme*

- ชิ้นงาน (Work product) ซึ่งเทียบได้กับข้อมูลที่รับมาและผลลัพธ์ในความหมายของ COBIT 5

- ต้นแบบระดับวุฒิภาวะ (maturity model) ใน COBIT 4.1 ให้รายละเอียดของวุฒิภาวะในแต่ละระดับสำหรับองค์กร วัตถุประสงค์หลักของรายละเอียดนี้ก็เพื่อระบุถึงมุมมองหรือคุณลักษณะที่มีจุดอ่อนที่ควรได้รับการปรับปรุง องค์กรจะใช้วิธีปฏิบัตินี้เมื่อต้องการเน้นที่การปรับปรุงให้ดีขึ้นมากกว่าที่จะทำเพื่อให้ได้มาซึ่งตัวเลขระดับวุฒิภาวะเพื่อจุดประสงค์ในการรายงาน ในรูปแบบการประเมินของ COBIT 5 ให้มาตราของการวัดผลสำหรับแต่ละคุณลักษณะด้านความสามารถ (capability attribute) และให้แนวทางในการประยุกต์ใช้ ดังนั้น การประเมินคุณลักษณะด้านความสามารถสำหรับแต่ละกระบวนการสามารถจึงทำได้ในแต่ละข้อของคุณลักษณะด้านความสามารถทั้ง 9 ข้อ
- คุณลักษณะของวุฒิภาวะใน COBIT 4.1 และคุณลักษณะความสามารถของกระบวนการใน COBIT 5 มีความแตกต่างกันแต่ทับซ้อนกันในระดับหนึ่งดังที่ได้แสดงไว้ใน**รูปภาพที่ 21** องค์กรที่ใช้วิธีปฏิบัติที่อิงกับคุณลักษณะของต้นแบบระดับวุฒิภาวะ (maturity model attribute approach) ใน COBIT 4.1 สามารถนำข้อมูลการประเมินที่มีอยู่มาจัดแบ่งประเภทใหม่ภายใต้การประเมินคุณลักษณะใน COBIT 5 ได้ ตาม**รูปภาพที่ 21**

รูปภาพที่ 20—ตารางเปรียบเทียบระดับวุฒิภาวะ (COBIT 4.1) และระดับความสามารถของกระบวนการ (COBIT 5)

ต้นแบบระดับวุฒิภาวะใน COBIT 4.1	ความสามารถของกระบวนการตาม ISO/IEC 15504	บริบท
5.เหมาะสม (Optimised)- กระบวนการได้รับการปรับให้อยู่ในระดับแนวปฏิบัติที่ดี ซึ่งเป็นผลจากการปรับปรุงอย่างต่อเนื่องและการใช้ต้นแบบระดับวุฒิภาวะเพื่อเปรียบเทียบกับองค์กรอื่นๆ มีการบูรณาการไอทีเพื่อให้เกิดกระแสงาน (workflow) ที่เป็นอัตโนมัติ เป็นเครื่องมือในการปรับปรุงคุณภาพและประสิทธิผล ทำให้องค์กรปรับตัวได้อย่างรวดเร็ว	**ระดับที่ 5** กระบวนการที่เหมาะสม (Optimising process)–มีการพัฒนาจากระดับที่ 4 กระบวนการที่คาดหวังได้ ด้วยการปรับปรุงอย่างต่อเนื่อง เพื่อให้บรรลุเป้าหมายทางธุรกิจที่เกี่ยวข้องทั้งในปัจจุบันและที่ประมาณการไว้	มุมมองขององค์กร- องค์ความรู้ขององค์กร
4. บริหารจัดการและวัดผล – ผู้บริหารเฝ้าติดตามและวัดผลการปฏิบัติตามขั้นตอน และดำเนินการเมื่อพบว่ากระบวนการไม่ได้ประสิทธิผล กระบวนได้รับการปรับปรุงอย่างสม่ำเสมอและให้แนวปฏิบัติที่ดี มีการใช้การทำงานที่เป็นอัตโนมัติและเครื่องมือต่างๆ อยู่บ้างอย่างกระจัดกระจาย	**ระดับที่ 4 กระบวนการที่คาดหวังได้** (Predictable process)–เมื่อกระบวนการที่ได้รับการจัดตั้งในระดับที่ 3 ดำเนินการภายใต้ข้อจำกัดที่ระบุเพื่อให้บรรลุถึงผลลัพธ์ของกระบวนการ	
3. กระบวนการที่ชัดเจน (defined process) – ขั้นตอนการปฏิบัติงานมีความเป็นมาตรฐานและจัดทำเป็นลายลักษณ์อักษร และสื่อสารผ่านทางการฝึกอบรม มีการบังคับใช้ให้ปฏิบัติตามกระบวนการดังกล่าว อย่างไรก็ตาม ไม่มีการตรวจสอบว่ามีความคลาดเคลื่อนไปจากกระบวนการหรือไม่ ขั้นตอนการปฏิบัติงานไม่ยุ่งยาก แต่ทำให้แนวปฏิบัติงานที่ใช้อยู่เป็นทางการมากขึ้น	**ระดับที่ 3 กระบวนการที่ได้รับการจัดตั้ง**(Established process)—กระบวนการที่ได้รับการบริหารจัดการในระดับที่ 2 ได้รับการนำไปใช้โดยมีการกำหนดกระบวนการที่สามารถทำให้บรรลุถึงผลลัพธ์ของกระบวนการ	
	ระดับที่ 2 กระบวนการที่ได้รับการบริหารจัดการ (Managed Process)—กระบวนการที่มีผลสำเร็จในระดับที่ 1 ได้รับนำไปใช้โดยมีการบริหารจัดการ(วางแผน เฝ้าติดตาม และแก้ไข) และชิ้นงานของกระบวนการได้รับการจัดทำ ควบคุม และเก็บรักษาอย่างเหมาะสม	มุมมองตามแต่กรณี- องค์ความรู้ของบุคคล
2. ทำซ้ำได้แต่ทำโดยสัญชาตญาณ (repeatable but intuitive) กระบวนการได้รับการพัฒนาไปถึงขั้นที่มีบุคคลหลายๆ คนที่ทำงานอย่างเดียวกันโดยปฏิบัติตามขั้นตอนการปฏิบัติงานแบบเดียวกัน ไม่มีการฝึกอบรมอย่างเป็นทางการหรือสื่อสารถึงกระบวนการที่เป็นมาตรฐาน การทำงานโดยส่วนใหญ่ขึ้นอยู่กับตัวบุคคลจึงมักมีความผิดพลาดเกิดขึ้นบ่อยครั้ง	**ระดับที่ 1 กระบวนการที่มีผลสำเร็จ** (Performed process)—กระบวนการที่ได้รับการนำไปใช้และบรรลุจุดประสงค์ของกระบวนการ **หมายเหตุ อาจเป็นไปได้ว่ากระบวนการที่ได้รับการจัดให้อยู่ระดับที่ 1 ภายใต้ต้นแบบระดับวุฒิภาวะอาจได้รับการจัดว่าอยู่ที่ระดับ 0 ตาม 15504 ถ้าไม่ได้บรรลุถึงผลลัพธ์ของกระบวนการนั้น**	
1. เริ่มต้น/เฉพาะกิจ (initial/adhoc)—มีหลักฐานว่าองค์กรตระหนักว่ามีประเด็นที่เป็นปัญหาและมีความจำเป็นต้องจัดการ อย่างไรก็ตาม ไม่มีกระบวนการที่เป็นมาตรฐาน แต่กลับใช้วิธีปฏิบัติเฉพาะกิจที่มักจะขึ้นอยู่กับตัวบุคคลหรือเป็นกรณีๆ ไป วิธีปฏิบัติในการบริหารจัดการโดยรวมไม่เป็นระบบระเบียบ		
0. ไม่มี (non existent)—ไม่มีกระบวนการใดๆ องค์กรไม่ได้รับทราบว่ามีประเด็นปัญหาที่จะต้องจัดการ	**ระดับ 0 กระบวนการที่ไม่สมบูรณ์** (Incomplete process)—กระบวนการไม่ถูกนำไปใช้ หรือล้มเหลวในการบรรลุถึงจุดประสงค์	

รูปภาพที่ 21—ตารางเปรียบเทียบคุณลักษณะของวุฒิภาวะ (COBIT 4.1) และคุณลักษณะของกระบวนการ (COBIT 5)									
	COBIT 5 คุณลักษณะด้านความสามารถของกระบวนการ								
COBIT 4.1 คุณลักษณะของวุฒิภาวะ	ประสิทธิภาพของกระบวนการ	การบริหารจัดการประสิทธิภาพ	การบริหารจัดการชิ้นงาน	คำนิยามกระบวนการ	การนำกระบวนการไปใช้	การวัดผลกระบวนการ	การควบคุมกระบวนการ	นวัตกรรมของกระบวนการ	การปรับกระบวนการให้เหมาะสมที่สุด
การตระหนักและสื่อสาร				■	■	■			
นโยบาย แผนงาน และขั้นตอนการปฏิบัติงาน							■		
เครื่องมือและการทำงานที่เป็นอัตโนมัติ				■					
ทักษะและความชำนาญ				■	■				
ความรับผิดชอบและความรับผิดชอบในผลงาน				■					
การกำหนดเป้าหมายและการวัดผล		■				■			

ประโยชน์จากการเปลี่ยนแปลง

ประโยชน์ของต้นแบบความสามารถของกระบวนการใน COBIT 5 เมื่อเปรียบเทียบกับต้นแบบระดับวุฒิภาวะ ของ COBIT 4.1 คือ

- การเน้นมากขึ้นในกระบวนการที่ได้นำไปปฏิบัติ เพื่อยืนยันว่าได้บรรลุวัตถุประสงค์จริงและส่งมอบผลลัพธ์ได้ตามที่คาดหวังจากกระบวนการนั้นๆ
- มีเนื้อหาเรียบง่ายไม่ซ้ำซ้อน เพราะการประเมินต้นแบบระดับวุฒิภาวะของ COBIT 4.1 ต้องใช้ส่วนประกอบหลายประการเพื่อสนับสนุนการประเมิน ซึ่งรวมถึงต้นแบบระดับวุฒิภาวะทั่วไป ต้นแบบระดับวุฒิภาวะของกระบวนการ วัตถุประสงค์การควบคุม และการควบคุมกระบวนการ
- ปรับปรุงให้กิจกรรมการประเมินความสามารถของกระบวนการและการประเมินผลมีความน่าเชื่อถือมากขึ้นและมีความสามารถในการทำซ้ำได้ดีขึ้น ลดข้อโต้แย้งและความเห็นต่างในผลของการประเมินระหว่างผู้มีส่วนได้เสียต่างๆ
- ใช้ผลลัพธ์จากการประเมินความสามารถของกระบวนการได้มากขึ้น เพราะต้นแบบใหม่นี้ได้สร้างพื้นฐานสำหรับการประเมินที่เป็นทางการและเข้มงวดมากขึ้น สำหรับจุดประสงค์ภายในองค์กรและจุดประสงค์ที่อาจเกิดขึ้นจากภายนอกองค์กร
- สอดคล้องกับมาตรฐานการประเมินกระบวนการที่ยอมรับกันโดยทั่วไป ดังนั้น จึงสนับสนุนวิธีปฏิบัติสำหรับการประเมินกระบวนการที่มีอยู่แล้วได้เป็นอย่างดี

ดำเนินการประเมินความสามารถของกระบวนการตาม COBIT 5

มาตรฐาน ISO /IEC 15504 ระบุว่า เราอาจประเมินความสามารถของกระบวนการด้วยจุดประสงค์ที่หลากหลาย และด้วยระดับความเข้มงวดที่แตกต่างกัน จุดประสงค์อาจเป็นการภายในโดยเน้นที่การเปรียบเทียบระหว่างหน่วยงานในองค์กร และ/หรือการปรับปรุงกระบวนการเพื่อประโยชน์ต่อองค์กรเป็นการภายใน หรืออาจเป็นจุดประสงค์จากภายนอกที่จะเน้นการประเมิน การรายงาน และการให้การรับรองแบบเป็นทางการ

COBIT 5 ซึ่งอิงกับวิธีปฏิบัติสำหรับการประเมินของ ISO /IEC 15504 เป็นวิธีปฏิบัติหลักของ COBIT มาตั้งแต่ปีค.ศ. 2000 ที่ยังคงช่วยให้บรรลุวัตถุประสงค์ดังต่อไปนี้เสมอมา

- เอื้อสำหรับหน่วยงานกำกับดูแลและผู้บริหาร ที่จะสามารถวิเคราะห์เปรียบเทียบความสามารถของกระบวนการ (benchmark process capability)
- เอื้อในการตรวจสอบสถานะ (health check) ในภาพรวม 'ตามสภาพปัจจุบัน' และ 'ที่ต้องการ' เพื่อสนับสนุนหน่วยงานกำกับดูแลและผู้บริหารสำหรับการตัดสินใจลงทุนในเรื่องการปรับปรุงกระบวนการ
- วิเคราะห์ช่องว่างและปรับปรุงข้อมูลในการวางแผนเพื่อสนับสนุนการให้คำนิยามของความสมเหตุผลสำหรับโครงการปรับปรุงต่างๆ
- ให้คะแนน (Rating) จากการประเมินแก่หน่วยงานกำกับดูแลและผู้บริหาร เพื่อวัดผลและเฝ้าติดตามขีดความสามารถในปัจจุบัน

ในส่วนนี้จะอธิบายว่า เราจะดำเนินการประเมินในภาพรวมโดยใช้ต้นแบบการประเมินความสามารถของกระบวนการใน COBIT 5 เพื่อให้บรรลุวัตถุประสงค์ต่างๆ ข้างต้นได้อย่างไร

การประเมินทำให้เห็นความแตกต่างระหว่างการประเมินความสามารถในระดับที่ 1 และระดับที่สูงกว่า ที่จริงแล้ว ตามที่ได้อธิบายไปแล้วว่า ความสามารถของกระบวนการในระดับที่ 1 บรรยายให้เราทราบได้ว่ากระบวนการได้บรรลุจุดประสงค์ที่ตั้งไว้หรือไม่ ดังนั้น จึงเป็นระดับที่สำคัญมากที่จะต้องบรรลุ และถือว่าเป็นพื้นฐานที่นำไปสู่ระดับความสามารถที่สูงขึ้น การประเมินว่ากระบวนการบรรลุเป้าหมายแล้วหรือไม่ หรือในอีกนัยหนึ่งคือการบรรลุความสามารถในระดับที่ 1 สามารถทำได้โดย

1. สอบทานผลลัพธ์ของกระบวนการ ตามที่ได้บรรยายไว้ในคำอธิบายกระบวนการในรายละเอียดสำหรับแต่ละกระบวนการ และใช้ระดับการประเมินตาม ISO/IEC 15504 เพื่อจัดระดับว่าแต่ละกระบวนการได้บรรลุเป้าหมายในระดับใด ระดับดังกล่าวนี้ประกอบด้วย
   - **N** (ไม่บรรลุวัตถุประสงค์) คือ ไม่มีหลักฐานหรือมีหลักฐานเพียงเล็กน้อย ที่แสดงให้เห็นได้ว่ากระบวนการได้บรรลุคุณลักษณะที่กำหนดไว้ในกระบวนการที่ได้รับการประเมิน (บรรลุร้อยละ 0 ถึง 15)
   - **P** (บรรลุบางส่วน) มีหลักฐานอยู่บ้างถึงการมีวิธีปฏิบัติเพื่อช่วยให้บรรลุผลและการบรรลุผลตามคุณลักษณะที่กำหนดไว้ในกระบวนการที่ได้รับการประเมิน การบรรลุผลตามคุณลักษณะในบางด้านอาจจะไม่สามารถคาดเดาได้ (บรรลุร้อยละ ร้อยละ 15 ถึง 50)
   - **L** (บรรลุได้เป็นส่วนใหญ่) มีหลักฐานของการมีวิธีปฏิบัติที่เป็นระบบและการบรรลุผลตามคุณลักษณะที่ได้กำหนดไว้ในกระบวนการที่ได้รับการประเมินเป็นส่วนใหญ่ พบจุดอ่อนบ้างในคุณลักษณะของกระบวนการที่ได้รับการประเมิน (บรรลุร้อยละ 50 ถึง 85)
   - **F** (บรรลุอย่างสมบูรณ์) มีหลักฐานที่แสดงว่ามีวิธีปฏิบัติที่สมบูรณ์และเป็นระบบ และได้บรรลุผลอย่างสมบูรณ์ตามคุณลักษณะที่ได้กำหนดไว้ในกระบวนการที่ได้รับการประเมิน ไม่มีจุดอ่อนที่เป็นนัยสำคัญในคุณลักษณะของกระบวนการที่ได้รับการประเมิน(ร้อยละ 85 ถึง 100 ของความสำเร็จ)
2. นอกจากนี้ แนวปฏิบัติของการกระบวนการ (การกำกับดูแลและการบริหารจัดการ) ยังสามารถได้รับการประเมินโดยใช้การจัดระดับสำหรับผลการประเมินแบบเดียวกัน เพื่อแสดงให้เห็นถึงระดับที่มีการนำแนวปฏิบัติขั้นพื้นฐานไปประยุกต์ใช้
3. เพื่อให้การประเมินมีความละเอียดมากขึ้นในอนาคต อาจพิจารณาจากชิ้นงานเพื่อระบุว่าได้บรรลุถึงคุณลักษณะที่ได้รับการประเมินบางรายการมากน้อยเพียงใด

ถึงแม้ว่าการกำหนดเป้าหมายให้กับระดับความสามารถจะขึ้นอยู่กับการตัดสินใจของแต่ละองค์กร หลายองค์กรอยากให้กระบวนการทั้งหมดขององค์กรบรรลุความสามารถในระดับที่ 1 (ไม่เช่นนั้นจะมีกระบวนการเหล่านี้ไปเพื่ออะไร) ถ้าไม่สามารถบรรลุระดับที่ 1 ได้ เราย่อมสามารถระบุถึงสาเหตุที่ทำให้ไม่บรรลุระดับดังกล่าวได้อย่างชัดเจนจากวิธีปฏิบัติข้างต้น และสามารถจัดทำแผนการปรับปรุงขึ้นมาได้
1. ถ้าหากไม่สามารถบรรลุผลลัพธ์ที่ต้องการจากกระบวนการได้อย่างสม่ำเสมอหมายถึงกระบวนการไม่บรรลุวัตถุประสงค์และจำเป็นต้องได้รับการปรับปรุงให้ดีขึ้น
2. การประเมินแนวปฏิบัติของกระบวนการจะเผยให้เห็นว่าแนวการปฏิบัติใดที่ยังบกพร่องหรือล้มเหลว ช่วยให้การนำไปใช้งานและ/หรือการปรับปรุงแนวปฏิบัติเหล่านั้นสัมฤทธิ์ผล และช่วยให้บรรลุผลลัพธ์ทั้งหมดจากกระบวนการ

สำหรับระดับความสามารถของกระบวนการที่สูงขึ้น มีการนำแนวปฏิบัติทั่วไปจาก ISO/IEC 15504:2 มาใช้ ซึ่งจะให้คำอธิบายโดยทั่วไปสำหรับระดับของความสามารถในแต่ละระดับ

ภาคผนวก A
ข้อมูลอ้างอิง

ในการพัฒนา COBIT 5 นี้ กรอบการดำเนินงาน มาตรฐาน และแนวทางอื่นๆ ต่อไปนี้ ได้รับการใช้เป็นเอกสารอ้างอิงและเป็นข้อมูลเบื้องต้น

Association for Project Management (APM); APM Introduction to Programme Management, Latimer, Trend and Co., UK, 2007
British Standards Institute (BSI), BS25999:2007 Business Continuity Management Standard, UK, 2007
CIO Council, Federal Enterprise Architecture (FEA), ver 1.0, USA, 2005
European Commission, The Commission Enterprise IT Architecture Framework (CEAF), Belgium, 2006
Kotter, John; Leading Change, Harvard Business School Press, USA, 1996
HM Government, Best Management Practice Portfolio, Managing Successful Programmes (MSP), UK, 2009
HM Government, Best Management Practice Portfolio, PRINCE2®, UK, 2009
HM Government, Best Management Practice Portfolio, Information Technology Infrastructure Library (ITIL®), 2011
International Organization for Standardization (ISO), 9001:2008 Quality Management Standard, Switzerland, 2008
ISO/International Electrotechnical Commission (IEC), 20000:2006 IT Service Management Standard, Switzerland, 2006
ISO/IEC, 27005:2008, Information Security Risk Management Standard, Switzerland, 2008
ISO/IEC, 38500:2008, Corporate Governance of Information Technology Standard, Switzerland, 2008
King Code of Governance Principles (King III), South Africa, 2009
Organisation for Economic Co-operation and Development (OECD), OECD Principles of Corporate Governance, France, 2004
The Open Group, TOGAF® 9, UK, 2009
Project Management Institute, Project Management Body of Knowledge (PMBOK2®), USA, 2008
UK Financial Reporting Council, 'Combined Code on Corporate Governance', UK, 2009

หน้านี้เป็นหน้าว่าง

ภาคผนวก B
รายละเอียดความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรกับเป้าหมายที่เกี่ยวข้องกับไอที

การส่งทอดเป้าหมาย (goals cascade) ของ COBIT 5 ได้อธิบายไว้ในบทที 2

จุดประสงค์ของตารางแสดงความสัมพันธ์ใน**รูปภาพที่ 22** คือการแสดงให้เห็นว่าเป้าหมายระดับองค์กรได้รับการสนับสนุนจาก (หรือการแปลงไปสู่) เป้าหมายที่เกี่ยวข้องกับไอทีได้อย่างไร ด้วยเหตุนี้ ตารางนี้จึงประกอบด้วยข้อมูลต่อไปนี้:
- ในแต่ละสดมภ์(แนวตั้ง) ระบุถึงเป้าหมายทั่วไปในระดับองค์กรทั้งหมด 17 ข้อใน COBIT 5 และจัดเป็นกลุ่มตามมิติของการวัดผลแบบสมดุล (BSC)
- ในแต่ละแถว(แนวนอน) ระบุถึงเป้าหมายที่เกี่ยวข้องกับไอทีทั้งหมด 17 ข้อ และจัดเป็นกลุ่มตามมิติของการการวัดผลแบบสมดุล (BSC) ทางด้านไอที เช่นกัน
- การแสดงความสัมพันธ์ว่าเป้าหมายในระดับองค์กรแต่ละข้อได้รับการสนับสนุนจากเป้าหมายที่เกี่ยวข้องกับไอทีอย่างไร โดยแสดงเป็นระดับของความสัมพันธ์ดังต่อไปนี้
  - "P" หมายความว่า เป็นความสัมพันธ์ในระดับหลัก ใช้เมื่อความสัมพันธ์มีความสำคัญ ได้แก่ เป้าหมายที่เกี่ยวข้องกับไอทีเป็นปัจจัยหลักที่สนับสนุนให้บรรลุเป้าหมายระดับองค์กรในข้อนั้นๆ
  - "S" หมายความว่า เป็นความสัมพันธ์ในระดับรอง ใช้เมื่อความสัมพันธ์ชัดเจนแต่มีความสำคัญน้อยกว่า ได้แก่ เป้าหมายที่เกี่ยวข้องกับไอที เป็นปัจจัยในระดับรองที่จะสนับสนุนให้บรรลุเป้าหมายระดับองค์กรในข้อนั้นๆ

ตัวอย่างที่ 7—ตารางแสดงความสัมพันธ์

ตารางแสดงความสัมพันธ์ ชี้ให้เห็นว่า
- เป้าหมายในระดับองค์กรข้อ 7 บริการของธุรกิจมีความต่อเนื่องและความพร้อมให้บริการซึ่ง:
  - ขึ้นอยู่กับการบรรลุเป้าหมายที่เกี่ยวข้องกับไอทีดังต่อไปนี้เป็นหลัก:
    - 04 ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้
    - 10 ความมั่นคงปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน
    - 14 ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้ และมีประโยชน์ในการตัดสินใจ
  - และขึ้นอยู่การบรรลุเป้าหมายที่เกี่ยวข้องกับไอทีดังต่อไปนี้เป็นอันดับรอง:
    - 01 กลยุทธ์ด้านไอทีสอดคล้องไปในแนวทางเดียวกันกับกลยุทธ์ด้านธุรกิจ
    - 07 การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ
    - 08 การใช้ระบบงาน สารสนเทศและเทคโนโลยีอย่างเหมาะสม
- การใช้ตารางแสดงความสัมพันธ์นี้ในทางกลับกัน กล่าวคือ การบรรลุเป้าหมายเกี่ยวข้องกับไอทีข้อ 09 ความคล่องตัวทางด้านไอที จะยังผลให้บรรลุเป้าหมายระดับองค์กรหลายข้อ ได้แก่
  - การยังผลที่เป็นหลักให้แก่เป้าหมายระดับองค์กรข้อต่อไปนี้
    - 2. กลุ่ม (Portfolio)ของผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน
    - 8. การตอบสนองอย่างฉับไวต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ
    - 11. หน้าที่งานในกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด
    - 17. วัฒนธรรมที่ส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ
  - การยังผลในอันดับรองให้แก่เป้าหมายระดับองค์กรข้อต่อไปนี้
    - 1. คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย
    - 3. ความเสี่ยงทางธุรกิจที่ได้รับการจัดการ (การปกป้องคุ้มครองสินทรัพย์)
    - 6. วัฒนธรรมที่เน้นการบริการลูกค้า
    - 13. ชุดโครงการเพื่อการเปลี่ยนแปลงทางธุรกิจที่ได้รับการบริหารจัดการ
    - 14. การปฏิบัติงานและบุคคลากรที่มีประสิทธิภาพ
    - 16. บุคคลากรที่มีทักษะและแรงจูงใจ

ตารางข้างต้นจัดทำขึ้นจากข้อมูลดังต่อไปนี้
- การวิจัยของมหาวิทยาลัย Antwerp Management School IT Alignment และ Governance Research Institute
- การสอบทานและความเห็นของผู้เชี่ยวชาญเพิ่มเติมที่ได้รับระหว่างกระบวนการพัฒนาและสอบทาน COBIT 5

เมื่อใช้ตารางในรูปภาพที่ 22 กรุณาพิจารณาถึงข้อสังเกตที่ได้ให้ไว้ในบทที่ 2 เรื่องการใช้การส่งทอดเป้าหมายของ COBIT 5

รูปภาพที่ 22— ความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรใน COBIT 5 กับเป้าหมายที่เกี่ยวข้องกับไอที

			เป้าหมายระดับองค์กร																
			1. คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	2. กลุ่มของผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน	3. ความเสี่ยงทางธุรกิจที่เกี่ยวข้องกับการบริการ (การปกป้องคุ้มครองและทรัพย์สิน)	4. การปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับจากภายนอก	5. ความโปร่งใสทางการเงิน	6. วัฒนธรรมที่เน้นการบริการลูกค้า	7. บริการของธุรกิจมีความต่อเนื่องและความพร้อมให้บริการ	8. การตอบสนองอย่างฉับไวต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	9. การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	10. ต้นทุนในการส่งมอบบริการที่ให้ประโยชน์สูงสุด	11. หน้าที่งานในกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	12. ต้นทุนของกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	13. ชุดโครงการเพื่อการเปลี่ยนแปลงทางธุรกิจที่ได้รับการบริหารจัดการ	14. การปฏิบัติตามและบุคลากรที่มีประสิทธิภาพ	15. การปฏิบัติตามนโยบายภายในองค์กร	16. บุคลากรที่มีทักษะและแรงจูงใจ	17. วัฒนธรรมที่สนับสนุนนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
เป้าหมายที่เกี่ยวข้องกับไอที			ด้านการเงิน					ด้านลูกค้า					ด้านกระบวนการภายใน					ด้านการเรียนรู้และเติบโต	
ด้านการเงิน	01	กลยุทธ์ด้านไอทีสอดคล้องไปในแนวทางเดียวกันกับกลยุทธ์ด้านธุรกิจ	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	ไอทีเอื้ออำนวยและสนับสนุนให้ธุรกิจสามารถปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับของหน่วยงานภายนอก			S	P											P		
	03	ผู้บริหารระดับสูงให้คำมั่นในการตัดสินใจต่างๆ ที่เกี่ยวข้องกับไอที	P	S	S					S	S		S		P			S	S
	04	ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้			P	S			P	S		P			S		S	S	
	05	ประโยชน์ที่ได้รับจริงจากกลุ่มของการลงทุนและการให้บริการในด้านต่างๆ ที่มีไอทีเป็นปัจจัยเอื้อ	P	P				S		S		S	S	P		S			S
	06	ต้นทุน ประโยชน์และความเสี่ยงทางด้านไอทีมีความโปร่งใส	S		S		P				S	P		P					
ด้านลูกค้า	07	การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	การใช้ระบบงาน สารสนเทศและเทคโนโลยีอย่างเหมาะสม	S	S	S			S	S		S	S	P	S		P		S	S
ด้านกระบวนการภายใน	09	ความคล่องตัวทางด้านไอที	S	P	S			S		P			P		S	S		S	P
	10	ความมั่นคงปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน			P	P			P								P		
	11	การใช้สินทรัพย์ ทรัพยากร และสมรรถนะทางด้านไอทีให้ได้ประโยชน์สูงสุด	P	S						S		P	S	P	S	S			S
	12	การเอื้ออำนวยและสนับสนุนการทำงานของกระบวนการทางธุรกิจโดยบูรณาการระบบงานและเทคโนโลยีเข้าไปใช้ในกระบวนการทางธุรกิจ	S	P	S			S		S		S	P	S	S	S			S
	13	การส่งมอบชุดโครงการต่างๆ ก่อให้เกิดประโยชน์ ตรงเวลา ตามงบประมาณที่ตั้งไว้ และตามความต้องการและมาตรฐานด้านคุณภาพ	P	S	S			S				S		S	P				
	14	ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้ และมีประโยชน์ในการตัดสินใจ	S	S	S	S			P		P		S						
	15	ไอทีที่ปฏิบัติตามนโยบายภายในขององค์กร			S	S											P		
ด้านการเรียนรู้และเติบโต	16	บุคลากรทั้งทางด้านไอทีและด้านธุรกิจที่มีความสามารถและมีแรงจูงใจ	S	S	P			S		S						P		P	S
	17	ความรู้ ความเชี่ยวชาญ และการริเริ่มดำเนินการเพื่อนวัตกรรมทางธุรกิจ	S	P				S		P	S		S		S			S	P

ภาคผนวก C
รายละเอียดความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีและกระบวนการที่เกี่ยวข้องกับไอที

ภาคผนวกนี้แสดงตารางที่อธิบายว่ากระบวนการทางด้านไอทีสนับสนุนเป้าหมายที่เกี่ยวข้องกับไอทีได้อย่างไร ซึ่งเป็นส่วนหนึ่งของการส่งทอดเป้าหมาย (goal cascade) ดังที่อธิบายในบทที่ 2

รูปภาพที่ 23 ประกอบด้วย
- ในแต่ละสดมภ์(แนวตั้ง) แสดงถึงเป้าหมายทั่วไปที่เกี่ยวข้องกับไอทีทั้งหมด 17 ข้อตามที่ระบุไว้ในบทที่ 2 และจัดเป็นกลุ่มตามมิติของการวัดผลแบบสมดุล (BSC)
- ในแต่ละแถว(แนวนอน) แสดงถึงกระบวนการใน COBIT 5 ทั้งหมด 37 กระบวนการ และจัดเป็นกลุ่มตามโดเมน
- การแสดงให้เห็นว่าเป้าหมายที่เกี่ยวข้องกับไอทีแต่ละข้อได้รับการสนับสนุนจากกระบวนการที่เกี่ยวข้องกับไอทีของ COBIT 5 อย่างไร โดยแสดงเป็นระดับของความสัมพันธ์ดังต่อไปนี้
  - "P" หมายความว่า เป็นความสัมพันธ์ในระดับหลัก ใช้เมื่อความสัมพันธ์มีความสำคัญ ได้แก่ กระบวนการของ COBIT 5 เป็นปัจจัยสนับสนุนหลักที่จะช่วยให้บรรลุเป้าหมายเกี่ยวข้องกับไอที
  - "S" หมายความว่า เป็นความสัมพันธ์ในระดับรอง ใช้เมื่อความสัมพันธ์ชัดเจนแต่มีความสำคัญน้อยกว่า ได้แก่ กระบวนการของ COBIT 5 เป็นปัจจัยสนับสนุนในระดับรองที่จะช่วยให้บรรลุเป้าหมายเกี่ยวข้องกับไอที

ตัวอย่างที่ 8—APO13 การบริหารจัดการการรักษาความมั่นคงปลอดภัย

กระบวนการ APO13 การบริหารจัดการการรักษาความมั่นคงปลอดภัย
- เป็นปัจจัยหลักที่จะช่วยให้บรรลุเป้าหมายที่เกี่ยวข้องกับไอทีต่อไปนี้
  - 02 ไอทีเอื้ออำนวยและสนับสนุนให้ธุรกิจสามารถปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับของหน่วยงานภายนอก
  - 04 ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้
  - 06 ต้นทุน ประโยชน์และความเสี่ยงทางด้านไอทีมีความโปร่งใส
  - 10 ความมั่นคงปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน
  - 14 ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้ และมีประโยชน์ในการตัดสินใจ
- ในระดับความเข้มที่ต่ำลง บรรลุเป้าหมายด้านไอที ที่เกี่ยวข้อง
  - 07 การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ
  - 08 การใช้ระบบงาน สารสนเทศและเทคโนโลยีอย่างเหมาะสม

ตารางข้างต้นจัดทำขึ้นจากข้อมูลดังต่อไปนี้
- การวิจัยของมหาวิทยาลัย Antwerp Management School IT Alignment และ Governance Research Institute
- การสอบทานและความเห็นของผู้เชี่ยวชาญเพิ่มเติมที่ได้รับระหว่างกระบวนการพัฒนาและสอบทาน COBIT 5

เมื่อใช้ตารางในรูปภาพที่ 23 กรุณาพิจารณาถึงข้อสังเกตที่ได้ให้ไว้ในบทที่ 2 เรื่องการใช้การส่งทอดเป้าหมาย ของ COBIT 5

รูปภาพที่ 23— ความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีกับกระบวนการต่างๆ ใน COBIT 5

			เป้าหมายที่เกี่ยวข้องกับไอที																
			กลยุทธ์ด้านไอทีสอดคล้องไปในแนวทางเดียวกันกับกลยุทธ์ด้านธุรกิจ	ไอทีเอื้ออำนวยและสนับสนุนให้ธุรกิจสามารถปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับของหน่วยงานภายนอก	ผู้บริหารระดับสูงให้คำมั่นในการตัดสินใจต่างๆ ที่เกี่ยวข้องกับไอที	ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้	ประโยชน์ที่ได้รับจริงจากกลุ่มของการลงทุนและการให้บริการในด้านต่างๆ ที่มีไอทีเป็นปัจจัยเอื้อ	ต้นทุน ประโยชน์และความเสี่ยงทางด้านไอทีมีความโปร่งใส	การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ	การใช้ระบบงาน สารสนเทศและเทคโนโลยีอย่างเหมาะสม	ความคล่องตัวทางด้านไอที	ความมั่นคงปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน	การใช้สินทรัพย์ ทรัพยากร และสมรรถนะทางด้านไอทีให้ได้ประโยชน์สูงสุด	การเอื้ออำนวยและสนับสนุนการทำงานของกระบวนการทางธุรกิจโดยบูรณาการระบบงานและเทคโนโลยีเข้าไปใช้ในกระบวนการทางธุรกิจ	การส่งมอบชุดโครงการต่างๆ ก่อให้เกิดประโยชน์ ตรงเวลา ตามงบประมาณที่ตั้งไว้ และตามความต้องการและมาตรฐานด้านคุณภาพ	ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้ และมีประโยชน์ในการตัดสินใจ	ไอทีที่ปฏิบัติตามนโยบายภายในขององค์กร	บุคลากรทั้งทางด้านไอทีและด้านธุรกิจที่มีความสามารถและมีแรงจูงใจ	ความรู้ ความเชี่ยวชาญ และความคิดริเริ่มเพื่อนวัตกรรมทางธุรกิจ
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
กระบวนการใน COBIT 5			ด้านการเงิน						ด้านลูกค้า		ด้านกระบวนการภายใน							ด้านการเรียนรู้และเติบโต	
ประเมิน สั่งการ และเฝ้าติดตาม	EDM01	มั่นใจในการกำหนดกรอบการดำเนินงานการกำกับดูแลและการบำรุงรักษา	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	มั่นใจในการส่งมอบผลประโยชน์	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	มั่นใจในความเสี่ยงที่เหมาะสม	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	มั่นใจในการใช้ทรัพยากรให้ได้ประโยชน์สูงสุด	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	มั่นใจในความโปร่งใสต่อผู้มีส่วนได้เสีย	S	S	P			P	P						S	S	S		S
จัดวางแนว จัดทำแผน และจัดระบบ	APO01	บริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	บริหารจัดการกลยุทธ์	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	บริหารจัดการสถาปัตยกรรมองค์กร	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	บริหารจัดการนวัตกรรม	S			S	P			P	P		P	S		S			P
	APO05	บริหารจัดการกลุ่มของชุดโครงการ	P		S	S	P	S	S	S	S		S		P				S
	APO06	บริหารจัดการงบประมาณและต้นทุน	S		S	S	P	P	S	S			S		S				
	APO07	บริหารจัดการทรัพยากรบุคคล	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	บริหารจัดการความสัมพันธ์	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	บริหารจัดการข้อตกลงการให้บริการ	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	บริหารจัดการผู้ขายหรือผู้ให้บริการ		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	บริหารจัดการคุณภาพ	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	บริหารจัดการความเสี่ยง		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	บริหารจัดการความมั่นคงปลอดภัย		P		P		P	S	S		P				P			

รูปภาพที่ 23— ความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีกับกระบวนการต่างๆ ใน COBIT 5 (ต่อ)

กระบวนการใน COBIT 5			เป้าหมายที่เกี่ยวข้องกับไอที																
			กลยุทธ์ด้านไอทีสอดคล้องไปในแนวทางเดียวกันกับกลยุทธ์ด้านธุรกิจ	ไอทีเอื้อด้านบวกและสนับสนุนให้ธุรกิจสามารถปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับของหน่วยงานภายนอก	ผู้บริหารระดับสูงให้ความสำคัญในการตัดสินใจต่างๆ ที่เกี่ยวข้องกับไอที	ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้	ประโยชน์ที่ได้รับจริงจากกลุ่มของการลงทุนและการให้บริการในด้านต่างๆ ที่มีไอทีเป็นปัจจัยเอื้อ	ประโยชน์ที่ได้รับจริงจากกลุ่มของการลงทุนและการให้บริการในด้านต่างๆ ที่มีไอทีเป็นปัจจัยเอื้อ	การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ	การใช้ระบบงาน สารสนเทศและเทคโนโลยีอย่างเหมาะสม	ความคล่องตัวทางด้านไอที	ความมั่นคงปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน	การใช้สินทรัพย์ ทรัพยากร และสมรรถนะบนด้านไอทีให้ได้ประโยชน์สูงสุด	การเลือกอ้างอิงและสนับสนุนการบังคับใช้กฎหมายและกระบวนการทางธุรกิจโดยบูรณาการระบบงานและเทคโนโลยีเข้าไปในกระบวนการทางธุรกิจ	การส่งมอบโครงการต่างๆ ก่อให้เกิดประโยชน์ ตรงเวลา ตามงบประมาณที่ตั้งไว้ และตอบสนองความต้องการของธุรกิจได้	ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้ และมีประโยชน์ในการตัดสินใจ	ไอทีที่ปฏิบัติตามนโยบายภายในขององค์กร	บุคลากรทั้งทางด้านไอทีและด้านธุรกิจมีความเข้าใจและมีแรงจูงใจ	ความรู้ ความเชี่ยวชาญ และความคิดริเริ่มเพื่อนวัตกรรมทางธุรกิจ
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
			ด้านการเงิน						ด้านลูกค้า		ด้านกระบวนการภายใน							ด้านการเรียนรู้และเติบโต	
จัดสร้าง จัดหา และนำไปใช้	BAI01	บริหารจัดการโครงการและชุดโครงการ	P		S	P	P	S	S	S			S		P			S	S
	BAI02	บริหารจัดการข้อกำหนดความต้องการ	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	บริหารจัดการการระบุและจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ	S			S	S		P	S			S	S	S	S			S
	BAI04	บริหารจัดการความพร้อมใช้งานและขีดความสามารถ				S	S		P	S	S		P		S	P			S
	BAI05	บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล	S		S		S		S	P	S		S	S	P				P
	BAI06	บริหารจัดการการเปลี่ยนแปลง			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	บริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน				S	S		S	P	S			P	S	S	S		S
	BAI08	บริหารจัดการความรู้	S				S		S	S	P	S	S			S		S	P
	BAI09	บริหารจัดการสินทรัพย์		S		S		P	S		S	S	P			S	S		
	BAI10	บริหารจัดการองค์ประกอบของระบบ		P		S		S		S	S	S	P			P	S		
ส่งมอบ บริการ และสนับสนุน	DSS01	บริหารจัดการการปฏิบัติการ		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	บริหารจัดการคำร้องขอบริการและเหตุการณ์ที่เกิดขึ้น				P			P	S		S				S	S		S
	DSS03	บริหารจัดการปัญหา		S		P	S		P	S	S		P	S		P	S		S
	DSS04	บริหารจัดการการความต่อเนื่อง	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	บริหารจัดการบริการด้านความมั่นคงปลอดภัย	S	P		P			S	S		P	S	S		S	S		
	DSS06	บริหารจัดการการควบคุมกระบวนการทางธุรกิจ		S		P			P	S		S	S	S		S	S	S	S
เฝ้าติดตาม วัดผล และประเมิน	MEA01	เฝ้าติดตาม วัดผล และประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	เฝ้าติดตาม วัดผล และประเมินระบบการควบคุมภายใน		P		P		S	S	S		S				S	P		S
	MEA03	เฝ้าติดตาม วัดผล และประเมินการปฏิบัติตามข้อกำหนดจากหน่วยงานภายนอก		P		P	S		S			S					S		S

หน้านี้เป็นหน้าว่าง

ภาคผนวก D
ความต้องการของผู้มีส่วนได้เสียและเป้าหมายระดับองค์กร

บทที่ 4 แสดงถึงแต่ละขั้นตอนของการส่งทอดเป้าหมาย (goal cascade) เริ่มจากความต้องการของผู้มีส่วนได้เสียลงไปถึงเป้าหมายของปัจจัยเอื้อ บทที่ 2 ได้รวมเอาตารางที่มีคำถามด้านไอทีที่พบบ่อยเกี่ยวกับการกำกับดูแลและการบริหารจัดการจากมุมมองของผู้มีส่วนได้เสียเป็นที่น่าสนใจว่า คำถามเหล่านี้เกี่ยวข้องกับเป้าหมายระดับองค์กรอย่างไร ด้วยเหตุผลนี้ จึงนำ **รูปภาพที่ 24** มาแสดงเพื่อให้เห็นว่าความต้องการของผู้มีส่วนได้เสียภายในแต่ละรายการมีความเชื่อมโยงกับเป้าหมายระดับองค์กรอย่างไร

ตารางนี้สามารถช่วยกำหนดและจัดลำดับความสำคัญให้กับเป้าหมายระดับองค์กรหรือเป้าหมายที่เกี่ยวข้องกับไอทีบนพื้นฐานของความต้องการของผู้มีส่วนได้เสีย การใช้ตารางนี้มีข้อควรระวังเช่นเดียวกับการใช้ตารางการส่งทอดเป้าหมายอื่นๆ กล่าวคือ แต่ละองค์กรมีสภาพแวดล้อมที่แตกต่างกัน และตารางนี้ไม่ควรได้รับนำมาใช้แบบตรงๆ โดยไม่คำนึงถึงปัจจัยอื่นๆ แต่ควรใช้เป็นเพียงแนวทางที่จะมองหาความสัมพันธ์แบบกว้างๆ เท่านั้น ใน**รูปภาพที่ 24** ช่องที่ตัดกันระหว่างความต้องการของผู้มีส่วนได้เสียกับเป้าหมายระดับองค์กรจะมีข้อมูล หากความต้องการเหล่านั้นควรได้รับการพิจารณาสำหรับเป้าหมายข้อนั้นๆ

รูปภาพที่ 24—ความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรของ COBIT 5 กับคำถามของผู้บริหาร

ความต้องการของผู้มีส่วนได้เสีย	1. คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	2. กลุ่มของผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน	3. ความเสี่ยงทางธุรกิจที่ได้รับการจัดการ (การปกป้องคุ้มครองทรัพย์สิน)	4. การปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับจากภายนอก	5. ความโปร่งใสทางการเงิน	6. วัฒนธรรมที่เน้นการบริการลูกค้า	7. บริการของธุรกิจมีความต่อเนื่องและความพร้อมให้บริการ	8. การตอบสนองอย่างมีประโยชน์ต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	9. การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	10. ต้นทุนในการส่งมอบบริการที่ให้ประโยชน์สูงสุด	11. หน้าที่งานในกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	12. ต้นทุนของกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	13. ชุดโครงการเพื่อการเปลี่ยนแปลงทางธุรกิจที่ได้รับการบริหารจัดการ	14. การปฏิบัติงานและบุคลากรที่มีประสิทธิภาพ	15. การปฏิบัติตามนโยบายภายในองค์กร	16. บุคลากรที่มีทักษะและแรงจูงใจ	17. วัฒนธรรมที่ส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
เราจะได้รับคุณค่าจากการใช้ไอทีได้อย่างไร ผู้ใช้งานมีความพอใจกับคุณภาพของบริการด้านไอทีหรือไม่	■	■				■	■						■			■	■
เราจะจัดการกับประสิทธิภาพด้านไอทีได้อย่างไร		■			■				■	■	■	■		■			
เราจะนำเทคโนโลยีใหม่ๆ มาใช้ให้ดีที่สุดเพื่อเปิดช่องทางกลยุทธ์ได้อย่างไร	■	■						■					■			■	■
เราจะจัดตั้งและจัดโครงสร้างหน่วยงานด้านไอทีให้ดีที่สุดได้อย่างไร								■		■	■	■		■	■	■	
เราต้องพึ่งพาผู้ให้บริการภายนอกมากน้อยเพียงใด มีการจัดการกับสัญญาบริการด้านไอทีกับบุคคลภายนอกได้ดีเพียงใด เราจะเชื่อมั่นในผู้ให้บริการภายนอกได้อย่างไร			■	■						■							
มีข้อกำหนด (ด้านการควบคุม) อะไรบ้างเกี่ยวกับสารสนเทศ				■					■						■		
เราได้ระบุถึงความเสี่ยงที่เกี่ยวข้องทั้งหมดแล้ว หรือยัง			■				■		■						■		
เรามีการดำเนินงานด้านไอทีที่มีประสิทธิภาพและด้านทานภัยต่างๆ ได้หรือไม่					■		■										
เราจะควบคุมต้นทุนด้านไอทีได้อย่างไร เราจะใช้ทรัพยากรด้านไอทีให้มีประสิทธิภาพและประสิทธิผลได้อย่างไร ทางเลือกใดที่มีประสิทธิภาพและประสิทธิผลมากที่สุดในการจ้างหน่วยงานภายนอก										■		■		■			
เรามีบุคลากรที่เพียงพอสำหรับงานด้านไอทีหรือไม่ เราจะพัฒนาและรักษาทักษะของบุคลากรได้อย่างไร และจะจัดการประสิทธิภาพในการทำงานได้อย่างไร										■		■		■			
เราจะมีความเชื่อมั่นในเรื่องของไอทีได้อย่างไร				■											■		

รูปภาพที่ 24—ความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรของ COBIT 5 กับคำถามของผู้บริหาร (ต่อ)

ความต้องการของผู้มีส่วนได้เสีย	คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	กลุ่มของผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน	ความเสี่ยงทางธุรกิจที่เกี่ยวข้องกับการจัดการ (การปกป้องคุ้มครองทรัพย์สิน)	การปฏิบัติตามกฎหมายและระเบียบข้อบังคับด้านภายนอก	ความโปร่งใสทางการเงิน	วัฒนธรรมที่เน้นการบริการลูกค้า	บริการของธุรกิจมีความต่อเนื่องและความพร้อมให้บริการ	การตอบสนองอย่างมีประสิทธิภาพต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	ต้นทุนในการส่งมอบบริการที่ให้ประโยชน์สูงสุด	หน่วยงานในกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	ต้นทุนของกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	ชุดโครงการเพื่อการเปลี่ยนแปลงทางธุรกิจที่ได้รับการบริหารจัดการ	การปฏิบัติงานและบุคลากรที่มีประสิทธิภาพ	การปฏิบัติตามนโยบายภายในองค์กร	บุคลากรที่มีทักษะและแรงจูงใจ	วัฒนธรรมที่ส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
ข้อมูลที่ได้รับการประมวลผลมีความปลอดภัยหรือไม่				■			■								■		
เราจะเพิ่มความคล่องตัวให้กับธุรกิจด้วยการมีสภาพแวดล้อมด้านไอทีที่มีความยืดหยุ่นได้อย่างไร	■							■								■	■
โครงการด้านไอทีประสบความล้มเหลวที่จะส่งมอบงานตามที่กำหนดหรือไม่ ถ้าใช่ เป็นด้วยสาเหตุใด ไอทีเป็นอุปสรรคในการดำเนินกลยุทธ์ทางธุรกิจหรือไม่	■	■	■					■			■	■	■				
ไอทีมีความสำคัญเพียงใดต่อความอยู่รอดขององค์กร จะทำอย่างไรหากไอทีไม่พร้อมใช้	■	■					■										
กระบวนการทางธุรกิจที่เป็นหลักสำคัญในการดำเนินธุรกิจใดที่ต้องพึ่งพาไอที และกระบวนการเหล่านั้นต้องการอะไรบ้าง	■	■									■	■					
มีการใช้จ่ายเกินงบประมาณสำหรับการปฏิบัติงานด้านไอทีโดยเฉลี่ยเท่าไร โครงการด้านไอทีมีการใช้จ่ายเงินเกินงบประมาณบ่อยครั้งหรือไม่และเป็นจำนวนเงินมากน้อยเพียงใด					■					■		■		■			
มีการใช้ความพยายามไปในการแก้ปัญหาเฉพาะหน้ามากกว่าการปรับปรุงทางธุรกิจมากน้อยเพียงใด		■	■									■					
มีทรัพยากรทางไอทีที่เพียงพอและมีโครงสร้างพื้นฐานที่พร้อมใช้ในการบรรลุถึงวัตถุประสงค์ด้านกลยุทธ์ขององค์กรหรือไม่		■			■					■		■					
การตัดสินใจในเรื่องสำคัญๆ ทางด้านไอทีใช้เวลานานมากน้อยเพียงใด	■	■			■			■									
การใช้กำลังคนและการลงทุนทางด้านไอทีมีความโปร่งใสหรือไม่		■		■	■										■		
ไอทีใช้ในการสนับสนุนองค์กรในการปฏิบัติตามกฎระเบียบข้อบังคับต่างๆ และระดับของการให้บริการหรือไม่ จะทราบได้อย่างไรว่าเราได้ปฏิบัติตามกฎระเบียบข้อบังคับต่างๆ ที่ใช้บังคับทั้งหมดแล้ว				■											■		

ภาคผนวก E
การเทียบ COBIT 5 กับมาตรฐาน/กรอบการดำเนินการอื่นที่เกี่ยวข้องและเกี่ยวเนื่องกันมากที่สุด

บทนำ

ในภาคผนวกนี้ได้เปรียบเทียบ COBIT กับมาตรฐาน/กรอบดำเนินงานอื่นที่เกี่ยวเนื่องและใช้กันมากที่สุดในด้านการกำกับดูแล สำหรับ ISO /IEC 38500 การเปรียบเทียบอยู่บนพื้นฐานของหลักการใน ISO /IEC 38500 สำหรับการเปรียบเทียบอื่นๆ การเปรียบเทียบจะอยู่ในรูปแบบของตารางโดยนำกระบวนการของ COBIT 5 ไปเทียบกับเนื้อหาในมาตรฐานและกรอบดำเนินงานต่างๆ ที่นำมาอ้างอิงถึง

COBIT 5 และ ISO /IEC 38500

ข้อมูลด้านล่างนี้ให้ข้อสรุปว่า COBIT 5 สนับสนุนการประยุกต์ใช้หลักการของมาตรฐานและวิธีปฏิบัติสำหรับการนำไปใช้งานอย่างไร มาตรฐาน *ISO /IEC 38500 ของปีค.ศ. 2008 การกำกับดูแลองค์กรด้านเทคโนโลยีสารสนเทศ (Corporate governance of information technology)* ตั้งอยู่บนหลักการสำคัญ 6 ประการ ความหมายเชิงปฏิบัติสำหรับหลักการในแต่ละข้อได้อธิบายไว้ในที่นี้ พร้อมกับคำอธิบายว่าแนวทางของ COBIT 5 เอื้อให้เกิดแนวปฏิบัติที่ดีได้อย่างไร

หลักการของ ISO /IEC 38500

หลักการที่ 1 – ความรับผิดชอบ
มีความหมายอย่างไรในทางปฏิบัติ

ธุรกิจ(ลูกค้า)และฝ่ายไอที (ผู้ให้บริการ) ควรร่วมมือกันแบบเป็นพันธมิตรที่มีการสื่อสารกันอย่างมีประสิทธิผลบนพื้นฐานของความสัมพันธ์ที่ดีและมีความเชื่อใจกัน และแสดงถึงความชัดเจนในหน้าที่ความรับผิดชอบและความรับผิดชอบในผลงานตามหน้าที่ (accountability) สำหรับในองค์กรขนาดใหญ่ คณะกรรมการด้านไอที (IT executive committee) (หรือมักเรียกว่าคณะกรรมการกลยุทธ์ด้านไอที - IT Strategy Committee) ปฏิบัติหน้าที่ ในนามของคณะกรรมการบริหารและมีประธานที่แต่งตั้งจากสมาชิกของคณะกรรมการบริหาร ถือเป็นกลไกที่มีประสิทธิผลมากสำหรับการประเมิน สั่งการ และเฝ้าติดตามการใช้ไอทีในองค์กร และสำหรับการแนะนำคณะกรรมการในประเด็นด้านไอทีที่สำคัญ กรรมการสำหรับองค์กรขนาดเล็กและขนาดกลาง ที่มีสายบังคับบัญชาที่ไม่ซับซ้อนและมีเส้นทางการสื่อสารที่สั้น จำเป็นต้องใช้วิธีปฏิบัติที่เข้าถึงโดยตรง (Direct approach) มากกว่าในการดูแลกิจกรรมทางด้านไอที และไม่ว่าจะเป็นกรณีใดก็ตาม หน่วยงานที่มีหน้าที่กำกับดูแลจะต้องสั่งการให้มี โครงสร้างองค์กร บทบาทหน้าที่และความรับผิดชอบที่เหมาะสมสำหรับการกำกับดูแล เพื่อให้มีความชัดเจนถึงความเป็นเจ้าของและความรับผิดชอบในผลงานอย่างชัดเจนสำหรับการตัดสินใจและภารกิจที่สำคัญ ซึ่งควรรวมถึง ความสัมพันธ์กับผู้ให้บริการหลักด้านไอทีหลักจากภายนอก

แนวทางของ ISACA เอื้อต่อแนวปฏิบัติที่ดีอย่างไร

1. กรอบดำเนินงาน COBIT 5 ระบุถึงปัจจัยเอื้อจำนวนหนึ่งสำหรับการกำกับดูแลไอทีระดับองค์กร ปัจจัยเอื้อด้าน "กระบวนการ" และปัจจัยเอื้อด้าน "โครงสร้างองค์กร" ประกอบกับตาราง RACI[13] มีความเกี่ยวพันกันในบริบทนี้ โดยสนับสนุนให้มีการมอบหมายหน้าที่ความรับผิดชอบ และให้ตัวอย่างบทบาทหน้าที่และความรับผิดชอบสำหรับสมาชิกของคณะกรรมการบริหารและผู้บริหารในเรื่องของกระบวนการและกิจกรรมที่สำคัญทั้งหมด
2. *การนำ COBIT 5 ไปใช้งาน (COBIT 5 Implementation)* อธิบายถึงหน้าที่ความรับผิดชอบของผู้มีส่วนได้เสียและกลุ่มที่มีส่วนร่วมอื่นๆ เมื่อนำการกำกับดูแลด้านไอทีไปใช้หรือปรับปรุงให้ดีขึ้น
3. COBIT 5 มีการเฝ้าติดตาม 2 ระดับ ระดับแรกมีความเกี่ยวข้องกับบริบทของการกำกับดูแล กระบวนการ EDM05 *มั่นใจในความโปร่งใสต่อผู้มีส่วนได้เสีย (ensure stakeholder transparency)* อธิบายถึงบทบาทของกรรมการในการเฝ้าติดตามและประเมินการกำกับดูแลด้านไอทีและประสิทธิภาพในการทำงานด้านไอทีด้วยวิธีทั่วไปสำหรับการกำหนดเป้าหมายและวัตถุประสงค์และมาตรวัดที่เกี่ยวข้อง

หลักการที่ 2 กลยุทธ์
มีความหมายอย่างไรในทางปฏิบัติ

การวางแผนกลยุทธ์ทางไอทีมีความซับซ้อนและมีความสำคัญยิ่งที่ต้องมีความร่วมมือกันอย่างใกล้ชิดระหว่างหน่วยงานด้านธุรกิจในองค์กรและไอที เราจำเป็นต้องให้ลำดับความสำคัญสำหรับแผนที่มีโอกาสที่จะบรรลุผลประโยชน์ตามคาดหวังและสำหรับการจัดสรรทรัพยากรอย่างมีประสิทธิผล เป้าหมายในภาพรวมต้องแปลงมาเป็นแผนยุทธวิธีที่สามารถทำให้บรรลุผลได้ เพื่อลดโอกาสเกิดความล้มเหลวหรือเหตุการณ์ที่ไม่คาดคิด โดยมีเป้าหมายคือการส่งมอบคุณค่าเพื่อสนับสนุนวัตถุประสงค์ของกลยุทธ์ไปพร้อมๆ กับการพิจารณาถึงความเสี่ยงที่เกี่ยวข้องกับการยอมรับความเสี่ยงของคณะกรรมการบริหาร แม้ว่าจะเป็นเรื่องสำคัญที่จะต้องส่งทอดแผนในลักษณะจากบนไปสู่ล่าง แต่แผนก็ต้องยืดหยุ่นและสามารถปรับให้รองรับความต้องการทางธุรกิจและโอกาสทางด้านไอทีที่มีการเปลี่ยนแปลงอย่างรวดเร็วด้วย

นอกจากนี้ การมีหรือขาดความสามารถด้านไอที สามารถเอื้อหรือขัดขวางกลยุทธ์ทางธุรกิจได้ ดังนั้นการวางแผนกลยุทธ์

[13]ตาราง RACI แสดงให้เห็นว่าใครเป็นผู้รับผิดชอบตามหน้าที่ (Responsible) ผู้รับผิดชอบในผลงาน (Accountable) ผู้ให้คำแนะนำปรึกษา (Consulted) และผู้ที่จะต้องได้รับแจ้งให้ทราบ (Informed) สำหรับงานหนึ่งๆ

ด้านไอทีควรรวมถึงการวางแผนความสามารถด้านไอทีที่โปร่งใสและเหมาะสม โดยรวมถึงการประเมินความสามารถของโครงสร้างพื้นฐานด้านไอทีและทรัพยากรบุคคลในปัจจุบัน เพื่อรองรับความต้องการของธุรกิจในอนาคต และพิจารณาถึงการพัฒนาเทคโนโลยีในอนาคตที่อาจช่วยให้เกิดความได้เปรียบในการแข่งขันและ/หรือต้นทุนที่เกิดประโยชน์สูงสุด ทรัพยากรด้านไอทียังรวมถึงความสัมพันธ์กับผู้ขายผลิตภัณฑ์และผู้ให้บริการต่างๆภายนอก ซึ่งบางรายอาจมีบทบาทสำคัญในการสนับสนุนการดำเนินงานของธุรกิจ ดังนั้นการกำกับดูแลกลยุทธ์ในการจัดซื้อจัดหานี้จึงมีนัยสำคัญมากในกิจกรรมการวางแผนกลยุทธ์ที่ต้องการทิศทางและการควบคุมดูแลจากผู้บริหารระดับสูง

แนวทางของ ISACA เอื้อต่อแนวปฏิบัติที่ดีอย่างไร

1.COBIT 5 ให้แนวทางเฉพาะในการจัดการการลงทุนด้านไอทีและ (โดยเฉพาะในกระบวนการ EDM02 *มั่นใจในการส่งมอบประโยชน์* ของโดเมนการกำกับดูแล) วัตถุประสงค์ด้านกลยุทธ์ควรได้รับการสนับสนุนจากเหตุผลทางธุรกิจต่างๆ ที่เหมาะสมอย่างไร

2.โดเมน APO ใน COBIT 5 อธิบายถึงกระบวนการที่จำเป็นเพื่อการวางแผนและการจัดการอย่างเป็นระบบที่มีประสิทธิผลสำหรับทรัพยากรด้านไอทีทั้งภายในและภายนอก ซึ่งรวมถึงการวางแผนกลยุทธ์ การวางแผนด้านเทคโนโลยีและสถาปัตยกรรม การวางแผนองค์กร การวางแผนนวัตกรรม การบริหารกลุ่มของชุดโครงการ การบริหารเงินลงทุน การบริหารความเสี่ยง การบริหารความสัมพันธ์ และการบริหารคุณภาพ มีการอธิบายถึงความสอดคล้องกันระหว่างเป้าหมายทางธุรกิจและเป้าหมายด้านไอทีด้วยตัวอย่างทั่วไปที่แสดงให้เห็นถึงการสนับสนุนวัตถุประสงค์ด้านกลยุทธ์สำหรับกระบวนการที่เกี่ยวข้องกับไอทีจากการวิจัยอย่างกว้างขวางในอุตสาหกรรม

3.การระบุและวางแนวเป้าหมายระดับองค์กรและเป้าหมายที่เกี่ยวข้องกับไอทีให้สอดคล้องกัน ช่วยให้เกิดความเข้าใจที่ดีขึ้นในความสัมพันธ์ที่ส่งทอดถึงกันระหว่างเป้าหมายระดับองค์กร เป้าหมายที่เกี่ยวข้องกับไอที และปัจจัยเอื้อต่างๆ ซึ่งรวมถึงกระบวนการด้านไอที โดยได้แสดงรายการที่เป็นเป้าหมายทั่วไประดับองค์กรที่ชัดเจนและสมบูรณ์ 17 ข้อและเป้าหมายทั่วไปที่เกี่ยวข้องกับไอทีอีก 17 ข้อ ที่ได้รับการตรวจสอบความสมเหตุสมผลและจัดลำดับความสำคัญสำหรับภาคส่วนต่างๆ อีกทั้งสารสนเทศที่เชื่อมโยงกันระหว่างเป้าหมายทั้งสองระดับเป็นพื้นฐานที่ดีที่ในการส่งทอดเป้าหมายทางธุรกิจไปยังเป้าหมายที่เกี่ยวข้องกับไอที

หลักการที่ 3 การจัดซื้อจัดหา (Acquisition)

มีความหมายอย่างไรในทางปฏิบัติ

กระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จด้านไอทีมีไว้เพื่อสนับสนุนกระบวนการด้านธุรกิจ ดังนั้นจึงต้องระมัดระวังที่จะไม่นำกระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จด้านไอทีไปพิจารณาแยกต่างหาก หรือมองเป็นเพียงแค่โครงการหรือบริการด้านเทคโนโลยีเท่านั้น ในทางกลับกัน การเลือกสถาปัตยกรรมของเทคโนโลยีที่ไม่เหมาะสม ความล้มเหลวที่จะทำให้โครงสร้างพื้นฐานด้านเทคนิคทันสมัยและเหมาะสม หรือการขาดบุคคลากรที่มีทักษะ ล้วนสามารถส่งผลให้โครงการล้มเหลว ขาดความสามารถที่จะดำเนินกิจกรรมทางธุรกิจได้อย่างยั่งยืน หรือลดคุณค่าที่มีต่อธุรกิจ การจัดซื้อจัดหาทรัพยากรด้านไอทีจึงควรพิจารณาเสมือนเป็นส่วนหนึ่งของการเปลี่ยนแปลงทางธุรกิจโดยมีไอทีเป็นปัจจัยเอื้อ เทคโนโลยีที่จัดซื้อมาจะต้องสนับสนุนและสามารถทำงานร่วมกับกระบวนการทางธุรกิจและโครงสร้างพื้นฐานด้านไอทีที่องค์กรมีอยู่แล้วและที่วางแผนไว้ การนำไปใช้งานก็ไม่ใช่เป็นเพียงแค่ประเด็นด้านเทคโนโลยีเท่านั้น แต่จะต้องผสมผสานไปกับการเปลี่ยนแปลงองค์กร การปรับปรุงกระบวนการทางธุรกิจ การฝึกอบรม และการเอื้อให้เกิดการเปลี่ยนแปลงด้วย ดังนั้น โครงการด้านไอทีควรเป็นส่วนหนึ่งของชุดโครงการ (programmes) เพื่อการเปลี่ยนแปลงในระดับองค์กร ซึ่งรวมเอาโครงการต่างๆ ที่มีการดำเนินกิจกรรมครบในทุกด้านตามที่ต้องการเพื่อช่วยให้มั่นใจว่าจะได้รับผลสำเร็จ

แนวทางของ ISACA เอื้อต่อแนวปฏิบัติที่ดีได้อย่างไร

1.โดเมน EDM ของ COBIT 5 ให้แนวทางในการกำกับดูแลและการบริหารจัดการการลงทุนของธุรกิจที่มีไอที เป็นปัจจัยเอื้อผ่านทางวัฏจักรที่ครบกระบวนการ (การจัดซื้อจัดหา การนำไปติดตั้งใช้งาน การปฏิบัติงาน และการเลิกใช้งาน) กระบวนการ APO05 *บริหารจัดการกลุ่มของชุดโครงการ (Manage portfolio)* ระบุถึงการนำการบริหารจัดการกลุ่มของชุดโครงการและชุดโครงการของที่มีการลงทุนมาใช้ให้มีประสิทธิผลเพื่อช่วยให้มั่นใจได้ว่าจะได้รับผลประโยชน์จริงและมีต้นทุนที่เหมาะสม

2.โดเมน APO ใน COBIT 5 ให้แนวทางสำหรับการวางแผนในการจัดซื้อจัดจ้าง ซึ่งรวมถึงการวางแผนการลงทุน การบริหารความเสี่ยง การวางแผนชุดโครงการและโครงการ และการวางแผนด้านคุณภาพ

3.โดเมน BAI ใน COBIT 5 ให้แนวทางสำหรับกระบวนการที่จำเป็นในการจัดซื้อจัดหาและการนำกระบวนการแก้ปัญหาแบบเบ็ดเสร็จด้านไอที(IT solution) ไปใช้งาน ซึ่งครอบคลุมถึงการระบุความต้องการ การระบุการแก้ปัญหาแบบเบ็ดเสร็จที่เป็นไปได้ การจัดเตรียมเอกสาร การฝึกอบรมและการเอื้อให้กับผู้ใช้งานและการปฏิบัติการในการใช้ระบบใหม่ นอกจากนี้แนวทางนี้ยังช่วยให้มั่นใจว่า กระบวนการแก้ปัญหาแบบเบ็ดเสร็จนี้ได้รับการทดสอบและควบคุมอย่างเหมาะสมเมื่อการเปลี่ยนแปลงได้รับมาใช้ในสภาพแวดล้อมของการดำเนินงานจริงทั้งทางด้านธุรกิจและไอที

4.โดเมน MEA ใน COBIT 5 และกระบวนการ EDM05 ได้รวมเอาแนวทางสำหรับกรรมการให้สามารถเฝ้าติดตามและประเมินกระบวนการจัดซื้อจัดหาและการควบคุมภายใน เพื่อช่วยให้มั่นใจว่าการจัดซื้อจัดหาได้รับการบริหารจัดการและดำเนินการอย่างเหมาะสม

หลักการที่ 4 ผลการดำเนินงาน
มีความหมายอย่างไรในทางปฏิบัติ
การวัดผลการดำเนินงานที่มีประสิทธิผลขึ้นอยู่กับมุมมองหลัก 2 ด้านคือ คำจำกัดความที่ชัดเจนของคำว่า "ผลการดำเนินงานเป้าหมาย" และ "การจัดทำมาตรวัดที่มีประสิทธิผลสำหรับการเฝ้าติดตามการบรรลุเป้าหมาย" เราจำเป็นต้องมีกระบวนการในการวัดผลการดำเนินงานเพื่อให้มั่นใจว่า ผลการดำเนินงานนั้นได้รับการเฝ้าติดตามอย่างสม่ำเสมอและเชื่อถือได้ การกำกับดูแลจะมีประสิทธิผลก็ต่อเมื่อวัตถุประสงค์กำหนดมาจากบนลงล่างซึ่งสอดคล้องกับเป้าหมายทางธุรกิจในภาพรวมที่ได้รับอนุมัติ และมาตรวัดจัดทำขึ้นจากล่างขึ้นบนซึ่งสอดคล้องไปในทางที่เอื้อให้บรรลุเป้าหมายในทุกระดับโดยมีผู้บริหารของแต่ละระดับชั้นเฝ้าติดตาม ปัจจัยสำคัญสู่ความสำเร็จในการกำกับดูแล 2 ปัจจัยคือ การที่ผู้มีส่วนได้เสียอนุมัติเป้าหมาย และการที่บุคลากรในระดับกรรมการและผู้จัดการ ยอมรับความรับผิดชอบในผลงาน (accountability) ในการบรรลุเป้าหมาย ไอทีเป็นหัวข้อที่มีความซับซ้อนและมีรายละเอียดเชิงเทคนิค ดังนั้น จึงเป็นสิ่งที่สำคัญที่จะต้องมีความโปร่งใสโดยการสื่อถึงเป้าหมาย มาตรวัด และการรายงานผลการดำเนินงานในภาษาที่เข้าใจได้ง่ายสำหรับผู้มีส่วนได้เสีย เพื่อให้มีการดำเนินการอย่างเหมาะสม

แนวทางของ ISACA เอื้อต่อแนวปฏิบัติที่ดีได้อย่างไร
1. กรอบการดำเนินงานของ COBIT 5 ให้ตัวอย่างทั่วไปที่แสดงถึงเป้าหมายและมาตรวัดที่ครบถ้วนสำหรับกระบวนการที่เกี่ยวข้องกับไอทีและปัจจัยเอื้ออื่นๆและยังแสดงให้เห็นถึงความเกี่ยวข้องกับเป้าหมายทางธุรกิจ ซึ่งเอื้อให้องค์กรสามารถนำมาปรับใช้ให้เข้ากับการใช้งานเฉพาะองค์กรได้
2. COBIT 5 ให้แนวทางสำหรับผู้บริหารในการกำหนดเป้าหมายด้านไอทีให้สอดคล้องกับเป้าหมายทางธุรกิจ และอธิบายว่าเราสามารถเฝ้าติดตามผลการดำเนินงานของวัตถุประสงค์เหล่านี้โดยการใช้เป้าหมายและมาตรวัดต่างๆ ได้อย่างไร เราสามารถประเมินความสามารถของกระบวนการได้โดยการใช้ต้นแบบการประเมินความสามารถตามที่ระบุไว้ใน ISO/IEC 11504
3. กระบวนการหลักใน COBIT 5 2 กระบวนการ ได้ให้แนวทางที่เฉพาะเจาะจงคือ
   -APO02 *บริหารจัดการกลยุทธ์ (Manage strategy)* เน้นในเรื่องการกำหนดเป้าหมาย
   -APO09 *บริหารจัดการข้อตกลงการให้บริการ (Manage service agreements)* เน้นในเรื่องการกำหนดบริการ และเป้าหมายของบริการที่เหมาะสม และจัดทำเป็นลายลักษณ์อักษรไว้ในข้อตกลงระดับการบริการ
4. ในกระบวนการ MEA01 *เฝ้าติดตาม วัดผล และประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน (Monitor, evaluate and assess performance and conformance)* ของ COBIT 5 ให้แนวทางเกี่ยวกับหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงในกิจกรรมนี้
5. *แนวทางการให้ความเชื่อมั่นสำหรับ COBIT 5 (COBIT 5 for Assurance)* ที่มีแผนจะนำออกสู่ตลาดในอนาคตจะอธิบายว่า ผู้ประกอบวิชาชีพเกี่ยวกับการให้ความเชื่อมั่น สามารถให้ความเชื่อมั่นที่เป็นอิสระแก่กรรมการในเรื่องประสิทธิภาพของการดำเนินงานด้านไอทีได้อย่างไร

หลักการที่ 5 ความสอดคล้องกัน
มีความหมายอย่างไรในทางปฏิบัติ
ตลาดโลกในวันนี้มีอินเตอร์เน็ตและเทคโนโลยีที่ก้าวหน้าเป็นปัจจัยเอื้อ องค์กรจำเป็นต้องปฏิบัติตามข้อกำหนดด้านกฎหมายและกฎระเบียบข้อบังคับที่มีจำนวนเพิ่มมากขึ้น จากข่าวอื้อฉาวและความล้มเหลวด้านการเงินของบริษัทต่างๆ เมื่อไม่กี่ปีที่ผ่านมา ทำให้คณะกรรมการเกิดความตระหนักอย่างมากในเรื่องของกฎหมายและกฎระเบียบข้อบังคับที่ออกมาบังคับใช้ซึ่งเข้มข้นขึ้นและผลกระทบที่มี ผู้มีส่วนได้เสียต้องการความเชื่อมั่นเพิ่มขึ้นว่า ในการดำเนินงานจริงองค์กรได้ปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับ และดำเนินการตามแนวปฏิบัติที่ดีด้านการกำกับดูแลองค์กรแล้ว นอกจากนี้ จากการที่ไอทีได้เอื้อให้เกิดกระบวนการทางธุรกิจระหว่างองค์กรอย่างไร้รอยต่อ จึงมีความจำเป็นที่จะต้องมั่นใจได้ว่า สัญญาต่างๆ ครอบคลุมถึงข้อกำหนดที่เกี่ยวข้องกับไอที ในเนื้อหาอาทิเช่น การรักษาความเป็นส่วนบุคคล การรักษาความลับ การรักษาสินทรัพย์ทางปัญญา และการรักษาความมั่นคงปลอดภัย เป็นต้น

กรรมการจำเป็นต้องมั่นใจได้ว่า การปฏิบัติตามข้อกำหนดจากองค์กรภายนอกถือเป็นส่วนหนึ่งของการวางแผนกลยุทธ์มากกว่าที่จะให้เกิดความเสียหายขึ้นแล้วค่อยมาคิดทีหลัง กรรมการยังจำเป็นต้องกำหนดแนวทางจากผู้บริหารระดับสูงพร้อมทั้งกำหนดเป็นนโยบายและขั้นตอนการปฏิบัติงานให้ผู้บริหารและพนักงานปฏิบัติตามเพื่อให้มั่นใจว่าได้บรรลุเป้าหมายขององค์กร ลดความเสี่ยง และมีการปฏิบัติตาม(กฎหมาย/กฎระเบียบข้อบังคับ) ผู้บริหารระดับสูงจะต้องทำให้เกิดความสมดุลระหว่างประสิทธิภาพในการดำเนินงานและการปฏิบัติตาม(กฎหมาย/กฎระเบียบข้อบังคับ) เพื่อให้มั่นใจว่าเป้าหมายของประสิทธิภาพในการดำเนินงานไม่ขัดแย้งกับการปฏิบัติตาม (กฎหมาย/กฎระเบียบข้อบังคับ) และในทางตรงกันข้าม การปฏิบัติตาม(กฎหมาย/กฎระเบียบข้อบังคับ) ก็ต้องมีความเหมาะสม ไม่เข้มงวดมากจนเกินไปกับการดำเนินธุรกิจ

แนวทางของ ISACA เอื้อต่อแนวปฏิบัติที่ดีได้อย่างไร
1. แนวปฏิบัติในการกำกับดูแลและการบริหารจัดการของ COBIT 5 ให้พื้นฐานในการสร้างสภาพแวดล้อมในการควบคุมที่เหมาะสมในองค์กร การประเมินความสามารถของกระบวนการเอื้อให้ผู้บริหารสามารถประเมินและเปรียบเทียบความสามารถของกระบวนการด้านไอที
2. กระบวนการ AOP02 *บริหารจัดการกลยุทธ์ (Manage strategy)* ของ COBIT 5 ช่วยให้มั่นใจว่าแผนด้านไอทีสอดคล้องกับวัตถุประสงค์ทางธุรกิจในภาพรวม ซึ่งรวมถึงข้อกำหนดด้านการกำกับดูแลด้วย
3. กระบวนการ MEA02 *เฝ้าติดตาม วัดผล และประเมินระบบการควบคุมภายใน (Monitor, evaluate and assess the system of internal control)* ของ COBIT 5 เอื้อให้กรรมการสามารถประเมินว่า การควบคุมเพียงพอต่อการปฏิบัติตามข้อกำหนดต่างๆ หรือไม่
4. กระบวนการ MEA03 *เฝ้าติดตาม วัดผล และประเมินการปฏิบัติตามข้อกำหนดจากหน่วยงานภายนอก (Monitor, evaluate*

and assess compliance with external requirements) ช่วยให้มั่นใจว่า มีการระบุถึงข้อกำหนดที่ต้องปฏิบัติตาม กรรมการได้กำหนดทิศทางสำหรับการปฏิบัติ และ มีการเฝ้าติดตาม ประเมิน และรายงานผลการปฏิบัติตามข้อกำหนดด้านไอที เสมือนเป็นส่วนหนึ่งของการปฏิบัติข้อกำหนดอื่นๆ ขององค์กร

5. *แนวทางการให้ความเชื่อมั่นสำหรับ COBIT 5 (COBIT 5 for Assurance)* อธิบายว่า ผู้ตรวจสอบจะให้ความเชื่อมั่นอย่างเป็นอิสระได้อย่างไรเกี่ยวกับการปฏิบัติตามและการยึดมั่นในนโยบายภายในที่มาจากการสั่งการภายใน ข้อกำหนดตามกฎหมายและตามสัญญา และยืนยันว่าเจ้าของกระบวนการที่รับผิดชอบได้ดำเนินการแก้ไขเพื่ออุดช่องว่างของการปฏิบัติตามข้อกำหนดในเวลาที่เหมาะสม

หลักการที่ 6 พฤติกรรมบุคคล
มีความหมายอย่างไรในทางปฏิบัติ

การนำการเปลี่ยนแปลงใดๆ ที่มีไอทีเป็นปัจจัยเอื้อไปใช้งาน ซึ่งรวมถึงการกำกับดูแลด้านไอทีด้วย มักต้องมีการเปลี่ยนแปลงอย่างเป็นนัยสำคัญต่อวัฒนธรรมและพฤติกรรมภายในองค์กร เช่นเดียวกับลูกค้าและพันธมิตรทางธุรกิจ ซึ่งอาจสร้างความวิตกและความไม่เข้าใจให้เกิดขึ้นท่ามกลางหมู่พนักงาน ดังนั้น การนำไปใช้จึงจำเป็นต้องได้รับการจัดการอย่างระมัดระวังเพื่อให้บุคลากรยังคงมีทัศนคติที่ดีในการทำงาน กรรมการจะต้องสื่อสารเป้าหมายอย่างชัดเจนและแสดงให้เห็นว่าเป็นผู้สนับสนุนการเปลี่ยนแปลงที่นำเสนอนั้น การฝึกอบรมและการเพิ่มทักษะของบุคลากรเป็นกุญแจสำคัญสำหรับการปลี่ยนแปลง โดยเฉพาะการเปลี่ยนแปลงด้านเทคโนโลยีที่มักเกิดขึ้นอย่างรวดเร็ว ไอทีมีผลกระทบต่อบุคลากรทุกระดับในองค์กร ไม่ว่าจะเป็นผู้มีส่วนได้เสีย ผู้จัดการ และผู้ใช้งาน หรือผู้เชี่ยวชาญที่ให้บริการที่เกี่ยวข้องกับไอทีและกระบวนการแก้ปัญหาแบบเบ็ดเสร็จให้กับองค์กร และ กระบวนการแก้ปัญหาแบบเบ็ดเสร็จแก่ธุรกิจ นอกจากส่งผลกระทบภายในองค์กรแล้ว ไอทียังส่งผลกระทบต่อลูกค้าและพันธมิตรทางธุรกิจ ทั้งยังเอื้อให้เกิดการบริการตนเองและการทำธุรกรรมอัตโนมัติระหว่างองค์กรทั้งภายในประเทศและข้ามประเทศ แม้ว่ากระบวนการทางธุรกิจที่มีไอทีเป็นปัจจัยเอื้อจะนำมาซึ่งประโยชน์และโอกาสใหม่ๆ แต่ก็มาพร้อมกับความเสี่ยงต่างๆ ที่เพิ่มขึ้นด้วย ประเด็นปัญหาเช่นข้อมูลส่วนบุคคลและการทุจริตเป็นเรื่องที่บุคคลมีความวิตกกังวลเพิ่มมากขึ้น และความเสี่ยงนี้พร้อมทั้งความเสี่ยงอื่นๆ ต้องได้รับการจัดการเพื่อให้ผู้ใช้เกิดความเชื่อมั่นในระบบไอทีที่ใช้อยู่ ระบบสารสนเทศยังส่งผลกระทบต่อแนวปฏิบัติในการทำงานอย่างมากโดยการแปลงขั้นตอนการปฏิบัติงานที่ทำโดยคนให้เป็นการทำงานโดยอัตโนมัติ

แนวทางของ ISACA เอื้อต่อแนวปฏิบัติที่ดีได้อย่างไร

ปัจจัยเอื้อใน COBIT 5 (รวมถึงกระบวนการต่างๆ) ต่อไปนี้ ให้แนวทางเกี่ยวกับความต้องการที่เกี่ยวข้องกับพฤติกรรมบุคคล

1. ปัจจัยเอื้อของ COBIT 5 รวมถึง คน ทักษะ ความสามารถ วัฒนธรรม จริยธรรม และพฤติกรรม สำหรับแต่ละ ปัจจัยเอื้อจะมีต้นแบบที่ใช้จัดการกับปัจจัยเอื้อโดยแสดงเป็นตัวอย่างให้เห็น
2. กระบวนการ APO07 *บริหารจัดการทรัพยากรบุคคล (Manage human resources)* ใน COBIT 5 อธิบายว่า ผลการดำเนินงานของแต่ละบุคคลควรจะสอดคล้องกับเป้าหมายขององค์กรได้อย่างไร ทักษะของผู้เชี่ยวชำนาญด้านไอทีจะถูกรักษาไว้ได้อย่างไร และบทบาทหน้าที่และความรับผิดชอบควรถูกกำหนดขึ้นมาอย่างไร
3. กระบวนการ BAI02 *บริหารจัดการข้อกำหนดความต้องการ (Manage requirements definition)* ใน COBIT 5 ช่วยให้มั่นใจว่า การออกแบบระบบงานตรงกับความต้องการในการปฏิบัติงานและการใช้งานของผู้ใช้
4. กระบวนการ BAI05 *บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล (Manage organisational change enablement)* และ BAI 08 *บริหารจัดการความรู้ (Manage knowledge)* ใน COBIT 5 ช่วยให้มั่นใจว่า ผู้ใช้งานสามารถใช้ระบบได้อย่างมีประสิทธิผล

นอกจากนี้ ISACA ยังให้วุฒิบัตร 4 แบบสำหรับผู้ประกอบวิชาชีพที่มีบทบาทหน้าที่หลักเกี่ยวข้องกับการกำกับดูแลด้านไอทีและมีองค์ความรู้ที่เนื้อหาใน COBIT 5 ได้ครอบคลุมถึงอย่างเป็นนัยสำคัญ ได้แก่

- 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™)

ผู้ถือวุฒิบัตรเหล่านี้แสดงถึงความสามารถและประสบการณ์ในการทำงานตามบทบาทหน้าที่นั้น

ISO/IEC 38500 ประเมิน สั่งการ และเฝ้าติดตาม

แนวทางของ ISACA เอื้อต่อแนวปฏิบัติที่ดีได้อย่างไร

โดเมนด้านการกำกับดูแลในกระบวนการต้นแบบของ COBIT 5 มี 5 กระบวนการ โดยแต่ละกระบวนการได้ระบุถึงแนวปฏิบัติสำหรับการประเมิน สั่งการ และเฝ้าติดตาม (EDM) ไว้ ซึ่งเป็นส่วนที่ COBIT 5 ได้ระบุถึงกิจกรรมที่เกี่ยวข้องกับการกำกับดูแล

การเปรียบเทียบกับมาตรฐานอื่นๆ

COBIT 5 พัฒนาขึ้นโดยคำนึงถึงมาตรฐานและกรอบการดำเนินงานอื่นๆ จำนวนหนึ่ง ซึ่งมาตรฐานเหล่านี้ได้แสดงไว้ในภาคผนวก A

หนังสือ *COBIT 5:การสัมฤทธิ์ผลของกระบวนการ (COBIT 5: Enabling Processes)* กล่าวถึงการเปรียบเทียบในภาพรวมระหว่าง กระบวนการใน COBIT 5 แต่ละกระบวนการกับส่วนที่ใกล้เคียงกันในมาตรฐาน/กรอบการดำเนินงานที่เกี่ยวข้อง ซึ่งให้เป็นแนวทางเพิ่มเติม

ในส่วนนี้จะกล่าวโดยสรุปถึงกรอบการดำเนินงานและมาตรฐานแต่ละอย่าง โดยระบุว่าเกี่ยวข้องกับจุดหรือโดเมนใดใน COBIT 5

ITIL® V3 2011 และ ISO/IEC 20000

ITIL V3 2011 and ISO/IEC 20000 ครอบคลุมถึงจุดและโดเมนใน COBIT 5 ต่อไปนี้
- ส่วนหนึ่งของกระบวนการต่างๆ ในโดเมน DSS
- ส่วนหนึ่งของกระบวนการต่างๆ ในโดเมน BAI
- บางกระบวนการในโดเมน APO

ชุดของ ISO/IEC 27000

ISO/IEC 27000 ครอบคลุมถึงจุดและโดเมนใน COBIT 5 ต่อไปนี้
- กระบวนการที่เกี่ยวข้องกับความมั่นคงปลอดภัยและความเสี่ยงในโดเมน EDM APO และ DSS
- กิจกรรมต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยภายใต้กระบวนการในโดเมนอื่นๆ
- กิจกรรมต่างๆ ในการเฝ้าติดตามและการประเมินจากโดเมน MEA

ชุด ISO/IEC 31000

ISO/IEC 31000 ครอบคลุมถึงจุดและโดเมนใน COBIT 5 ต่อไปนี้
- กระบวนการที่เกี่ยวข้องกับการบริหารความเสี่ยงในโดเมน EDM และ APO

TOGAF®

TOGAF ครอบคลุมถึงจุดและโดเมนใน COBIT 5 ต่อไปนี้
- กระบวนการที่เกี่ยวข้องกับทรัพยากรในโดเมน EDM (การกำกับดูแล) – ส่วนประกอบของ TOGAF ซึ่งได้แก่ Architecture Board, Architecture Governance และ Architecture Maturity Model เทียบได้กับการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด
- กระบวนการในการสร้างสถาปัตยกรรมองค์กรในโดเมน APO โดยแก่นของ TOGAF คือ Architecture development method (ADM) cycle ซึ่งเทียบได้กับแนวปฏิบัติของ COBIT 5 เรื่องการพัฒนาวิสัยทัศน์ด้านสถาปัตยกรรม (ADM Phase A) การระบุถึงสถาปัตยกรรมอ้างอิง (ADM Phase B,C,D) การเลือกโอกาสและแนวทางการแก้ไขปัญหาแบบเบ็ดเสร็จ (ADM Phase E) และการกำหนดการนำสถาปัตยกรรมไปใช้งาน (ADM Phase F, G) องค์ประกอบของ TOGAF จำนวนหนึ่งสามารถเทียบได้กับแนวปฏิบัติของ COBIT 5 เรื่องการให้บริการด้านสถาปัตยกรรมองค์กร ซึ่งรวมถึง
  – การบริหารจัดการความต้องการของ ADM
  – หลักการของสถาปัตยกรรม
  – การบริหารจัดการผู้มีส่วนได้เสีย
  – การประเมินความพร้อมในการปรับเปลี่ยนธุรกิจ
  – การบริหารความเสี่ยง
  – การวางแผนบนพื้นฐานของความสามารถ
  – การปฏิบัติตามข้อกำหนดของสถาปัตยกรรม
  – สัญญาด้านสถาปัตยกรรม

Capability Maturity Model Integration (CMMI) (development)

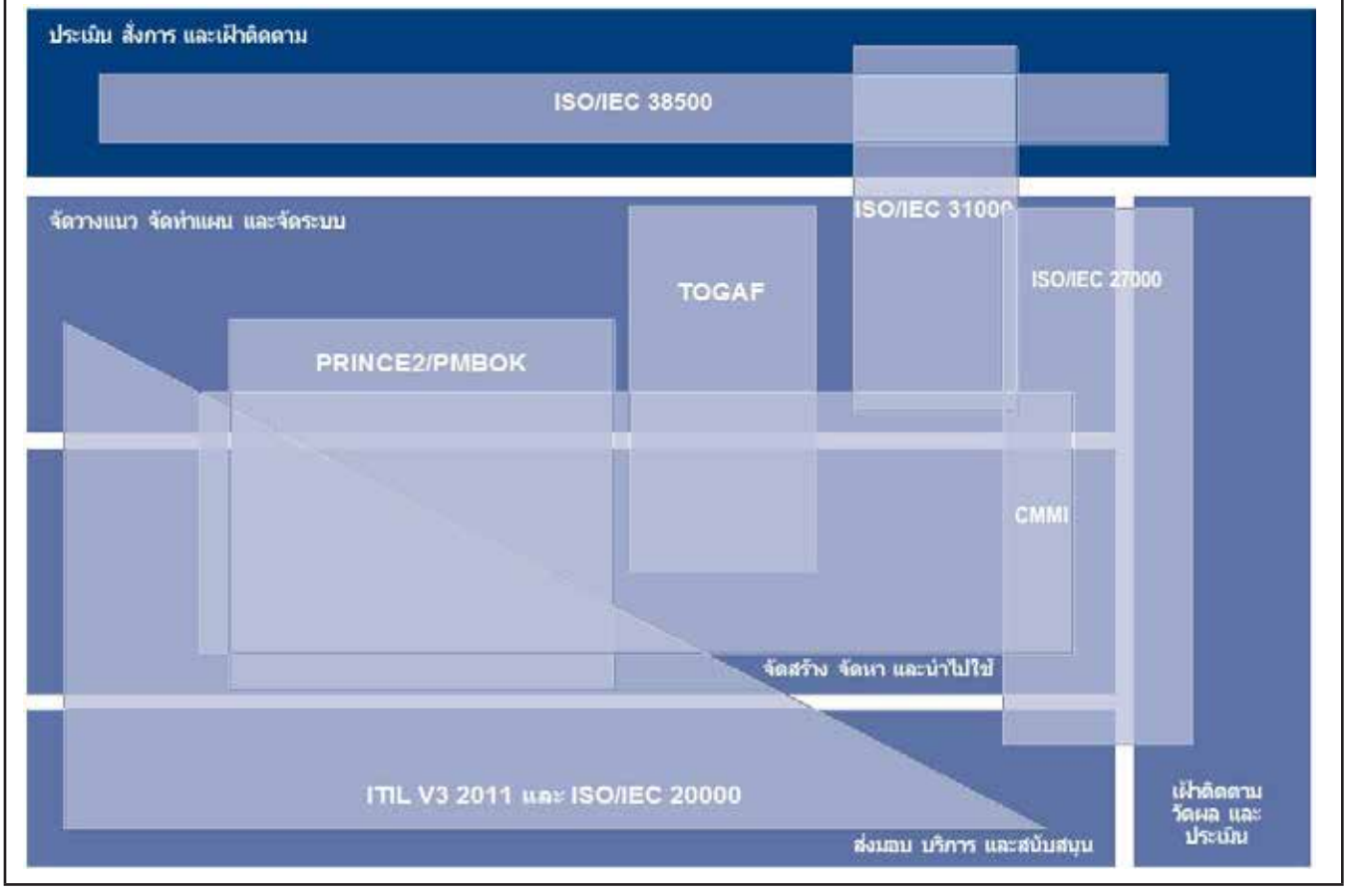
CMMI ครอบคลุมถึงจุดและโดเมนใน COBIT 5 ต่อไปนี้
- กระบวนการที่เกี่ยวข้องกับการจัดสร้างและจัดซื้อจัดหาระบบงานในโดเมน BAI
- กระบวนการที่เกี่ยวข้องกับการจัดองค์กรและจัดการคุณภาพในโดเมน APO

PRINCE2®

PRINCE2 ครอบคลุมถึงจุดและโดเมนใน COBIT 5 ต่อไปนี้
- กระบวนการที่เกี่ยวข้องกับการบริหารจัดการกลุ่มของชุดโครงการในโดเมน APO
- กระบวนการที่เกี่ยวข้องการบริหารจัดการชุดโครงการและโครงการในโดเมน BAI

รูปภาพที่ 25 แสดงถึงความสัมพันธ์ระหว่าง COBIT 5 กับมาตรฐานและกรอบการดำเนินงานอื่นๆ

รูปภาพที่ 25—ความสัมพันธ์ระหว่าง COBIT 5 กับมาตรฐานและกรอบการดำเนินงานอื่นๆ



ภาคผนวก F
การเปรียบเทียบระหว่างต้นแบบสารสนเทศใน COBIT 5 กับเกณฑ์คุณสมบัติของสารสนเทศใน COBIT 4.1

เกณฑ์คุณสมบัติของสารสนเทศ (Information Criteria) 7 ข้อใน COBIT 4.1 — ความมีประสิทธิผล ความมีประสิทธิภาพ ความถูกต้องสมบูรณ์ ความเชื่อถือได้ ความพร้อมใช้ การรักษาความลับ การปฏิบัติตาม (กฎหมายหรือกฎระเบียบข้อบังคับ) — เกี่ยวข้องกับประเภทของคุณภาพสำหรับสารสนเทศและมิติต่างๆ ของปัจจัยเอื้อด้านสารสนเทศ (information enabler) ของ COBIT 5 ดังที่ได้แสดงไว้ในภาคผนวก G **รูปภาพที่ 32**

ตารางข้างล่างนี้ประกอบด้วย 2 คอลัมน์ คือ
- คอลัมน์แรกแสดงรายการเกณฑ์คุณสมบัติของสารสนเทศทั้ง 7 ข้อใน COBIT 4.1
- คอลัมน์ที่สองแสดงรายการทางเลือกใน COBIT 5 ได้แก่ เป้าหมายของปัจจัยเอื้อด้านสารสนเทศที่สัมพันธ์กับเกณฑ์คุณสมบัติของสารสนเทศในแต่ละข้อ

รูปภาพที่ 26—COBIT 5 ที่เทียบได้กับเกณฑ์คุณสมบัติของสารสนเทศใน COBIT 4.1

เกณฑ์คุณสมบัติของสารสนเทศใน COBIT 4.1	COBIT 5 ที่เทียบเท่า
ความมีประสิทธิผล	สารสนเทศจะมีประสิทธิผลถ้าสามารถบรรลุความต้องการของผู้ใช้สารสนเทศซึ่งใช้สารสนเทศสำหรับภารกิจเฉพาะหนึ่งๆ ถ้าผู้ใช้สารสนเทศสามารถปฏิบัติภารกิจด้วยการใช้สารสนเทศนั้นก็แสดงว่าสารสนเทศนั้นมีประสิทธิผล ซึ่งสัมพันธ์กับเป้าหมายด้านคุณภาพของสารสนเทศในเรื่องจำนวนที่เหมาะสมของความเกี่ยวเนื่อง เข้าใจได้ง่าย สามารถแปลความหมายได้ และเที่ยงตรง.
ความมีประสิทธิภาพ	ในขณะที่ความมีประสิทธิผลจะมองสารสนเทศเป็นผลลัพธ์ ประสิทธิภาพจะเกี่ยวข้องกับกระบวนการในการได้มาและการใช้สารสนเทศ ดังนั้น จึงสอดคล้องกับมุมมองที่ว่า 'สารสนเทศเป็นการให้บริการ' ('information as service') ถ้าสารสนเทศตรงกับความต้องการของผู้ใช้สารสนเทศและใช้ได้อย่างสะดวกสบาย (เช่น ใช้ทรัพยากรน้อย ไม่ว่าจะเป็นการลงแรง การใช้ความคิด เวลา และเงิน) ก็เรียกได้ว่าการใช้งานสารสนเทศนั้นมีประสิทธิภาพ ซึ่งสัมพันธ์กับเป้าหมายด้านคุณภาพของสารสนเทศในเรื่องความน่าเชื่อถือ การเข้าถึงได้ ความง่ายในการใช้งาน และชื่อเสียง
ความถูกต้องสมบูรณ์	ถ้าสารสนเทศมีความถูกต้องสมบูรณ์ ก็หมายถึงสารสนเทศนั้นครบถ้วนและไม่มีความผิดพลาด ซึ่งสัมพันธ์กับเป้าหมายด้านคุณภาพของสารสนเทศในเรื่องความครบถ้วนและถูกต้อง
ความเชื่อถือได้	ความเชื่อถือได้มักจะถูกมองว่ามีความหมายเช่นเดียวกับคำว่า ความถูกต้อง อย่างไรก็ตาม เราอาจกล่าวได้ว่า สารสนเทศมีความเชื่อถือได้หากเป็นเรื่องจริงและได้อย่างถูกต้องและวางใจได้ หากเปรียบกับความถูกต้องสมบูรณ์ ความเชื่อถือได้เป็นเรื่องของดุลพินิจซึ่งขึ้นกับมุมมองของแต่ละบุคคล ไม่ได้มองเพียงข้อเท็จจริงอย่างเดียว ซึ่งสัมพันธ์กับเป้าหมายด้านคุณภาพของสารสนเทศในเรื่อง ความน่าเชื่อถือ ชื่อเสียง ความเที่ยงตรง
ความพร้อมใช้	ความพร้อมใช้ เป็นหนึ่งในเป้าหมายด้านคุณภาพของสารสนเทศภายใต้หัวข้อการเข้าถึงได้และความมั่นคงความปลอดภัย
การรักษาความลับ	การรักษาความลับ สัมพันธ์กับเป้าหมายด้านคุณภาพของสารสนเทศในเรื่องของการจำกัดการเข้าถึง
การปฏิบัติตาม	การปฏิบัติตาม ใช้ในความหมายที่สารสนเทศต้องสอดคล้องกับข้อกำหนดต่างๆ ซึ่งเป็นส่วนหนึ่งของเป้าหมายด้านคุณภาพของสารสนเทศที่ขึ้นอยู่กับข้อกำหนดที่มีการปฏิบัติตามกฎระเบียบข้อบังคับมักจะเป็นเป้าหมายหรือข้อกำหนดในการใช้สารสนเทศ ซึ่งไม่ค่อยเกี่ยวเนื่องกับคุณภาพของสารสนเทศ

ตารางข้างต้น แสดงถึงเกณฑ์คุณสมบัติของสารสนเทศทั้งหมดจาก COBIT 4.1 ที่ COBIT 5 ได้ครอบคลุมถึง อย่างไรก็ตาม ต้นแบบสารสนเทศ (information model) ของ COBIT 5 สามารถกำหนดชุดของเกณฑ์เพิ่มเติมได้ จึงเพิ่มคุณค่าให้กับเกณฑ์ของ COBIT 4.1

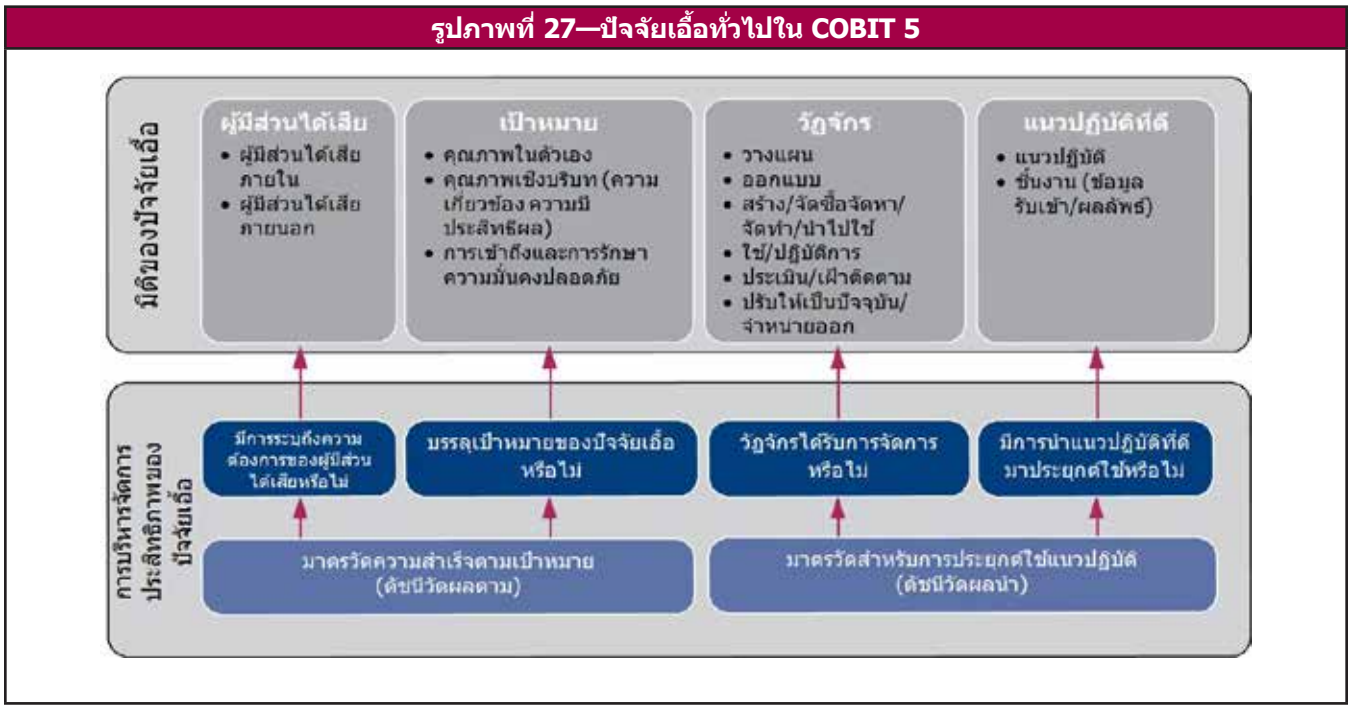
หน้านี้เป็นหน้าว่าง

ภาคผนวก G
คำอธิบายอย่างละเอียดของปัจจัยเอื้อใน COBIT 5

บทนำ

ในส่วนนี้จะประกอบด้วย คำอธิบายประเภทของปัจจัยเอื้อทั้ง 7 ประเภทในรายละเอียด ซึ่งเป็นส่วนหนึ่งของกรอบการดำเนินงาน COBIT 5 ซึ่งได้อธิบายในเบื้องต้นไว้ในบทที่ 5 และจะนำมากล่าวซ้ำอีกใน**รูปภาพที่ 27**

รูปภาพที่ 27—ปัจจัยเอื้อทั่วไปใน COBIT 5



มิติต่างๆ ของปัจจัยเอื้อ

มิติที่ทุกปัจจัยเอื้อมีร่วมกันทั้ง 4 มิติได้แก่

- **ผู้มีส่วนได้เสีย**—แต่ละปัจจัยเอื้อมีผู้มีส่วนได้เสีย ได้แก่ผู้ที่มีบทบาทสำคัญหรือมีผลประโยชน์ในปัจจัยเอื้อนั้น ยกตัวอย่างเช่น กระบวนการมีหน่วยงานต่างๆ ที่ดำเนินกิจกรรมของกระบวนการ และ/หรือที่ได้รับประโยชน์จากผลลัพธ์ของกระบวนการนั้นๆ โครงสร้างองค์กรมีผู้ที่มีส่วนได้เสียซึ่งแต่ละคนก็มีบทบาทหน้าที่และผลประโยชน์อันเป็นส่วนหนึ่งของโครงสร้าง ผู้มีส่วนได้เสียอาจจะอยู่ภายในหรืออยู่ภายนอกองค์กรก็ได้ ผู้มีส่วนได้เสียต่างก็มีผลประโยชน์และความต้องการของตนซึ่งในบางครั้งอาจจะขัดแย้งกันเอง ความต้องการของผู้มีส่วนได้เสียแปลงมาเป็นเป้าหมายขององค์กร ซึ่งเป้าหมายนี้ก็จะถูกแปลงมาเป็นเป้าหมายที่เกี่ยวข้องกับไอทีสำหรับองค์กร รายละเอียดของผู้มีส่วนได้เสียแสดงอยู่ใน**รูปภาพที่ 7**
- **เป้าหมาย**—แต่ละปัจจัยเอื้อมีเป้าหมายจำนวนหนึ่งและปัจจัยเอื้อให้คุณค่าโดยการบรรลุเป้าหมายเหล่านั้นเป้าหมายเหล่านี้อาจระบุเป็นลักษณะของ
  – ผลลัพธ์ที่คาดหวังจากปัจจัยเอื้อ
  – ระบบงานหรือปฏิบัติการของปัจจัยเอื้อเอง

เป้าหมายของปัจจัยเอื้อเป็นขั้นตอนสุดท้ายของการส่งทอดเป้าหมายใน COBIT 5 เป้าหมายสามารถแยกออกเป็นกลุ่มต่างๆ ได้ดังนี้

– **คุณภาพในตัวเอง** (intrinsic quality) ครอบคลุมถึงการที่ปัจจัยเอื้อทำงานอย่างถูกต้อง เที่ยงตรง และให้ผลลัพธ์ที่แม่นยำเที่ยงตรง และเชื่อถือได้
– **คุณภาพเชิงบริบท** (contextual quality) ครอบคลุมถึงการที่ปัจจัยเอื้อและผลลัพธ์เป็นไปตามจุดประสงค์ในบริบทที่ปัจจัยเอื้อนั้นดำเนินงานอยู่ ได้แก่ ผลลัพธ์ควรจะเกี่ยวเนื่อง สมบูรณ์ เป็นปัจจุบัน เหมาะสม สม่ำเสมอ เข้าใจได้ง่าย และใช้งานง่าย.
– **การเข้าถึงและการรักษาความมั่นคงปลอดภัย** ครอบคลุมถึงการที่ปัจจัยเอื้อและผลลัพธ์สามารถเข้าถึงได้และมีความปลอดภัย
  • ปัจจัยเอื้อมีความพร้อมใช้เมื่อต้องการ
  • มีการรักษาความปลอดภัยให้กับผลลัพธ์ ยกตัวอย่างเช่น การเข้าถึงผลลัพธ์จำกัดให้เฉพาะผู้ที่ได้รับอนุมัติและจำเป็นต้องใช้เท่านั้น

- **วัฏจักร**—แต่ละปัจจัยเอื้อมีวัฏจักรจากจุดเริ่มต้นผ่านช่วงเวลาของการดำเนินงาน/การใช้ประโยชน์จนถึงการจำหน่ายออก วัฏจักรนี้ประยุกต์ใช้กับสารสนเทศ โครงสร้าง กระบวนการ นโยบาย และอื่นๆ วัฏจักรประกอบด้วยการดำเนินงานในระยะต่างๆ ดังนี้
  –การวางแผน (รวมถึง การพัฒนาและการคัดเลือกแนวคิด)
  –การออแบบ
  –การสร้าง/การจัดซื้อจัดหา/การจัดทำ/การนำไปใช้
  –ใช้/ดำเนินการ
  –ประเมิน/เฝ้าติดตาม
  –ปรับให้เป็นปัจจุบัน/จำหน่ายออก
- **แนวปฏิบัติที่ดี** —เราสามารถกำหนดแนวปฏิบัติที่ดีสำหรับปัจจัยเอื้อแต่ละรายการได้ แนวปฏิบัติที่ดีสนับสนุนปัจจัยเอื้อให้บรรลุถึงเป้าหมาย แนวปฏิบัติที่ดีให้ตัวอย่างหรือข้อแนะนำว่าจะนำปัจจัยเอื้อไปใช้งานอย่างไรให้ได้ดีที่สุด และชิ้นงานหรือข้อมูลรับเข้าและผลลัพธ์อะไรบ้างที่ต้องการ COBIT 5 ได้ให้ตัวอย่างของแนวปฏิบัติที่ดีสำหรับปัจจัยเอื้อใน COBIT 5 เฉพาะบางรายการ (เช่น กระบวนการ) ส่วนปัจจัยเอื้ออื่นๆ ที่เหลือสามารถใช้แนวทางจากมาตรฐานและกรอบการดำเนินงานอื่นๆ ได้

การบริหารจัดการประสิทธิภาพของปัจจัยเอื้อ
องค์กรคาดหวังที่จะได้ผลลัพธ์ในด้านดีจากระบบงานและการใช้ปัจจัยเอื้อต่างๆ ในการบริหารจัดการประสิทธิภาพของปัจจัยเอื้อจะต้องเฝ้าติดตามคำถามเหล่านี้และหาคำตอบจากมาตรวัดอย่างสม่ำเสมอ
- มีการระบุความต้องการของผู้มีส่วนได้เสียหรือไม่
- บรรลุเป้าหมายของปัจจัยเอื้อหรือไม่
- วัฏจักรของปัจจัยเอื้อได้รับการจัดการหรือไม่
- มีการประยุกต์ใช้แนวปฏิบัติที่ดีหรือไม่

คำถามสองข้อแรกเป็นคำถามเกี่ยวกับผลที่เกิดขึ้นจริงจากปัจจัยเอื้อ มาตรวัดที่ใช้วัดว่าได้บรรลุถึงเป้าหมายเพียงใดนั้น เรียกว่า 'ดัชนีตาม' (lag indicators)

คำถามสองข้อหลังเป็นคำถามเกี่ยวกับการทำงานจริงของปัจจัยเอื้อ และมาตรวัดที่ใช้จะเรียกว่า 'ดัชนีชี้นำ' (lead indicators) สำหรับแต่ละปัจจัยเอื้อยังมีส่วนที่แยกออกมา ซึ่งมีรูปคล้ายกับรูปภาพที่ 27 แต่ได้รวมถึงส่วนประกอบจำนวนหนึ่งสำหรับปัจจัยเอื้อนั้นๆ โดยได้แสดงเป็นตัวอักษรเข้มสีแดง

ขั้นต่อไป เป็นการอธิบายในรายละเอียดสำหรับแต่ละองค์ประกอบทั้ง 4 โดยอธิบายองค์ประกอบที่สำคัญและความสัมพันธ์กับปัจจัยเอื้ออื่นๆ

ตัวอย่างจำนวนหนึ่งได้ถูกรวมไว้พร้อมกับภาพที่แสดงให้เห็นถึงความหมายและการใช้งานของปัจจัยเอื้อต่างๆ

จุดประสงค์ในส่วนนี้คือ การให้ความเข้าใจเพิ่มเติมในกรอบการดำเนินงาน COBIT 5 และแนวคิดของปัจจัยเอื้อสามารถนำไปประยุกต์ใช้เพื่อให้การกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรได้รับการนำไปใช้และปรับปรุงให้ดีขึ้นได้อย่างไร

ปัจจัยเอื้อใน COBIT 5: หลักการ นโยบาย และกรอบการดำเนินงาน

หลักการและนโยบายเป็นกลไกในการสื่อสารที่จัดทำขึ้นเพื่อถ่ายทอดทิศทางและคำสั่งจากผู้บริหารและหน่วยงานกำกับดูแล รายละเอียดเฉพาะของปัจจัยเอื้อสำหรับหลักการ นโยบาย และกรอบการดำเนินงานเปรียบเทียบกับคำอธิบายของปัจจัยเอื้อทั่วไป (generic enabler) ได้แสดงไว้ใน**รูปภาพที่ 28**

ต้นแบบของหลักการ นโยบาย และกรอบการดำเนินงาน แสดงถึง
- **ผู้มีส่วนได้เสีย**—ผู้มีส่วนได้เสียสำหรับหลักการและนโยบายอาจอยู่ภายในหรือภายนอกองค์กรก็ได้ โดยรวมถึงคณะกรรมการบริหารและผู้บริหารระดับสูง เจ้าหน้าที่ด้านการปฏิบัติตาม(กฎระเบียบข้อบังคับ) ผู้จัดการความเสี่ยง ผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอก ผู้ให้บริการ ลูกค้าและหน่วยงานกำกับดูแล ส่วนได้เสียมี 2 ด้าน: ผู้มีส่วนได้เสียบางคนที่เป็นผู้กำหนดนโยบาย และที่เหลือเป็นผู้ที่ต้องปฏิบัติตนให้สอดคล้องและเป็นตามนโยบาย
- **เป้าหมายและมาตรวัด**—หลักการ นโยบายและกรอบการดำเนินงานเป็นเครื่องมือในการสื่อสารถึงกฎขององค์กรที่กำหนดขึ้นโดยคณะกรรมการบริหารและผู้บริหารระดับสูง เพื่อสนับสนุนวัตถุประสงค์ด้านการกำกับดูแลและคุณค่าขององค์กร หลักการจำเป็นต้อง
  – จำกัดจำนวน
  – ใช้ภาษาที่ง่าย แสดงออกให้ชัดเจนมากที่สุดถึงแก่นของคุณค่าองค์กร

นโยบายให้แนวทางที่ละเอียดมากขึ้น ว่าจะนำหลักการไปปฏิบัติได้อย่างไรและมีอิทธิพลต่อการตัดสินใจว่าสอดคล้องกับหลักการอย่างไร นโยบายที่ดีต้อง
– มีประสิทธิผล—บรรลุตามจุดประสงค์ที่ตั้งไว้
– มีประสิทธิภาพ—ช่วยให้มั่นใจว่าได้นำหลักการไปใช้อย่างมีประสิทธิภาพ
– ไม่ก้าวก่ายหรือเป็นที่รบกวน (Non-intrusive) —แสดงถึงความสมเหตุผลแก่ผู้ที่ปฏิบัติตาม นั่นคือ ไม่ทำให้เกิดการต่อต้านที่ไม่จำเป็น

การเข้าถึงนโยบาย—มีกลไกที่ช่วยให้ผู้มีส่วนได้เสียทั้งหมดสามารถเข้าถึงนโยบายได้โดยง่ายหรือไม่ หรืออีกนัยหนึ่ง ผู้มีส่วนได้เสียทราบหรือไม่ว่าจะหาอ่านนโยบายได้จากที่ใด

รูปภาพที่ 28—ปัจจัยเอื้อใน COBIT 5: หลักการ นโยบาย และกรอบการดำเนินงาน

กรอบการดำเนินงานด้านการกำกับดูแลและการบริหารจัดการ ควรให้โครงสร้าง แนวปฏิบัติ เครื่องมือ และอื่นๆ แก่ผู้บริหาร ที่ช่วยให้เกิดการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่เหมาะสม กรอบดำเนินงานควร
– กว้างและครอบคลุมถึงทุกจุดที่จำเป็น
– เปิดรับและยืดหยุ่น สามารถปรับให้สอดคล้องเข้ากับสถานการณ์เฉพาะขององค์กร
– เป็นปัจจุบัน กล่าวคือ สะท้อนถึงทิศทางในปัจจุบันขององค์กรและเป้าหมายการกำกับดูแลในปัจจุบัน
– พร้อมใช้งานและผู้มีส่วนได้เสียทั้งหมดสามารถเข้าถึงได้

- **วัฏจักร** - นโยบายมีวัฏจักรที่จะต้องสนับสนุนการบรรลุถึงเป้าหมายที่กำหนดไว้ กรอบการดำเนินงานสิ่งสำคัญที่ให้โครงสร้างที่ช่วยจะกำหนดแนวทางที่สอดคล้องกัน ยกตัวอย่างเช่น กรอบการดำเนินงานด้านนโยบายให้โครงสร้างที่เอื้อให้มีการกำหนดและรักษาชุดของนโยบายที่สอดคล้องกัน และยังให้จุดนำทางแบบง่ายๆ ภายในและระหว่างนโยบายแต่ละข้อ

องค์กรอาจมีข้อกำหนดที่ใช้บังคับควบคุมในระดับที่แตกต่างกันไปเพื่อการควบคุมภายในและกรอบการดำเนินงานด้านนโยบายที่เข้มแข็ง ขึ้นอยู่กับสภาพแวดล้อมภายนอกที่องค์กรดำเนินงานอยู่ จุดสำคัญที่ควรนำมาพิจารณาเกี่ยวกับกรอบการดำเนินงานและนโยบายคือ ความเป็นปัจจุบันของนโยบาย—ว่านโยบายได้รับการสอบทานและปรับให้เป็นปัจจุบันเมื่อใด มีกลไกที่แข็งแกร่งที่จะทำให้มั่นใจได้ว่า บุคคลได้รับรู้ถึงการปรับให้เป็นปัจจุบันนี้หรือไม่ นโยบายที่ปรับให้เป็นปัจจุบันใหม่นี้สามารถเข้าถึงได้ง่ายหรือไม่(กรุณาดูประเด็นก่อนหน้านี้) และสารสนเทศที่เลิกใช้แล้วได้รับการจัดเก็บไว้ต่างหาก (archived) หรือทำลายอย่างเหมาะสมหรือไม่

- **แนวปฏิบัติที่ดี:**
  - แนวปฏิบัติที่ดีจำเป็นต้องมีนโยบายที่เป็นส่วนหนึ่งของกรอบดำเนินงานด้านการกำกับดูแลและการบริหารจัดการ ซึ่งให้โครงสร้าง (เชิงลำดับชั้น) ที่ทำให้นโยบายทั้งหมดสอดคล้องและสามารถเชื่อมโยงกับหลักการที่เป็นพื้นฐานได้อย่างชัดเจน
  - ในการเป็นส่วนหนึ่งของกรอบการดำเนินงานด้านนโยบาย หัวข้อดังต่อไปนี้จะต้องมีคำอธิบาย
    - ขอบเขต และความสมเหตุสมผล
    - ผลที่ตามมาจากการที่ไม่ปฏิบัติตามนโยบาย
    - วิธีการรับมือกับข้อยกเว้น
    - วิธีตรวจสอบและวัดผลการปฏิบัติตามนโยบาย
  - กรอบการดำเนินงานด้านการกำกับดูแลและการบริหารจัดการที่ได้รับการยอมรับกันโดยทั่วไปนั้น ให้แนวทางที่เป็นประโยชน์ในการระบุถึงข้อความที่ควรจะรวมอยู่ในนโยบาย
  - นโยบายควรจะสอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ นโยบายเป็นองค์ประกอบสำคัญของระบบควบคุมภายในขององค์กรซึ่งมีจุดประสงค์เพื่อบริหารจัดการและควบคุมความเสี่ยง ส่วนหนึ่งในกิจกรรมด้านการกำกับดูแลความเสี่ยงรวมถึงการกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ และระดับความเสี่ยงที่ยอมรับได้นี้ควรสะท้อนให้เห็นอยู่ในนโยบายด้วย องค์กรที่หลีกเลี่ยงการรับความเสี่ยง (risk averse enterprise) ย่อมมีนโยบายที่เข้มงวดกว่าองค์กรที่พร้อมจะยอมรับความเสี่ยง (risk-aggressive enterprise)
  - นโยบายจำเป็นต้องได้รับการประเมินความสมเหตุสมผลใหม่ (revalidated) และ/หรือปรับให้เป็นปัจจุบันตามช่วงเวลาที่สม่ำเสมอ
- **ความสัมพันธ์กับปัจจัยเอื้ออื่นๆ** —ความเชื่อมโยงกับปัจจัยเอื้ออื่นๆ รวมถึง:
  - หลักการ นโยบาย และกรอบการดำเนินงานควรจะสะท้อนถึงคุณค่าของวัฒนธรรมและจริยธรรมขององค์กร และควรส่งเสริมให้เกิดพฤติกรรมที่ต้องการ ดังนั้น จึงมีความเชื่อมโยงที่แน่นแฟ้นกับปัจจัยเอื้อด้านวัฒนธรรม จริยธรรม และพฤติกรรม
  - แนวปฏิบัติและกิจกรรมของกระบวนการ เป็นพาหนะที่สำคัญในการปฏิบัติตามนโยบาย
  - โครงสร้างองค์กรสามารถกำหนดนโยบายและนำไปใช้งานงานภายใต้ขอบเขตของการควบคุม(span of control) และในทางกลับกันกิจกรรมต่างๆ ก็จะถูกกำหนดขึ้นโดยนโยบายเช่นกัน
  - นโยบายก็เป็นสารสนเทศ ดังนั้น แนวปฏิบัติที่ดีทั้งหมดที่ประยุกต์ใช้กับสารสนเทศก็สามารถประยุกต์ใช้กับนโยบายเช่นกัน

ตัวอย่างที่ 9—สื่อสังคม

องค์กรกำลังพิจารณาว่าจะจัดการกับสื่อสังคม (social media) ที่ใช้กันอย่างแพร่หลายและแรงกดดันจากพนักงานที่ต้องการเข้าถึงเพื่อใช้งานได้อย่างไร จนถึงปัจจุบัน องค์กรยังคงใช้ความระมัดระวังหรือจำกัดการให้สิทธิในการเข้าถึงบริการนี้ ด้วยเหตุผลหลักคือการรักษาความมั่นคงปลอดภัย

มีแรงกดดันจากด้านต่างๆ ให้พิจารณาเปลี่ยนจุดยืนขององค์กรเกี่ยวกับสื่อสังคมนี้ พนักงานต้องการให้สามารถเข้าถึงสื่อสังคมได้เช่นเดียวกับที่พวกเขาทำที่บ้าน และองค์กรก็ต้องการใช้สื่อสังคมเพื่อประโยชน์ด้านการตลาดและเพื่อจุดประสงค์ในการสร้างความตระหนักในหมู่สาธารณะชน

ได้มีการตัดสินใจที่จะกำหนดนโยบายในการใช้สื่อสังคมบนเครือข่ายและระบบขององค์กร ซึ่งรวมถึงเครื่องคอมพิวเตอร์พกพาที่องค์กรให้กับพนักงานขององค์กรใช้ นโยบายที่กำหนดใหม่นี้สอดคล้องกับกรอบการดำเนินงานด้านนโยบายที่มีอยู่ภายใต้หัวข้อ 'นโยบายการใช้งานที่ยอมรับได้' (acceptable use policy) ซึ่งผ่อนปรนมากกว่านโยบายเดิม ดังนั้น จึงได้มีการพัฒนาการสื่อสารเพื่อที่อธิบายถึงเหตุผลของนโยบายใหม่ ในขณะเดียวกันก็มีผลกระทบกับปัจจัยเอื้อบางรายการ เช่น

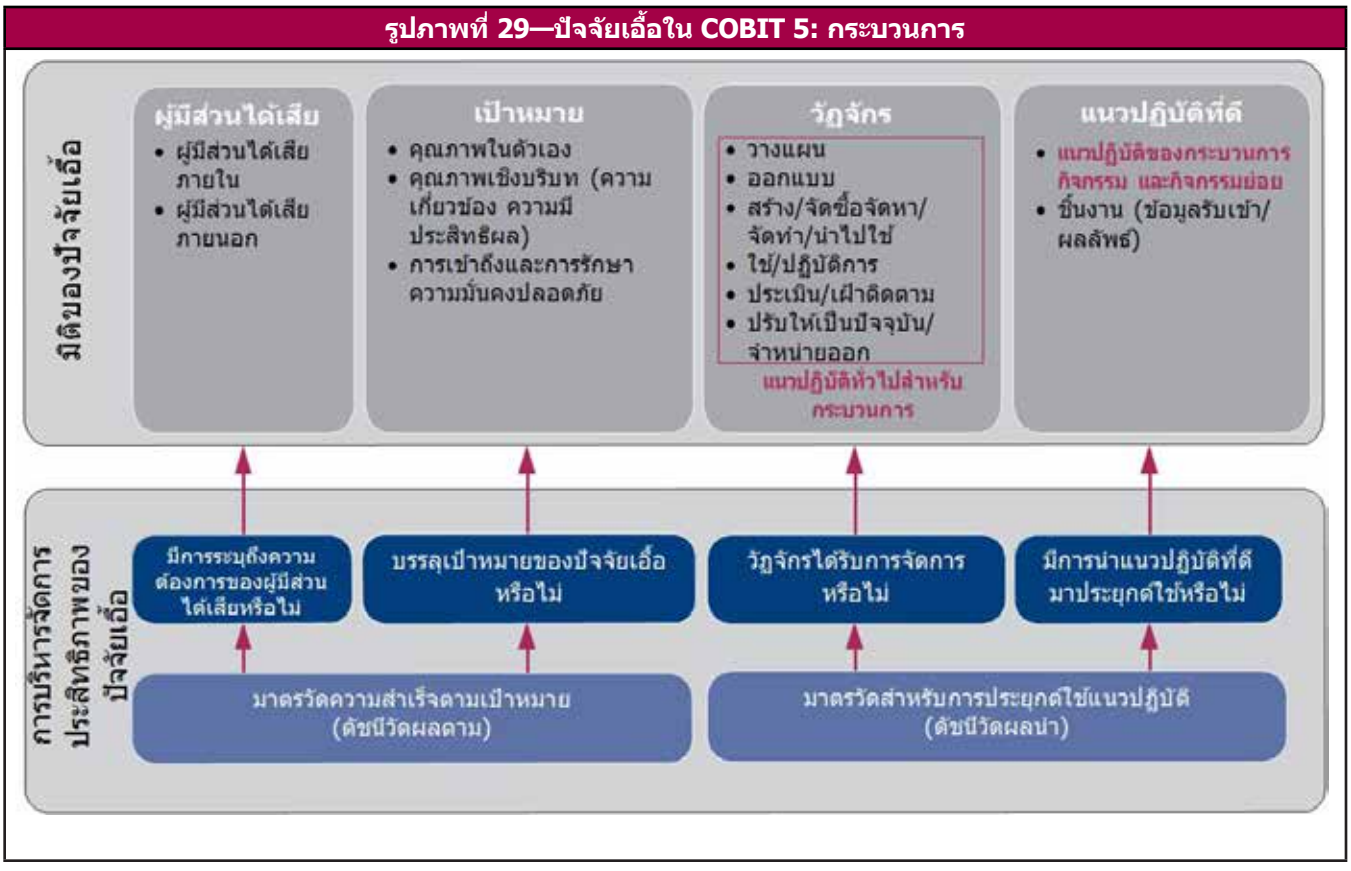
- พนักงานจำเป็นต้องเรียนรู้ว่าจะจัดการกับสื่อใหม่นี้อย่างไรเพื่อจะหลีกเลี่ยงสถานการณ์ที่จะก่อให้เกิดความเสื่อมเสียแก่องค์กร พวกเขาจำเป็นต้องเรียนรู้ถึงพฤติกรรมที่เหมาะสมให้สอดคล้องกับทิศทางใหม่ที่องค์กรกำลังจะไปและพัฒนาทักษะที่เหมาะสม
- กระบวนการจำนวนหนึ่งที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยจำเป็นต้องเปลี่ยนไป เมื่อเปิดให้เข้าถึงสื่อสังคมเหล่านี้ก็จะต้องมีการเปลี่ยนแปลงการกำหนดค่าการทำงานและค่าตัวแปรต่างๆ ด้านการรักษาความมั่นคงปลอดภัย และอาจต้องกำหนดมาตรการทดแทนบางประการขึ้นมาใช้

หมายเหตุ: COBIT 5 เป็นตัวอย่างของกรอบการดำเนินงานดังที่อธิบายไว้ในปัจจัยเอื้อนี้

ปัจจัยเอื้อใน COBIT 5: กระบวนการ

รายละเอียดเฉพาะของปัจจัยเอื้อด้านกระบวนการ (Process enabler) เปรียบเทียบกับปัจจัยเอื้อทั่วไป (generic enabler) ได้แสดงไว้ใน**รูปภาพที่ 29**

รูปภาพที่ 29—ปัจจัยเอื้อใน COBIT 5: กระบวนการ



กระบวนการ หมายถึง **'กลุ่มของแนวปฏิบัติที่ได้รับอิทธิพลจากนโยบายและขั้นตอนการปฏิบัติงานขององค์กร ที่รับข้อมูลจากแหล่งต่างๆ (รวมถึงกระบวนการอื่นๆ) จัดดำเนินการข้อมูลที่รับเข้ามา และจัดทำผลลัพธ์ (ยกตัวอย่างเช่น ผลิตภัณฑ์ บริการ)'**

ต้นแบบของกระบวนการ (Process model) แสดงถึง

- **ผู้มีส่วนได้เสีย**— กระบวนการมีผู้มีส่วนได้เสียทั้งภายในและภายนอกและต่างมีบทบาทหน้าที่ของตน ผู้มีส่วนได้เสีย และระดับหน้าที่ความรับผิดชอบของแต่ละคนได้แสดงไว้ในตาราง RACI ผู้มีส่วนได้เสียภายนอกรวมถึง ลูกค้า พันธมิตรทางธุรกิจ ผู้ถือหุ้น และหน่วยงานกำกับดูแล ผู้มีส่วนได้เสียภายในได้แก่ คณะกรรมการบริหาร ผู้บริหาร เจ้าหน้าที่ และอาสาสมัคร
- **เป้าหมาย**—เป้าหมายของกระบวนการ นิยามไว้ว่าเป็น 'ข้อความที่อธิบายถึงผลลัพธ์ที่คาดหวังจากกระบวนการ ผลลัพธ์อาจจะเป็นสิ่งที่จัดทำขึ้นมา (artifact) การเปลี่ยนแปลงสถานะอย่างเป็นนัยสำคัญ หรือการปรับปรุงความสามารถของกระบวนการอื่นๆ อย่างเป็นนัยสำคัญ' เป้าหมายของกระบวนการเป็นส่วนหนึ่งของการส่งทอดเป้าหมาย (goal cascade) นั่นคือ เป้าหมายของกระบวนการสนับสนุนเป้าหมายที่เกี่ยวข้องกับไอที ซึ่งในทางเดียวกันก็สนับสนุนเป้าหมายขององค์กร

เป้าหมายของกระบวนการสามารถจัดประเภทได้ดังนี้:

– **เป้าหมายในตัวเอง** (Intrinsic goal)—กระบวนการมีคุณภาพในตัวเองหรือไม่ มีความถูกต้องแม่นยำและสอดคล้องกับแนวปฏิบัติที่ดีหรือไม่ เป็นตามตามกฎทั้งภายในและภายนอกหรือไม่
– **เป้าหมายเชิงบริบท** (Contextual goal)—กระบวนการได้ถูกปรับแต่งและรับมาใช้ให้เข้ากับสถานการณ์เฉพาะขององค์กรหรือไม่ กระบวนการมีความเกี่ยวข้อง เข้าใจได้ และง่ายต่อการนำไปประยุกต์ใช้งานหรือไม่
– **เป้าหมายการเข้าถึงและการรักษาความมั่นคงปลอดภัย**—กระบวนการเป็นความลับ และสามารถรับรู้และเข้าถึงได้เฉพาะผู้ที่จำเป็นใช้เมื่อต้องการ

ในแต่ละระดับของการส่งทอดเป้าหมาย ซึ่งรวมถึงกระบวนการด้วย มีการกำหนดมาตรวัดเพื่อวัดผลการบรรลุถึงเป้าหมาย มาตรวัดอาจสามารถระบุเป็น 'หน่วยเชิงปริมาณที่ช่วยวัดการบรรลุถึงเป้าหมายของกระบวนการ มาตรวัดควรเป็น SMART – เฉพาะเจาะจง (Specific) วัดผลได้ (Measurable) สามารถนำไปปฏิบัติได้จริง (Actionable) มีความเกี่ยวเนื่อง (Relevant) และทันเวลา (Timely)'

ในการบริหารจัดการปัจจัยเอื้อให้มีประสิทธิภาพและประสิทธิผล จำเป็นต้องกำหนดมาตรวัดเพื่อวัดว่าบรรลุผลลัพธ์ที่คาดหวังมากน้อยเพียงใด นอกจากนี้ ในมุมมองที่สองของการบริหารประสิทธิภาพในการดำเนินงานของปัจจัยเอื้อยังได้อธิบายถึงการนำแนวปฏิบัติที่ดีมาประยุกต์ใช้ ซึ่งสามารถกำหนดมาตรวัดที่เกี่ยวข้องขึ้นมาเพื่อช่วยในการบริหารปัจจัยเอื้อ

- **วัฏจักร**—แต่ละกระบวนการมีวัฏจักรในการดำเนินงาน ซึ่งได้แก่ กำหนดขึ้น จัดทำให้มีขึ้น ดำเนินงาน เฝ้าติดตาม และแก้ไข/ปรับปรุง หรือเลิกใช้งาน แนวปฏิบัติทั่วไปดังเช่นที่ได้ระบุไว้ในต้นแบบการประเมินกระบวนการ (process assessment model) ของ COBIT ซึ่งอิงกับมาตรฐาน ISO/IEC 15504 จะช่วยในการระบุ การดำเนินการ การเฝ้าติดตาม และการทำให้กระบวนการนั้นให้ประโยชน์สูงสุด
- **แนวปฏิบัติที่ดี**— ในเอกสาร *การสัมฤทธิ์ผลของกระบวนการของ COBIT 5 (COBIT 5: Enabling process*) มีต้นแบบอ้างอิงของกระบวนการ (process reference model) ซึ่งได้อธิบายรายละเอียดมากขึ้นสำหรับแนวปฏิบัติที่ดีสำหรับกระบวนการภายใน ได้แก่ แนวปฏิบัติ กิจกรรม และกิจกรรมย่อย[14]

แนวปฏิบัติ

- สำหรับแต่ละกระบวนการใน COBIT 5 แนวปฏิบัติเกี่ยวกับการกำกับดูแล/การบริหารจัดการได้ให้ข้อกำหนดในภาพรวมที่เป็นชุดสมบูรณ์สำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่มีประสิทธิผล ซึ่งประกอบด้วย
  - คำแถลงการณ์กระทำ (Statements of actions) เพื่อส่งมอบผลประโยชน์ เพื่อรักษาระดับความเสี่ยงในระดับที่เหมาะสมและเพื่อการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด
  - สอดคล้องกับมาตรฐานและแนวปฏิบัติที่ดีที่เกี่ยวข้อง ซึ่งเป็นที่ยอมรับกันโดยทั่วไป
  - มีลักษณะทั่วไป (Generic) จึงจำเป็นต้องนำมาปรับใช้ให้เหมาะสมสำหรับแต่ละองค์กร
  - ครอบคลุมถึงผู้ที่มีบทบาทหน้าที่ทั้งในภาคธุรกิจและภาคไอทีในกระบวนการ (ตั้งแต่ต้นจนจบ)
- หน่วยงานกำกับดูแลและผู้บริหารขององค์กรจำเป็นต้องตัดสินใจเลือกในเรื่องที่เกี่ยวข้องกับแนวปฏิบัติด้านการกำกับดูแลและการบริหารจัดการ โดย
  - เลือกสิ่งที่สามารถนำมาประยุกต์ใช้ได้ และตัดสินใจว่าสิ่งใดที่จะนำมาใช้
  - เพิ่มเติม และ/หรือปรับใช้แนวปฏิบัติตามความจำเป็น
  - กำหนดและเพิ่มเติมแนวปฏิบัติที่ไม่เกี่ยวข้องกับไอที เพื่อบูรณาการให้เข้ากับกระบวนการทางธุรกิจ
  - เลือกว่าจะนำไปใช้อย่างไร (ความถี่ ขอบเขต ความเป็นอัตโนมัติ และอื่นๆ)
  - ยอมรับความเสี่ยงจากการไม่นำสิ่งที่อาจนำไปประยุกต์ใช้ได้ไปใช้

กิจกรรม—ใน COBIT ได้แก่การกระทำที่สำคัญเพื่อดำเนินกระบวนการ

- นิยามว่าเป็น 'แนวทางเพื่อช่วยให้บรรลุแนวปฏิบัติในการบริหารจัดการสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร' กิจกรรมต่างๆ ใน COBIT 5 ได้ให้แนวทางว่าจะต้องนำอะไรไปใช้งานในแต่ละแนวปฏิบัติของการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร นำไปใช้อย่างไรและทำไมต้องนำไปใช้ เพื่อที่จะปรับปรุงประสิทธิภาพในการดำเนินงานด้านไอที และ/หรือจัดการกับความเสี่ยงในการส่งมอบกระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จด้านไอทีและการส่งมอบบริการ ข้อมูลเหล่านี้เป็นประโยชน์ต่อ
  - ผู้บริหาร ผู้ให้บริการ ผู้ใช้งาน และผู้ประกอบวิชาชีพด้านไอที ผู้ซึ่งจำเป็นต้องวางแผน จัดทำ ดำเนินการ หรือเฝ้าติดตามไอทีระดับองค์กร
  - ผู้ประกอบวิชาชีพด้านการให้ความเชื่อมั่น (assurance professional) ผู้ซึ่งให้ความเห็นเกี่ยวกับการนำไปใช้งานในปัจจุบันหรือที่กำลังนำเสนอ หรือการปรับปรุงที่จำเป็น
- ชุดของกิจกรรมทั่วไปและกิจกรรมเฉพาะที่ครบถ้วนสมบูรณ์ ซึ่งให้วิธีปฏิบัติหนึ่งเดียวที่ประกอบด้วยขั้นตอนทั้งหมดที่จำเป็นและเพียงพอสำหรับการบรรลุถึงแนวปฏิบัติหลักด้านการกำกับดูแล (GP) และด้านการบริหารจัดการ (MP) และยังให้แนวทางในภาพรวมในระดับที่ต่ำกว่า GP/MP สำหรับการประเมินผลการดำเนินงานที่เกิดขึ้นจริง และเพื่อพิจารณาถึงการปรับปรุงที่อาจเกิดขึ้น กิจกรรมประกอบด้วย
  – การอธิบายถึงชุดของขั้นตอนที่จำเป็นและเพียงพอสำหรับการนำไปใช้งานในเชิงปฏิบัติ เพื่อบรรลุ GP/MP
  – พิจารณาถึงข้อมูลรับเข้า (input) และผลลัพธ์ของกระบวนการ
  – อิงกับมาตรฐานและแนวปฏิบัติที่ดีที่ยอมรับกันโดยทั่วไป
  – สนับสนุนการจัดให้มีบทบาทหน้าที่และความรับผิดชอบที่ชัดเจน
  – ไม่ตายตัว และจำเป็นต้องนำมาปรับใช้และพัฒนาไปสู่กระบวนการเฉพาะที่เหมาะสมสำหรับองค์กร

กิจกรรมย่อย—กิจกรรมอาจจะไม่มีรายละเอียดเพียงพอในการนำไปใช้งาน อาจจำเป็นต้องใช้แนวทางเพิ่มเติม
– จากมาตรฐานและแนวปฏิบัติที่ดีที่เกี่ยวข้อง เช่น ITIL ชุด ISO/IEC 27000 และ PRINCE2
– จากการพัฒนาเพิ่มเติมเมื่อมีรายละเอียดมากขึ้นหรือมีกิจกรรมเฉพาะโดยมีการพัฒนาเพิ่มในชุดผลิตภัณฑ์ของ COBIT 5

ข้อมูลรับเข้าและผลลัพธ์—ข้อมูลรับเข้าและผลลัพธ์ใน COBIT 5 เป็นชิ้นงานหรือสิ่งที่ทำขึ้นของกระบวนการที่ถือว่าเป็นสิ่งจำเป็นในการสนับสนุนการดำเนินกระบวนการ ซึ่งเอื้อต่อการตัดสินใจที่สำคัญ ให้ข้อมูลและร่องรอยสำหรับการตรวจสอบกิจกรรมของกระบวนการ และเอื้อต่อการติดตามเมื่อเกิดเหตุการณ์ผิดปกติขึ้น กิจกรรมย่อยกำหนดขึ้นในระดับของแนว

[14]เฉพาะแนวปฏิบัติและกิจกรรมเท่านั้นที่ได้รับการพัฒนาภายใต้โครงการปัจจุบัน ระดับของรายละเอียดที่มากขึ้นยังจำเป็นต้องพัฒนาเพิ่มเติม ได้แก่ แนวทางสำหรับวิชาชีพต่างๆ ที่ให้แนวทางเฉพาะวิชาชีพ นอกจากนี้ แนวทางเพิ่มเติมยังสามารถหาได้จากมาตรฐานและกรอบการดำเนินงานอื่นๆ ที่เกี่ยวข้อง ดังที่ได้ระบุไว้ในคำอธิบายกระบวนการในรายละเอียด

ปฏิบัติหลักด้านการกำกับดูแล/การบริหารจัดการ และอาจรวมถึงชิ้นงานที่ใช้เฉพาะภายในกระบวนการนั้นๆ และบ่อยครั้งจะเป็นข้อมูลรับเข้าที่จำเป็นสำหรับกระบวนการอื่นๆ[15]

แนวปฏิบัติที่ดีจากภายนอก อาจมีรูปแบบและระดับของรายละเอียดที่แตกต่างกัน และส่วนใหญ่จะอิงกับมาตรฐานและกรอบการดำเนินงานอื่นๆ COBIT สอดคล้องกับมาตรฐานที่เกี่ยวข้องเหล่านี้และมีข้อมูลการเปรียบเทียบไว้ให้ ผู้ใช้จึงสามารถอ้างอิงแนวปฏิบัติที่ดีจากภายนอกเหล่านี้ได้ตลอดเวลา

การบริหารจัดการประสิทธิภาพในการดำเนินงานของปัจจัยเอื้อ

องค์กรคาดหวังผลลัพธ์ในด้านดีจากระบบงานและการใช้ปัจจัยเอื้อ สำหรับการบริหารจัดการประสิทธิภาพในการดำเนินงานของปัจจัยเอื้อ คำถามต่อไปนี้จำเป็นต้องได้รับการเฝ้าติดตามและหาคำตอบจากมาตรวัดอย่างสม่ำเสมอ

- มีการระบุถึงความต้องการของผู้มีส่วนได้เสียหรือไม่
- บรรลุเป้าหมายของปัจจัยเอื้อหรือไม่
- วัฏจักรของปัจจัยเอื้อได้รับการจัดการหรือไม่
- มีการนำแนวปฏิบัติที่ดีมาประยุกต์ใช้หรือไม่

ในกรณีของปัจจัยเอื้อด้านกระบวนการ 2 หัวข้อแรกเกี่ยวข้องกับผลลัพธ์ของกระบวนการที่เกิดขึ้นจริง มาตรวัดที่ใช้วัดว่าได้บรรลุเป้าหมายมากน้อยเพียงใดนั้นเรียกว่า 'ดัชนีตาม (lag indicator)' ใน COBIT 5: การสัมฤทธิ์ผลของกระบวนการ (COBIT 5: Enabling Process) มีการกำหนดมาตรวัดจำนวนหนึ่งสำหรับแต่ละเป้าหมายของกระบวนการ

2 หัวข้อหลังเกี่ยวข้องกับหน้าที่การทำงานจริงของปัจจัยเอื้อ และมาตรวัดสำหรับกลุ่มนี้จะเรียกว่า 'ดัชนีนำ (lead indicator)'

ระดับความสามารถของกระบวนการ (Process capability level)–ของ COBIT 5 ได้รวมเอาแบบแผนการประเมินความสามารถของกระบวนการจาก ISO /IEC 15504 โดยได้อธิบายไว้ในบทที่ 8 ของ COBIT 5 และยังมีแนวทางเพิ่มเติมที่สามารถหาได้จากในเอกสารเล่มอื่นของ COBIT 5 ที่ตีพิมพ์โดย ISACA โดยสรุปแล้ว ระดับความสามารถกระบวนการวัดผลทั้งการบรรลุเป้าหมายหมายและการประยุกต์ใช้แนวปฏิบัติที่ดี

ความสัมพันธ์กับปัจจัยเอื้ออื่นๆ – มีการเชื่อมโยงกันระหว่างกระบวนการและปัจจัยเอื้อประเภทอื่นๆ ผ่านทางความสัมพันธ์ต่อไปนี้

- กระบวนการต้องการสารสนเทศ (เป็นส่วนหนึ่งของข้อมูลรับเข้า) และกระบวนการสามารถทำให้เกิดสารสนเทศได้ (เป็นชิ้นงาน (work product))
- กระบวนการจำเป็นต้องมีโครงสร้างการจัดองค์กรและบทบาทหน้าที่ในการดำเนินงาน (ตามที่ระบุไว้ในตาราง RACI ยกตัวอย่างเช่น คณะกรรมการอำนวยการด้านไอที (IT steering committee) คณะกรรมการความเสี่ยงองค์กร (enterprise risk committee) คณะกรรมการบริหาร หน่วยงานตรวจสอบ ผู้บริหารสูงสุดด้านสารสนเทศ (CIO) ประธานเจ้าหน้าที่บริหาร (CEO)
- กระบวนการทำให้เกิดและต้องการใช้ความสามารถในการให้บริการ (โครงสร้างพื้นฐาน ระบบงาน และอื่นๆ)
- กระบวนการอาจและจะขึ้นอยู่กับกระบวนการอื่น
- กระบวนการกำหนดหรือจำเป็นต้องมีนโยบายและขั้นตอนการปฏิบัติงานเพื่อให้มั่นใจถึงความสอดคล้องกันในการนำไปใช้งานและการใช้ปฏิบัติ
- มุมมองด้านวัฒนธรรมและพฤติกรรมจะกำหนดว่ากระบวนการจะถูกนำไปปฏิบัติได้ดีมากน้อยเพียงใด

ตัวอย่างในเชิงปฏิบัติของปัจจัยเอื้อด้านกระบวนการ

ตัวอย่างที่ 10 แสดงถึงปัจจัยเอื้อด้านกระบวนการ การเชื่อมโยงกันระหว่างปัจจัยเอื้อ และมิติต่างๆ ของปัจจัยเอื้อ ตัวอย่างนี้จัดทำตามตัวอย่างที่ 7 ที่กล่าวไว้ก่อนหน้านี้

ต้นแบบอ้างอิงของกระบวนการใน COBIT 5

กระบวนการกำกับดูแลและบริหารจัดการ

หนึ่งในหลักการสำคัญของ COBIT คือความแตกต่างระหว่างการกำกับดูแลและการบริหารจัดการ ในหลักการนี้ทุกองค์กรล้วนคาดหวังให้นำกระบวนการต่างๆ ด้านการกำกับดูแลและกระบวนการต่างๆ ด้านการบริหารจัดการไปใช้งานเพื่อให้เกิดการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรอย่างครอบคลุม

[15]รายการที่แสดงถึงข้อมูลรับเข้าและผลลัพธ์ใน COBIT 5 ไม่ควรถือว่ามีเพียงข้อมูลตามที่รายการแสดงไว้เท่านั้น เพราะอาจมีการระบุกระแสสารสนเทศเพิ่มเติมขึ้นอีกได้ ขึ้นอยู่กับสภาพแวดล้อมขององค์กรและกรอบการดำเนินงานของกระบวนการ

เมื่อพิจารณาถึงกระบวนการด้านการกำกับดูแลและการบริหารจัดการในบริบทขององค์กรแล้ว ความแตกต่างระหว่างประเภทของกระบวนการอยู่ที่วัตถุประสงค์ของกระบวนการ

- **กระบวนการด้านการกำกับดูแล**—กระบวนการด้านการควบคุมกำกับดูแลจะใช้กับวัตถุประสงค์ด้านการกำกับดูแลผู้มีส่วนได้เสีย—การส่งมอบคุณค่า การรักษาระดับความเสี่ยงให้เหมาะสม และการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด—และรวมถึงแนวปฏิบัติและกิจกรรมที่มุ่งไปยังการประเมินทางเลือกด้านกลยุทธ์ การให้ทิศทางด้านไอที และการเฝ้าติดตามผลลัพธ์ (EDM- ที่เป็นไปตามแนวคิดของมาตรฐาน ISO/IEC 38500)
- **กระบวนการบริหารจัดการ**—เป็นไปตามคำนิยามของการบริหารจัดการ แนวปฏิบัติ และกิจกรรรมในกระบวนการบริหารจัดการที่ครอบคลุมถึงหน้าที่ความรับผิดชอบด้านการวางแผน จัดสร้าง ดำเนินการและเฝ้าติดตาม (PBRM-Plan, Build, Run and Monitor) ไอทีระดับองค์กร และต้องให้การครอบคลุมไอทีอย่างครบวงจร

ตัวอย่างที่ 10—การเชื่อมโยงกันในระหว่างปัจจัยเอื้อด้านกระบวนการ

องค์กรได้แต่งตั้ง 'ผู้จัดการกระบวนการ' สำหรับกระบวนการที่เกี่ยวข้องกับไอที เพื่อรับผิดชอบในการกำหนดและดำเนินกระบวนการให้มีประสิทธิภาพและประสิทธิผล ในบริบทของการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

เริ่มด้วยผู้จัดการกระบวนการจะมุ่งเน้นไปที่ปัจจัยเอื้อด้านกระบวนการ โดยพิจารณาถึงมิติต่างๆ ของปัจจัยเอื้อ

- **ผู้มีส่วนได้เสีย**:ผู้มีส่วนได้เสียของกระบวนการซึ่งรวมถึงผู้กระทำการในกระบวนการทั้งหมด (process actor) ได้แก่ ทุกฝ่ายที่รับผิดชอบตามหน้าที่ รับผิดชอบในผลงาน (Accountability) ให้คำปรึกษา (Consulted) หรือได้รับแจ้งให้ทราบ (Informed) (RACI) สำหรับหรือในระหว่างการดำเนินกิจกรรมของกระบวนการ เพื่อการนี้ สามารถใช้ตาราง RACI Chart ตามที่ได้ได้อธิบายไว้ใน COBIT 5: ***การสัมฤทธิ์ผลของกระบวนการ*** (COBIT 5: Enabling Process)
- **เป้าหมาย**: แต่ละกระบวนการจะต้องกำหนดเป้าหมายที่เหมาะสมและมาตรวัดที่เกี่ยวข้อง ยกตัวอย่างเช่น กระบวนการ AP008 ***บริหารจัดการความสัมพันธ์*** ใน *COBIT 5: **การสัมฤทธิ์ผลของกระบวนการ** (COBIT 5: Enabling Process)* เราสามารถค้นหาชุดเป้าหมายของกระบวนการและมาตรวัด เช่น
  - **เป้าหมาย**: มีความเข้าใจกลยุทธ์ทางธุรกิจ แผนงาน และความต้องการต่างๆ อย่างถ่องแท้จัดทำเป็นเอกสารและได้รับการอนุมัติ
    - **มาตรวัด**: ร้อยละของชุดโครงการ (programmes) ที่สอดคล้องกับความต้องการทางธุรกิจ/ลำดับความสำคัญขององค์กร
  - **เป้าหมาย**: ความสัมพันธ์ที่ดีระหว่างองค์กรกับหน่วยงานด้านไอที
    - **มาตรวัด**: คะแนนจากผลสำรวจความพึงพอใจของผู้ใช้และบุคคลากรด้านไอที
- **วัฏจักร**: แต่ละกระบวนการมีวัฏจักร ได้แก่ สร้างขึ้น ดำเนินการ และเฝ้าติดตาม รวมทั้งปรับเปลี่ยนตามความเหมาะสม ท้ายที่สุดกระบวนการก็จะถูกยกเลิกไป ในกรณีนี้ ก่อนอื่นผู้จัดการกระบวนการจำเป็นต้องออกแบบและกำหนดกระบวนการขึ้นมาเป็นอย่างแรก โดยสามารถใช้องค์ประกอบต่างๆ ใน *COBIT 5: **การสัมฤทธิ์ผลของกระบวนการ** (COBIT 5: Enabling Process)* เพื่อออกแบบกระบวนการ ได้แก่ ใช้ในการกำหนดหน้าที่ความรับผิดชอบและแตกกระบวนการลงมาเป็นแนวปฏิบัติและกิจกรรมต่างๆ รวมถึงระบุชิ้นงาน (work product) ของกระบวนการ (ข้อมูลรับเข้าและผลลัพธ์) ขั้นตอนถัดมา กระบวนการจำเป็นต้องมีความทนทาน (robust) และมีประสิทธิภาพมากขึ้น และด้วยจุดประสงค์ดังกล่าวผู้จัดการกระบวนการสามารถเพิ่มระดับความสามารถของกระบวนการได้ ต้นแบบความสามารถกระบวนการ (process capability model) และคุณลักษณะความสามารถของกระบวนการ (process capability attribute) ใน COBIT 5 ที่อ้างอิงมาจาก ISO/IEC 15504 สามารถนำมาใช้สำหรับจุดประสงค์ดังกล่าว เช่น
  - ความสามารถของกระบวนการระดับ 2 จะต้องบรรลุคุณลักษณะ 2 ประการ ได้แก่ การบริหารจัดการประสิทธิภาพในการดำเนินงาน (performance management) และการบริหารจัดการชิ้นงาน (work product management) คุณลักษณะแรกจำเป็นต้องมีกิจกรรมต่างๆ ที่เกี่ยวข้องกับระยะในการวางแผน ได้แก่ เช่น
    - กำหนดวัตถุประสงค์สำหรับประสิทธิภาพของกระบวนการ
    - มีการวางแผนด้านประสิทธิภาพของกระบวนการ
    - มีการกำหนดหน้าที่ความรับผิดชอบในการดำเนินกระบวนการ
    - มีการกำหนดทรัพยากรที่ต้องใช้
    - อื่นๆ

    ที่ระดับของความสามารถเดียวกันนี้ ได้ระบุถึงกิจกรรมต่างๆ ในระยะของ 'การเฝ้าติดตาม' ภายใต้วัฏจักรของกระบวนการ อาทิเช่น
    - การเฝ้าติดตามประสิทธิภาพในการดำเนินงานของกระบวนการ
    - ประสิทธิภาพในการดำเนินงานของกระบวนการได้รับการปรับแก้ให้เป็นไปตามแผน
    - อื่นๆ
  - เราสามารถใช้วิธีปฏิบัติเดียวกันนี้เพื่อที่จะให้ได้แนวทางสำหรับระยะอื่นๆ ภายใต้วัฏจักร จากคุณลักษณะของประสิทธิภาพความสามารถต่างๆ ในระดับความสามารถของกระบวนการที่เพิ่มขึ้น
- **แนวปฏิบัติที่ดี**: COBIT 5 ได้อธิบายถึงแนวปฏิบัติที่ดีอย่างละเอียดสำหรับกระบวนการต่างๆ ไว้ใน *COBIT 5: การสัมฤทธิ์ผลของกระบวนการ (COBIT 5: Enabling Process)* ตามที่ได้กล่าวไว้ในหัวข้อก่อน โดยมีแรงบันดาลใจและตัวอย่างของกระบวนการต่างๆ แสดงไว้ซึ่งครอบคลุมถึงกิจกรรมหลากหลายอย่างครบด้วนสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่ดี

นอกจากแนวทางในเรื่องของปัจจัยเอื้อด้านกระบวนการแล้ว ผู้จัดการกระบวนการอาจจะตัดสินใจที่จะพิจารณาปัจจัยเอื้อ อื่นๆ ด้วย เช่น

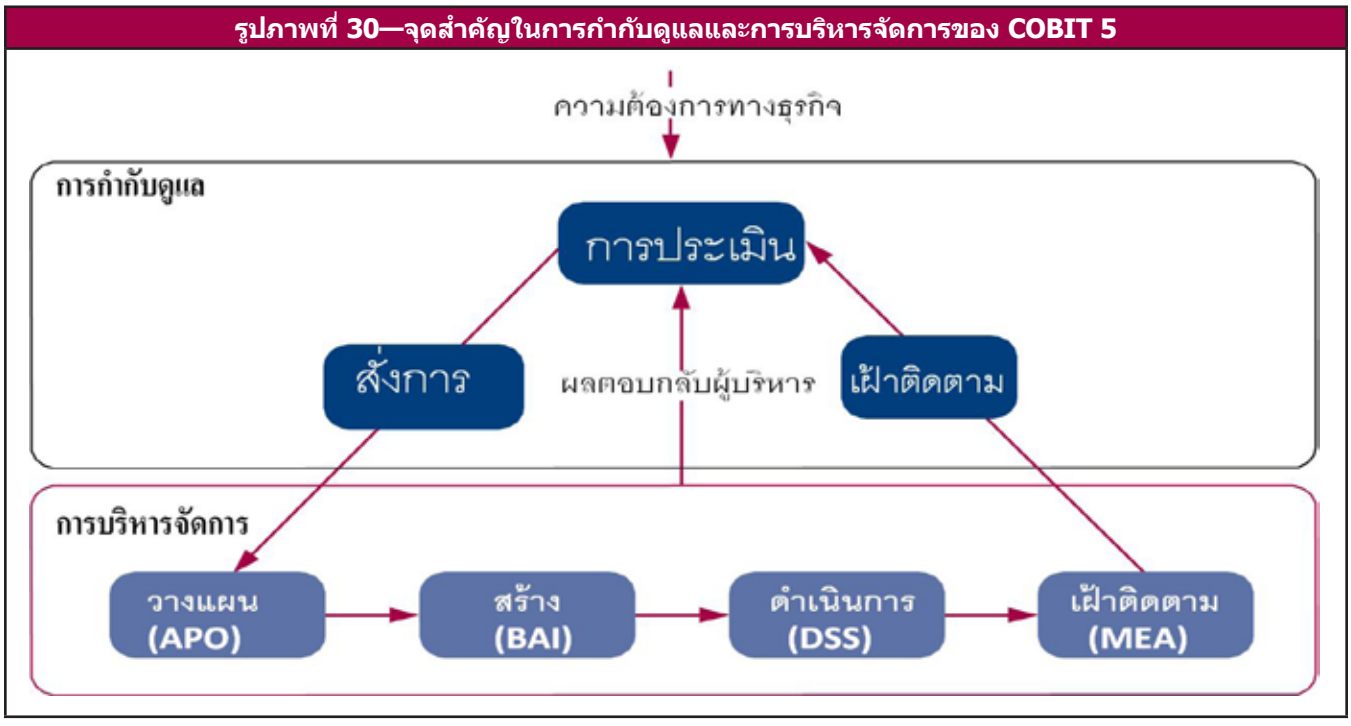
- ตาราง RACI ได้อธิบายถึงบทบาทแหน้าที่และความรับผิดชอบ ปัจจัยเอื้ออื่นๆ จะช่วยให้สามารถลงไปในรายละเอียดของมิตินี้ เช่น
  - ในเรื่องทักษะและความสามารถของปัจจัยเอื้อ จะต้องกำหนดทักษะและความสามารถที่จำเป็นต้องมีสำหรับแต่ละบทบาทหน้าที่ และกำหนดเป้าหมายที่เหมาะสม (เช่น ระดับของทักษะทางพฤติกรรมและทางเทคนิค) และสามารถกำหนดมาตรวัดที่เกี่ยวข้อง
  - ตาราง RACI ได้บรรจุโครงสร้างองค์กรต่างๆ ไว้ ซึ่งโครงสร้างเหล่านี้ได้มีอธิบายเพิ่มเติมไว้ในปัจจัยเอื้อด้านโครงสร้างองค์กร ซึ่งได้ให้รายละเอียดของโครงสร้างมากขึ้น มีการกำหนดผลลัพธ์ที่คาดหวังและมาตรวัดที่เกี่ยวข้อง (เช่น การตัดสินใจ) มีการกำหนดแนวปฏิบัติที่ดี (เช่น ขอบเขตของการควบคุม หลักการดำเนินงานของโครงสร้าง ระดับของอำนาจในการสั่งการ)
  - หลักการและนโยบายจะทำให้กระบวนการเป็นทางการและอธิบายถึงเหตุผลของความจำเป็นที่จะต้องมีกระบวนการนี้ ใครเป็นผู้ที่เกี่ยวข้องและจะใช้อย่างไร ซึ่งเป็นจุดที่สำคัญของปัจจัยเอื้อด้านหลักการและนโยบาย

.ถึงแม้ว่าผลลัพธ์ของกระบวนการทั้ง 2 ประเภทจะมีความแตกต่างกันและมีบุคคลที่เกี่ยวข้องที่แตกต่างกัน แต่ภายในแล้วภายใต้บริบทของกระบวนการ กระบวนการทั้งหมดจำเป็นต้องมีกิจกรรมต่างๆ ในการวางแผน การจัดทำหรือการนำไปใช้งาน การปฏิบัติ และการเฝ้าติดตาม ภายในกระบวนการ

ต้นแบบอ้างอิงของกระบวนการใน COBIT 5
COBIT 5 ไม่ใช่สิ่งที่ตายตัว แต่จากรายละเอียดข้างต้นเป็นที่ชัดเจนว่า COBIT 5 สนับสนุนให้องค์กรนำกระบวนการกำกับดูแลและบริหารจัดการไปใช้งานโดยได้ครอบคลุมถึงหัวข้อหลักตามที่แสดงไว้ใน**รูปภาพที่ 30**

ในทางทฤษฎีแล้ว องค์กรสามารถจัดให้มีกระบวนการต่างๆ ตามที่เห็นว่าเหมาะสม ตราบใดที่ยังครอบคลุมวัตถุประสงค์ขั้นพื้นฐานของการกำกับดูแลและการบริหารจัดการ เพื่อให้ครอบคลุมวัตถุประสงค์เดียวกัน องค์กรขนาดเล็กอาจใช้เพียงไม่กี่กระบวนการในขณะที่องค์กรที่ขนาดใหญ่และซับซ้อนกว่าอาจจะจำเป็นต้องมีกระบวนการมากมาย

รูปภาพที่ 30—จุดสำคัญในการกำกับดูแลและการบริหารจัดการของ COBIT 5



COBIT 5 ได้รวมเอาต้นแบบอ้างอิงของกระบวนการที่ระบุและอธิบายถึงรายละเอียดของกระบวนการกำกับดูแลและบริหารจัดการต่างๆ โดยให้ต้นแบบอ้างอิงของกระบวนการที่เป็นตัวแทนของกระบวนการทั้งหมดที่เกี่ยวข้องกับกิจกรรมทางด้านไอทีซึ่งมักจะพบในองค์กร ช่วยให้มีต้นแบบอ้างอิงที่ใช้ร่วมกันระหว่างผู้ปฏิบัติงานด้านไอทีและผู้จัดการทางธุรกิจซึ่งสามารถเข้าใจได้ ต้นแบบของกระบวนการที่นำเสนอนี้เป็นต้นแบบที่มีความครบถ้วนสมบูรณ์และครอบคลุม แต่ไม่ได้เป็นแค่ต้นแบบเดียวเท่านั้นที่สามารถใช้ได้ แต่ละองค์กรจะต้องกำหนดชุดของกระบวนการขึ้นมาใช้โดยคำนึงถึงความเหมาะสมในแต่ละสถานการณ์

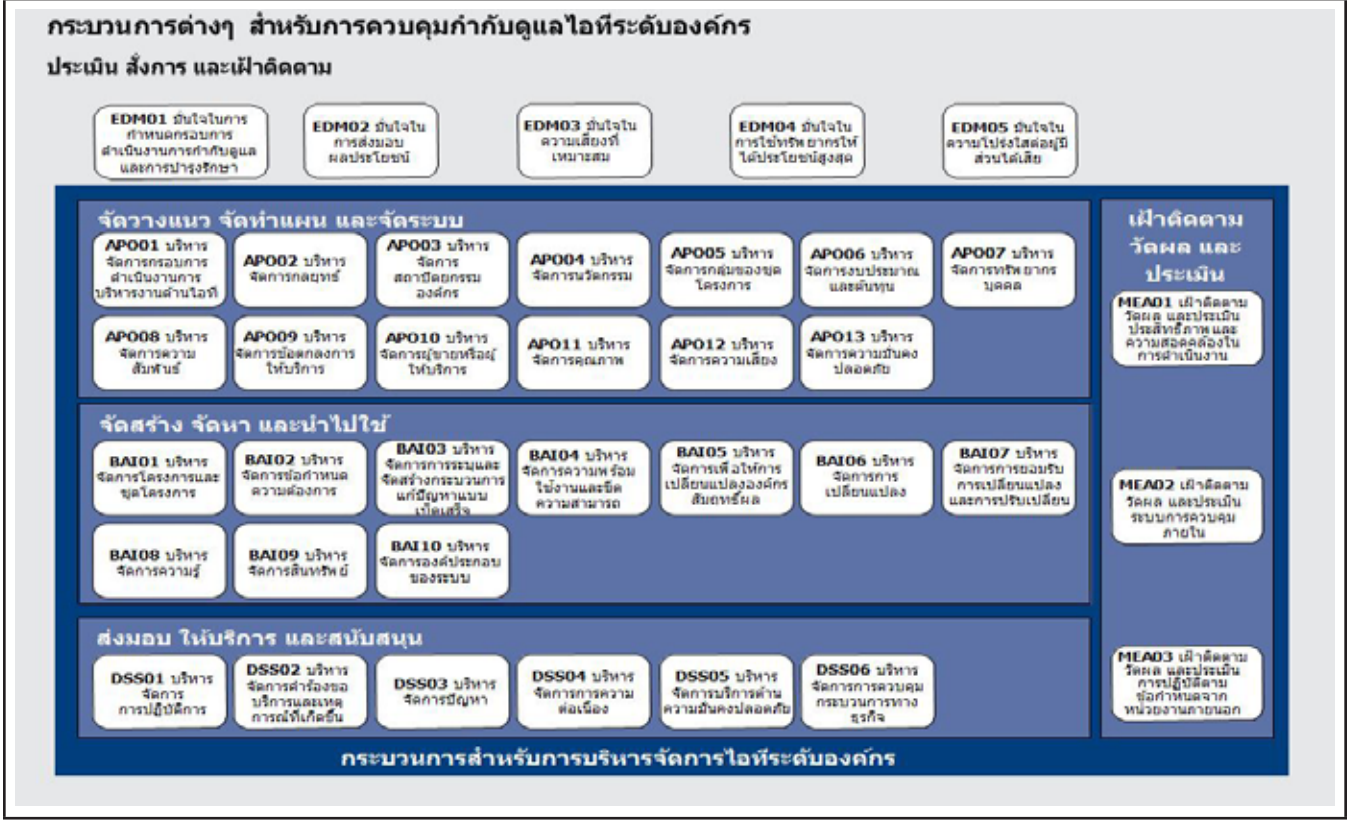
โดยการรวมเอารูปแบบในการดำเนินงาน (Operational model) และภาษาสามัญทั่วไป (common language) เข้าไปไว้ในทุกส่วนขององค์กรที่เกี่ยวข้องกับกิจกรรมด้านไอที ถือเป็นขั้นตอนที่จำเป็นและสำคัญอย่างยิ่งที่จะนำไปสู่การกำกับดูแลที่ดีและยังให้กรอบดำเนินการสำหรับการวัดผลและการเฝ้าติดตามประสิทธิภาพในการดำเนินงานด้านไอที สื่อสารกับผู้ให้บริการและบูรณาการแนวปฏิบัติที่ดีที่สุดในการบริหารจัดการ

ต้นแบบอ้างอิงของกระบวนการใน COBIT 5 แบ่งกระบวนการด้านการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร ออกเป็น 2 กลุ่มกิจกรรมที่สำคัญ—การกำกับดูแลและการบริหารจัดการ—และยังแบ่งย่อยเพิ่มเติมออกเป็นโดเมนของกระบวนการดังนี้

- **การควบคุมกำกับดูแล**—โดเมนนี้มีกระบวนการกำกับดูแล 5 กระบวนการ ซึ่งในแต่ละกระบวนการมีการกำหนดแนวปฏิบัติสำหรับประเมิน สั่งการ และเฝ้าติดตาม (EDM)
- **การบริหารจัดการ**—โดเมนทั้ง 4 นี้สอดคล้องกับจุดที่เป็นความรับผิดชอบของ PBRM (วางแผน จัดทำ ดำเนินการ และเฝ้าติดตาม) (วิวัฒนาการจากโดเมนต่างๆ ของ COBIT 4.1) และครอบคลุมไอทีอย่างครบวงจร แต่ละโดเมนมีกระบวนการต่างๆ เช่นเดียวกับใน COBIT 4.1 และรุ่นอื่นๆ ก่อนหน้านั้น จากที่ได้อธิบายไปแล้ว ถึงแม้ว่ากระบวนการส่วนใหญ่จำเป็นต้องมีกิจกรรมด้าน 'การวางแผน' 'การนำไปใช้งาน' 'การปฏิบัติงาน' และ 'การเฝ้าติดตาม' ภายในกระบวนการหรือภายในประเด็นที่กำลังพิจารณาอยู่ (เช่น คุณภาพ การรักษาความมั่นคงปลอดภัย) กิจกรรมเหล่านี้ได้ถูกจัดไปไว้ในแต่ละโดเมนตามจุดของกิจกรรมที่โดยทั่วไปแล้วมีความเกี่ยวเนื่องที่ใกล้ชิดมากที่สุดเมื่อกล่าวถึงเรื่องของไอทีในระดับองค์กร

ใน COBIT 5 กระบวนการยังได้ครอบคลุมถึงขอบเขตทั้งหมดของกิจกรรมทั้งทางธุรกิจและทางด้านไอทีที่เกี่ยวข้องกับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร ดังนั้นจึงทำให้ต้นแบบของกระบวนการใช้ได้ทั่วทั้งองค์กรอย่างแท้จริง ต้นแบบอ้างอิงของกระบวนการใน COBIT 5 พัฒนามาจากต้นแบบของกระบวนการใน COBIT 4.1 ที่ได้บูรณาการต้นแบบของกระบวนการใน Risk IT และ Val IT เข้าไปไว้ด้วย **รูปภาพที่ 31** แสดงถึงกระบวนการด้านการกำกับดูแลและการบริหารจัดการทั้ง 37 กระบวนการอย่างครบชุดใน COBIT 5 รายละเอียดของกระบวนการทั้งหมดตามที่ต้นแบบของกระบวนการได้อธิบายไว้ก่อนหน้านี้ได้รวมไว้ใน *COBIT 5: การสัมฤทธิ์ผลของกระบวนการ (COBIT 5: Enabling Processes)*

รูปภาพที่ 31—ต้นแบบอ้างอิงของกระบวนการใน COBIT 5



ปัจจัยเอื้อใน COBIT 5: โครงสร้างการจัดองค์กร

ข้อมูลรายละเอียดเฉพาะของปัจจัยเอื้อด้านโครงสร้างองค์กร เปรียบเทียบกับคำอธิบายปัจจัยเอื้อทั่วไป แสดงไว้ใน **รูปภาพที่ 32**

รูปแบบของโครงสร้างการจัดองค์กรแสดงให้เห็นถึง
- **ผู้มีส่วนได้เสีย**—ผู้มีส่วนได้เสียอาจอยู่ภายในหรือภายนอกองค์กรก็ได้ และรวมถึงสมาชิกแต่ละคนที่อยู่ในโครงสร้าง โครงสร้างอื่นๆ หน่วยงานต่างๆ ในองค์กร ลูกค้า ผู้ขาย/ผู้ให้บริการ และหน่วยงานกำกับดูแล บทบาทหน้าที่ของพวกเขาก็มีความหลากหลาย ซึ่งรวมถึงการตัดสินใจ การบังคับควบคุม และการให้คำแนะนำ ส่วนได้เสียของผู้มีส่วนได้เสียแต่ละคนก็มีความหลากหลาย เช่น ผลประโยชน์อะไรที่จะได้รับจากการตัดสินใจที่มาตามโครงสร้าง
- **เป้าหมาย**—เป้าหมายของปัจจัยเอื้อด้านโครงสร้างองค์กรรวมถึง การมอบหมายอำนาจที่เหมาะสม หลักการดำเนินงานที่ระบุไว้อย่างชัดเจน และการประยุกต์ใช้แนวปฏิบัติที่ดีอื่นๆ ผลลัพธ์ที่ได้จากปัจจัยเอื้อด้านโครงสร้างการจัดองค์กรควรรวมถึงกิจกรรมและการตัดสินใจต่างๆ ที่ดี
- **วัฏจักร**—โครงสร้างการจัดองค์กร มีวัฏจักรในการดำเนินงาน ซึ่งสร้างขึ้น ตั้งอยู่ และปรับแก้ และท้ายที่สุดก็จะถูกยกเลิกไป ในช่วงเริ่มต้นจะต้องระบุการมอบหมายอำนาจ—เป็นเหตุผลและจุดประสงค์สำหรับการมีโครงสร้างการจัดองค์กร
- **แนวปฏิบัติที่ดี**—แนวปฏิบัติที่ดีต่างๆ สำหรับการจัดโครงสร้างองค์กร สามารถแยกแยะได้เป็น
  - หลักการในการดำเนินงาน—การจัดระเบียบสำหรับการดำเนินงานของโครงสร้างที่สามารถนำไปปฏิบัติได้ เช่นความถี่ของการประชุม การจัดทำเอกสารต่างๆ และกฎในการรักษาความเป็นระเบียบเรียบร้อย (housekeeping rules)
  - ส่วนประกอบ—โครงสร้างมีสมาชิกซึ่งเป็นผู้มีส่วนได้เสียทั้งภายในและภายนอก
  - ขอบเขตของการควบคุม—การจำกัดวงของอำนาจในการตัดสินใจตามโครงสร้างการจัดองค์กร
  - ระดับของอำนาจ/สิทธิ์ในการตัดสินใจ—การตัดสินใจตามที่โครงสร้างที่ได้ให้อำนาจไว้
  - การมอบหมายอำนาจ—โครงสร้างสามารถมอบหมาย (บางส่วนของ) อำนาจในการตัดสินใจไปให้โครงสร้างอื่นที่ขึ้นต่อโครงสร้างนั้น
  - ขั้นตอนในการแจ้งเรื่องตามระดับ (Escalation procedures)—เส้นทางการแจ้งเรื่องตามระดับการสำหรับโครงสร้างหนึ่งๆ จะอธิบายถึงการกระทำที่จำเป็นในกรณีที่เกิดปัญหาในการตัดสินใจ

รูปภาพที่ 32—ปัจจัยเอื้อใน COBIT 5: โครงสร้างการจัดองค์กร

ความสัมพันธ์กับปัจจัยเอื้ออื่นๆ —ความเชื่อมโยงกับปัจจัยเอื้ออื่นๆ รวมถึง
- ตาราง RACI เชื่อมกิจกรรมต่างๆ ของกระบวนการกับโครงสร้างการจัดองค์กร และ/หรือกับบทบาทหน้าที่ของแต่ละบุคคลในองค์กร โดยอธิบายถึงระดับของการมีส่วนร่วมในกระบวนการของแต่ละบทบาทหน้าที่: รับผิดชอบตามหน้าที่ รับผิดชอบในผลงาน ให้คำปรึกษา หรือได้รับแจ้งให้ทราบ
- วัฒนธรรม จริยธรรม และพฤติกรรม เป็นสิ่งที่กำหนดความมีประสิทธิภาพและประสิทธิผลของโครงสร้างการจัดองค์กรและการตัดสินใจ
- องค์ประกอบของโครงสร้างการจัดองค์กรควรพิจารณาและกำหนดชุดของทักษะที่เหมาะสมของสมาชิกในโครงสร้าง
- การมอบหมายอำนาจและหลักการดำเนินงานของโครงสร้างการจัดองค์กร เป็นไปตามแนวทางของกรอบดำเนินงานด้านนโยบายที่มีอยู่
- ข้อมูลรับเข้าและผลลัพธ์—โครงสร้างจำเป็นต้องมีการรับเข้า (มักได้แก่ สารสนเทศ) ก่อนจะสามารถตัดสินใจโดยมีข้อมูลที่เหมาะสมและก่อให้เกิดผลลัพธ์ได้ ยกตัวอย่างเช่น การตัดสินใจ สารสนเทศอื่นๆ หรือการขอข้อมูลเพิ่มเติม

ภาพของโครงสร้างการจัดองค์กรใน COBIT 5
ตามที่ได้กล่าวไว้ในต้นแบบของกระบวนการใน COBIT 5 ว่าได้มีการจัดทำภาพแสดงต้นแบบอ้างอิงของกระบวนการใน COBIT 5 และอธิบายรายละเอียดไว้ใน *COBIT 5: การสัมฤทธิ์ผลของกระบวนการ (COBIT 5: Enabling Process)* ต้นแบบนี้รวมถึงตาราง RACI ซึ่งมีบทบาทและโครงสร้างจำนวนหนึ่ง **รูปภาพที่ 33** อธิบายถึงบทบาทหน้าที่และโครงสร้างที่ได้มีการกำหนดไว้แล้ว

หมายเหตุ
- หน้าที่การทำงานจริงที่มีอยู่ในองค์กรอาจไม่จำเป็นต้องเป็นไปตามบทบาทหน้าที่เหล่านี้ แต่อย่างไรก็ดี ข้อมูลเหล่านี้ให้ประโยชน์ในแง่ของการอธิบายถึงจุดประสงค์ของโครงสร้างหรือบทบาทหน้าที่ที่ยังคงใช้ได้สำหรับองค์กรส่วนใหญ่
- จุดประสงค์ของตารางนี้ ไม่ได้เป็นการกำหนดผังการจัดองค์กรที่ใช้ได้สำหรับทุกองค์กร แต่ควรดูไว้เป็นตัวอย่าง

รูปภาพที่ 33—บทบาทหน้าที่และโครงสร้างการจัดองค์กรของ COBIT 5

บทบาทหน้าที่/โครงสร้าง	คำนิยาม/คำอธิบาย
คณะกรรมการบริหาร	กลุ่มของผู้บริหารระดับสูงสุดและ/หรือกรรมการที่ไม่ใช่ผู้บริหารขององค์กร ที่รับผิดชอบในผลงานด้านการกำกับดูแลองค์กรและการควบคุมทรัพยากรขององค์กรโดยรวม
ประธานเจ้าหน้าที่บริหาร (CEO)	เจ้าหน้าที่ระดับสูงสุดที่รับผิดชอบด้านการบริหารจัดการทั้งหมดขององค์กร
ผู้บริหารสูงสุดด้านการเงิน (CFO)	เจ้าหน้าที่อาวุโสที่สุดขององค์กรที่รับผิดชอบในผลการบริหารจัดการด้านการเงินในทุกรูปแบบ ซึ่งรวมถึง ความเสี่ยงและการควบคุมด้านการเงิน และความเชื่อถือได้และความถูกต้องของบัญชี
ผู้บริหารสูงสุดด้านปฏิบัติการ(COO)	เจ้าหน้าที่อาวุโสที่สุดขององค์กรที่รับผิดชอบในผลปฏิบัติการขององค์กร
ผู้บริหารสูงสุดด้านความเสี่ยง(CRO)	เจ้าหน้าที่อาวุโสที่สุดขององค์กรที่รับผิดชอบในผลการบริหารความเสี่ยงในทุกรูปแบบทั่วทั้งองค์กร อาจมีการจัดตั้งหน้าที่งานสำหรับเจ้าหน้าที่ดูแลความเสี่ยงด้านไอทีขึ้นมาเพื่อดูแลความเสี่ยงที่เกี่ยวข้องกับไอที
ผู้บริหารสูงสุดด้านสารสนเทศ (CIO)	เจ้าหน้าที่อาวุโสที่สุดขององค์กรที่รับผิดชอบให้ไอทีเป็นไปในแนวทางเดียวกับกลยุทธ์ทางธุรกิจ และรับผิดชอบในผลงานด้านการวางแผน การจัดหาทรัพยากร และการบริหารจัดการเพื่อการส่งมอบบริการและกระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จด้านไอที เพื่อสนับสนุนวัตถุประสงค์ขององค์กร
ผู้บริหารสูงสุดด้านความมั่นคงปลอดภัยสารสนเทศ (CISO)	เจ้าหน้าที่อาวุโสที่สุดขององค์กรที่รับผิดชอบในผลงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรในทุกรูปแบบ
ผู้บริหารทางธุรกิจ	เจ้าหน้าที่อาวุโสขององค์กรที่รับผิดชอบในผลงานด้านปฏิบัติการของหน่วยงานหนึ่งๆ หรือบริษัทในเครือหนึ่งๆ
เจ้าของกระบวนการทางธุรกิจ	บุคคลที่รับผิดชอบในผลงานด้านประสิทธิภาพการดำเนินงานของกระบวนการ ในการบรรลุวัตถุประสงค์ในการผลักดันให้เกิดการปรับปรุง และในการอนุมัติการเปลี่ยนแปลงกระบวนการ
คณะกรรมการ (ผู้บริหารด้านไอที) ด้านกลยุทธ์	กลุ่มของผู้บริหารระดับสูงที่แต่งตั้งขึ้นโดยคณะกรรรมการบริหาร เพื่อให้มั่นใจว่าคณะกรรมการบริหารมีส่วนร่วมและได้รับทราบในเรื่องต่างๆ และการตัดสินใจที่สำคัญที่เกี่ยวข้องกับไอที คณะกรรมการรับผิดชอบในผลงานของการบริหารจัดการกลุ่ม (portfolio) ของการลงทุนที่มีไอทีเป็นปัจจัยเอื้อ บริการด้านไอที และสินทรัพย์ด้านไอที ทำให้มั่นใจได้ว่ามีการส่งมอบคุณค่าและบริหารจัดการความเสี่ยง โดยปกติแล้วคณะกรรมการจะมีสมาชิกของคณะกรรมการบริหารเป็นประธาน ไม่ใช่ผู้บริหารสูงสุดด้านสารสนเทศ (CIO)
คณะกรรมการอำนวยการ (โครงการและชุดโครงการ)	กลุ่มของผู้มีส่วนได้เสียและผู้เชี่ยวชาญที่รับผิดชอบในผลงานของการให้แนวทาง (guidance) สำหรับชุดโครงการ (programmes) และโครงการ ซึ่งรวมถึงการบริหารจัดการและการเฝ้าติดตามการวางแผน การจัดสรรทรัพยากร การส่งมอบผลประโยชน์และคุณค่า และการบริหารจัดการความเสี่ยงชุดโครงการและโครงการ
คณะกรรมการสถาปัตยกรรมระบบ	กลุ่มของผู้มีส่วนได้เสียและผู้เชี่ยวชาญที่รับผิดชอบในผลงานของการให้คำแนะนำในเรื่องที่เกี่ยวข้องและการตัดสินใจด้านสถาปัตยกรรมระบบขององค์กร และการกำหนดนโยบายและมาตรฐานด้านสถาปัตยกรรมระบบ
คณะกรรมการความเสี่ยงระดับองค์กร	กลุ่มของผู้บริหารระดับสูงขององค์กรที่รับผิดชอบในผลงานด้านความร่วมมือและความเห็นชอบร่วมกันในระดับองค์กรที่จะสนับสนุนกิจกรรมและการตัดสินใจต่างๆ ในเรื่องของการบริหารจัดการความเสี่ยงระดับองค์กร (ERM) สภาความเสี่ยงด้านไอที (IT risk Council) อาจจัดตั้งขึ้นเพื่อพิจารณาความเสี่ยงด้านไอทีในรายละเอียดและให้คำแนะนำแก่คณะกรรมการความเสี่ยงระดับองค์กร
หัวหน้าหน่วยงานทรัพยากรบุคคล	เจ้าหน้าที่อาวุโสที่สุดขององค์กรที่รับผิดชอบในผลงานด้านการวางแผนและนโยบายในเรื่องทั้งหมดที่เกี่ยวข้องกับทรัพยากรบุคคลในองค์กร
หน่วยงานกำกับดูแล	หน้าที่งานในองค์กรที่รับผิดชอบในการให้แนวทางที่เกี่ยวข้องกับการปฏิบัติตามกฎหมาย กฎระเบียบข้อบังคับ และสัญญา
หน่วยงานตรวจสอบ	หน้าที่งานในองค์กรที่รับผิดชอบในการจัดให้มีการตรวจสอบภายใน

รูปภาพที่ 33—บทบาทหน้าที่และโครงสร้างการจัดองค์กรของ COBIT 5 (ต่อ)	
บทบาทหน้าที่/ โครงสร้าง	**คำนิยาม/คำอธิบาย**
หัวหน้าด้านสถาปัตยกรรมระบบ	เจ้าหน้าที่อาวุโสที่รับผิดชอบในผลงานของกระบวนการด้านสถาปัตยกรรมระบบขององค์กร
หัวหน้าด้านพัฒนาระบบ	เจ้าหน้าที่อาวุโสที่รับผิดชอบในผลงานสำหรับกระบวนการพัฒนาการแก้ไขปัญหาแบบเบ็ดเสร็จด้านไอที
หัวหน้าด้านปฏิบัติการไอที	เจ้าหน้าที่อาวุโสที่รับผิดชอบในผลงานด้านสภาพแวดล้อมและโครงสร้างพื้นฐานของปฏิบัติการด้านไอที
หัวหน้าด้านการบริหารหน่วยงานไอที	เจ้าหน้าที่อาวุโสที่รับผิดชอบในผลงานด้านระเบียนที่เกี่ยวข้องกับไอที และรับผิดชอบในการสนับสนุนการบริหารกิจกรรมต่างๆ ที่เกี่ยวข้องกับไอที
สำนักงานบริหารชุดโครงการและโครงการ (PMO)	หน้าที่งานที่รับผิดชอบในการสนับสนุนผู้จัดการชุดโครงการ (programme) และโครงการ และรวบรวม ประเมิน และรายงานสารสนเทศที่เกี่ยวข้องกับการดำเนินชุดโครงการ (programmes) และโครงการที่อยู่ภายใต้ชุดโครงการ
สำนักงานบริหารคุณค่า(VMO)	หน้าที่งานที่เสมือนเลขานุการสำหรับการบริหารกลุ่ม(portfolio) ของการลงทุนและการให้บริการ ซึ่งรวมถึงการประเมินและให้คำแนะนำเกี่ยวกับโอกาสและเหตุผลทางธุรกิจ ให้คำแนะนำเกี่ยวกับวิธีการกำกับดูแล/การบริหารจัดการคุณค่า การควบคุมคุณค่า และการรายงานความคืบหน้าของการสร้างและรักษาไว้ซึ่งคุณค่าจากการลงทุนและบริการ
Service Manager ผู้จัดการงานบริการ (ไอที)	บุคคลที่บริหารการพัฒนา การนำไปใช้งาน การประเมิน และการบริหารจัดการอย่างต่อเนื่องสำหรับผลิตภัณฑ์และบริการใหม่หรือที่มีอยู่เดิม สำหรับลูกค้า (ผู้ใช้) หรือกลุ่มของลูกค้า (ผู้ใช้)
ผู้จัดการด้านความมั่นคงปลอดภัยสารสนเทศ	บุคคลที่บริหาร ออกแบบ ดูแล และ/หรือประเมินความมั่นคงปลอดภัยของสารสนเทศในองค์กร
ผู้จัดการด้านความต่อเนื่องในการดำเนินธุรกิจ	บุคคลที่บริหาร ออกแบบ ดูแล และ/หรือประเมินความสามารถในการดำเนินธุรกิจต่อเนื่องขององค์กร เพื่อให้ความมั่นใจว่า องค์กรยังคงสามารถปฏิบัติหน้าที่งานที่สำคัญได้อย่างต่อเนื่องภายหลังเกิดเหตุการณ์หยุดชะงักของระบบ
เจ้าหน้าที่ด้านการรักษาความเป็นส่วนบุคคล	บุคคลที่รับผิดชอบในการเฝ้าติดตามความเสี่ยงและผลกระทบต่อธุรกิจจากกฎหมายข้อมูลส่วนบุคคล (privacy laws) และให้แนวทางและความร่วมมือในการนำนโยบายและกิจกรรมต่างๆ ไปใช้งาน เพื่อให้เกิดความมั่นใจว่าได้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ตำแหน่งนี้อาจจะเรียกอีกชื่อหนึ่งว่า เจ้าหน้าที่คุ้มครองข้อมูล (data protection officer)

หน้านี้เป็นหน้าว่าง

ปัจจัยเอื้อใน COBIT 5: วัฒนธรรม จริยธรรม และพฤติกรรม

วัฒนธรรม จริยธรรม และพฤติกรรม หมายถึงกลุ่มของพฤติกรรมอย่างใดอย่างหนึ่งหรือหลายอย่างรวมกันภายในองค์กร ข้อมูลรายละเอียดเฉพาะของปัจจัยเอื้อด้านวัฒนธรรม จริยธรรม และพฤติกรรม เปรียบเทียบกับคำอธิบายปัจจัยเอื้อทั่วไปได้แสดงไว้ใน**รูปภาพที่ 34**

รูปภาพที่ 34—ปัจจัยเอื้อใน COBIT 5: วัฒนธรรม จริยธรรม และพฤติกรรม

รูปแบบของวัฒนธรรม จริยธรรม และพฤติกรรมแสดงถึง

- **ผู้มีส่วนได้เสีย**—ผู้มีส่วนได้เสียที่เกี่ยวข้องกับวัฒนธรรม จริยธรรม และพฤติกรรมอาจอยู่ภายในหรือภายนอกองค์กรก็ได้ ผู้มีส่วนได้เสียภายในรวมถึงหน่วยงานทั้งหมดในองค์กร ผู้มีส่วนได้เสียภายนอกรวมถึงผู้กำกับดูแล เช่น ผู้ตรวจสอบภายนอกหรือหน่วยงานที่ควบคุมดูแล (supervisory bodies) ส่วนได้เสียมี 2 ด้าน: ผู้มีส่วนได้เสียบางคน เช่น เจ้าหน้าที่ด้านกฎหมาย ผู้จัดการด้านความเสี่ยง ผู้จัดการด้านทรัพยากรบุคคล คณะกรรมการกำหนดค่าจ้าง (remuneration board) และเจ้าหน้าที่อื่นๆ เป็นผู้ซึ่งมีหน้าที่กำหนด นำไปใช้ และบังคับใช้ให้เกิดพฤติกรรมที่ต้องการ ส่วนที่เหลือเป็นผู้ที่ต้องปฏิบัติตนให้เป็นไปตามกฎและบรรทัดฐาน
- **เป้าหมาย**—เป้าหมายของปัจจัยเอื้อด้านวัฒนธรรม จริยธรรม และพฤติกรรมเกี่ยวข้องกับ
  - จริยธรรมองค์กร ซึ่งกำหนดโดยคุณค่าที่องค์กรต้องการ
  - จริยธรรมบุคคล กำหนดโดยค่านิยมของแต่ละบุคคลในองค์กร และขึ้นอยู่กับระดับความสำคัญของปัจจัยภายนอก เช่น ศาสนา เชื้อชาติ พื้นฐานทางเศรษฐกิจและสังคม พื้นฐานทางภูมิศาสตร์ และประสบการณ์ส่วนบุคคล
  - พฤติกรรมบุคคล ซึ่งเมื่อรวมกันแล้วจะเป็นเป็นสิ่งที่กำหนดวัฒนธรรมขององค์กร ปัจจัยหลายๆ อย่าง เช่น ปัจจัยภายนอกที่กล่าวถึงข้างต้น รวมถึงความสัมพันธ์ระหว่างบุคคลในองค์กร วัตถุประสงค์และความทะเยอทะยานของบุคคล ล้วนผลักดันให้เกิดพฤติกรรมส่วนบุคคล ประเภทของพฤติกรรมที่เกี่ยวข้องภายใต้บริบทนี้รวมถึง:
    - พฤติกรรมการยอมรับความเสี่ยง—ความเสี่ยงเท่าใดที่องค์กรสามารถยอมรับได้ และความเสี่ยงอะไรที่องค์กรเต็มใจที่จะยอมรับ
    - พฤติกรรมการปฏิบัติตามนโยบาย—บุคคลสามารถยอมรับและ/หรือปฏิบัติตามนโยบายได้มากน้อยเพียงใด
    - พฤติกรรมที่มีต่อผลลัพธ์ในด้านลบ—องค์กรรับมือกับผลลัพธ์ในด้านลบอย่างไร ได้แก่ เหตุการณ์ที่ก่อให้เกิดความสูญเสียหรือการพลาดโอกาส องค์กรได้เรียนรู้จากสิ่งผิดพลาดเหล่านั้นและพยายามปรับปรุงหรือไม่ หรือจะกล่าวโทษโดยไม่แก้ที่ต้นเหตุของปัญหา
- **วัฏจักร**—วัฒนธรรมองค์กร จุดยืนทางจริยธรรม และพฤติกรรมบุคคล ต่างก็มีวัฏจักร เริ่มต้นจากวัฒนธรรมที่มีอยู่ องค์กรสามารถระบุการเปลี่ยนแปลงที่ต้องการและดำเนินการไปสู่การนำการเปลี่ยนแปลงดังกล่าวไปใช้ มีเครื่องมือหลายอย่าง—ดังที่อธิบายไว้ในแนวปฏิบัติที่ดี—ที่สามารถนำมาใช้ได้
- **แนวปฏิบัติที่ดี**—แนวปฏิบัติที่ดีสำหรับการทำให้เกิดการสนับสนุนผลักดัน และการรักษาไว้ซึ่งพฤติกรรมที่พึงปรารถนาทั่วทั้งองค์กร ประกอบด้วย
  - การสื่อสารทั่วทั้งองค์กรเกี่ยวกับพฤติกรรมที่พึงปรารถนาและพื้นฐานคุณค่าขององค์กร
  - การทำให้ตระหนักถึงพฤติกรรมที่ปรารถนา เสริมด้วยการที่ผู้บริหารระดับสูงและผู้ที่เป็นแชมเปี้ยนปฏิบัติเป็นแบบอย่าง
  - ผลตอบแทนที่สนับสนุนและยับยั้งเพื่อทำให้เกิดพฤติกรรมที่พึงปรารถนา โดยมีความเชื่อมโยงที่ชัดเจนระหว่างพฤติกรรม บุคคลกับแบบแผนการให้รางวัลตามที่หน่วยงานทรัพยากรบุคคลขององค์กรกำหนดขึ้นมา
  - กฎและบรรทัดฐาน ซึ่งให้แนวทางเพิ่มเติมสำหรับพฤติกรรมองค์กรที่พึงปรารถนา โดยเชื่อมโยงอย่างชัดเจนมากกับหลักการและนโยบายที่องค์กรกำหนดขึ้น

- **ความสัมพันธ์กับปัจจัยเอื้ออื่นๆ**—ความเชื่อมโยงกับปัจจัยเอื้ออื่นๆ รวมถึง
  - เราสามารถออกแบบกระบวนการให้สมบูรณ์แบบได้ แต่ถ้าผู้มีส่วนได้เสียของกระบวนการไม่ต้องการปฏิบัติตามกิจกรรมต่างๆ ของกระบวนการตามที่ออกแบบไว้—กล่าวคือ ถ้าพวกเขามีพฤติกรรมไม่ปฏิบัติตามในทางใดทางหนึ่ง—ก็จะไม่สามารถบรรลุผลลัพธ์จากกระบวนการได้
  - เช่นเดียวกัน โครงสร้างการจัดองค์กรอาจออกแบบและจัดตั้งขึ้นตามตำรา แต่การตัดสินใจไม่ได้รับการนำไปใช้งาน—ด้วยเหตุผลส่วนบุคคล ขาดผลตอบแทนที่จูงใจ หรืออื่นๆ —ย่อมไม่ก่อให้เกิดการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่ดี
  - หลักการและนโยบาย เป็นกลไกในการสื่อสารที่สำคัญเกี่ยวกับคุณค่าและพฤติกรรมที่พึงปรารถนาขององค์กร

ตัวอย่างที่ 11—การปรับปรุงคุณภาพ

องค์กรเผชิญหน้ากับปัญหาหนักเกี่ยวกับคุณภาพของระบบงานใหม่ซ้ำแล้วซ้ำเล่า แม้ว่าองค์กรจะมีระเบียบวิธีในการพัฒนาซอฟแวร์ที่ดีแล้วก็ตาม แต่บ่อยครั้งที่ปัญหาด้านซอฟแวร์ทำให้เกิดปัญหาในการดำเนินธุรกิจประจำวัน

จากการสืบสวนพบว่า การประเมินผลงานและการให้ผลตอบแทนแก่เจ้าหน้าที่และผู้บริหารในทีมพัฒนาระบบตั้งอยู่บนพื้นฐานของการส่งมอบงานให้ทันเวลา ภายใต้งบประมาณที่มีอยู่ของโครงการ พวกเขาไม่ได้ถูกวัดด้วยเกณฑ์ด้านคุณภาพหรือเกณฑ์ผลประโยชน์ทางธุรกิจ ส่งผลให้พวกเขาเน้นแค่เพียงการส่งมอบงานให้ทันเวลาและการลดต้นทุนในการพัฒนาระบบเท่านั้น เช่น ลดเวลาในการทดสอบ การสืบสวนยังแสดงให้เห็นด้วยว่าไม่มีการปฏิบัติตามระเบียบวิธีและขั้นตอนการปฏิบัติงานที่กำหนดไว้ เพื่อลดเวลาที่ต้องใช้ในการพัฒนาระบบ (แลกกับคุณภาพ) นอกจากนี้ โครงสร้างการจัดองค์กรยังได้กำหนดให้การมีส่วนร่วมของทีมพัฒนาระบบจะหยุดการมีส่วนร่วมทันทีเมื่อระบบที่พัฒนานั้นได้ส่งมอบให้กับทีมปฏิบัติการแล้ว หลังจากนั้นการมีส่วนร่วมของทีมพัฒนาระบบจะเป็นลักษณะทางอ้อม (indirect) ผ่านทางกระบวนการบริหารจัดการเหตุการณ์ผิดปกติ (incident management) และกระบวนการบริหารจัดการปัญหา (problem management) ที่มีอยู่เท่านั้น

บทเรียนที่ได้รับคือจะต้องใช้ผลตอบแทนเพื่อจูงใจที่ดีกว่านี้สำหรับเจ้าหน้าที่และผู้บริหารในทีมพัฒนาระบบ เพื่อส่งเสริมให้งานมีคุณภาพ

ตัวอย่างที่ 12—ความเสี่ยงที่เกี่ยวข้องกับไอที

สิ่งที่บ่งบอกบางอย่างที่ส่อถึงวัฒนธรรมที่ไม่เหมาะสมหรือมีปัญหาด้านวัฒนธรรมที่เกี่ยวข้องกับความเสี่ยงด้านไอที ได้แก่

- ความไม่สอดคล้องระหว่างการยอมรับความเสี่ยง (risk appetite) ที่แท้จริงกับที่นำมาแปลงเป็นนโยบาย ค่านิยมที่แท้จริงของผู้บริหารในเรื่องของความเสี่ยงอาจได้แก่ กล้าได้กล้าเสียพอสมควรและชอบความเสี่ยง ในขณะที่นโยบายที่กำหนดขึ้นใช้จริงกลับสะท้อนถึงทัศนคติเชิงอนุรักษ์มากกว่า ดังนั้น จึงมีความไม่สอดคล้องกันระหว่างค่านิยมกับวิธีการที่จะบรรลุถึงค่านิยมดังกล่าว จึงนำไปสู่ความขัดแย้งอย่างหลีกเลี่ยงไม่ได้ ความขัดแย้งอาจเกิดขึ้นได้ เช่น ความขัดแย้งกันระหว่างผลตอบแทนเพื่อจูงใจที่ให้กับผู้บริหารกับการบังคับใช้นโยบายที่ไม่สอดคล้องกัน
- วัฒนธรรมการกล่าวโทษ (Blame culture) ที่มีอยู่ วัฒนธรรมประเภทนี้ควรหลีกเลี่ยงเพราะเป็นการปิดกั้นความมีประสิทธิผลของการสื่อสาร ในวัฒนธรรมการกล่าวโทษนี้ เมื่อโครงการไม่สามารถส่งมอบงานได้ตามเวลาที่กำหนดหรือไม่ตรงกับสิ่งที่คาดหวัง หน่วยงานธุรกิจมักจะกล่าวโทษไปที่หน่วยงานไอทีโดยไม่ทันได้ตระหนักว่าการมีส่วนร่วมของหน่วยงานธุรกิจตั้งแต่ต้นจะช่วยส่งผลให้โครงการประสบความสำเร็จได้ ในกรณีที่รุนแรงที่สุด หน่วยงานธุรกิจอาจจะกล่าวโทษในเรื่องความล้มเหลวที่จะเป็นไปตามความคาดหวังไปที่หน่วยงานไอที ทั้งที่หน่วยงานไอทีอาจไม่เคยไม่ได้รับการสื่อสารความคาดหวังอย่างชัดเจนเลย การกล่าวโทษกันเช่นนี้ไม่เพียงแต่ทำลายการสื่อสารที่มีประสิทธิผลระหว่างหน่วยงานเท่านั้น แต่ยังเป็นสาเหตุให้เกิดความล่าช้าอีกด้วย ผู้บริหารระดับสูงในฐานะของผู้นำต้องระบุและควบคุมวัฒนธรรมการกล่าวโทษนี้ให้ได้อย่างรวดเร็วหากต้องการให้เกิดความร่วมมือกันทั่วทั้งองค์กร

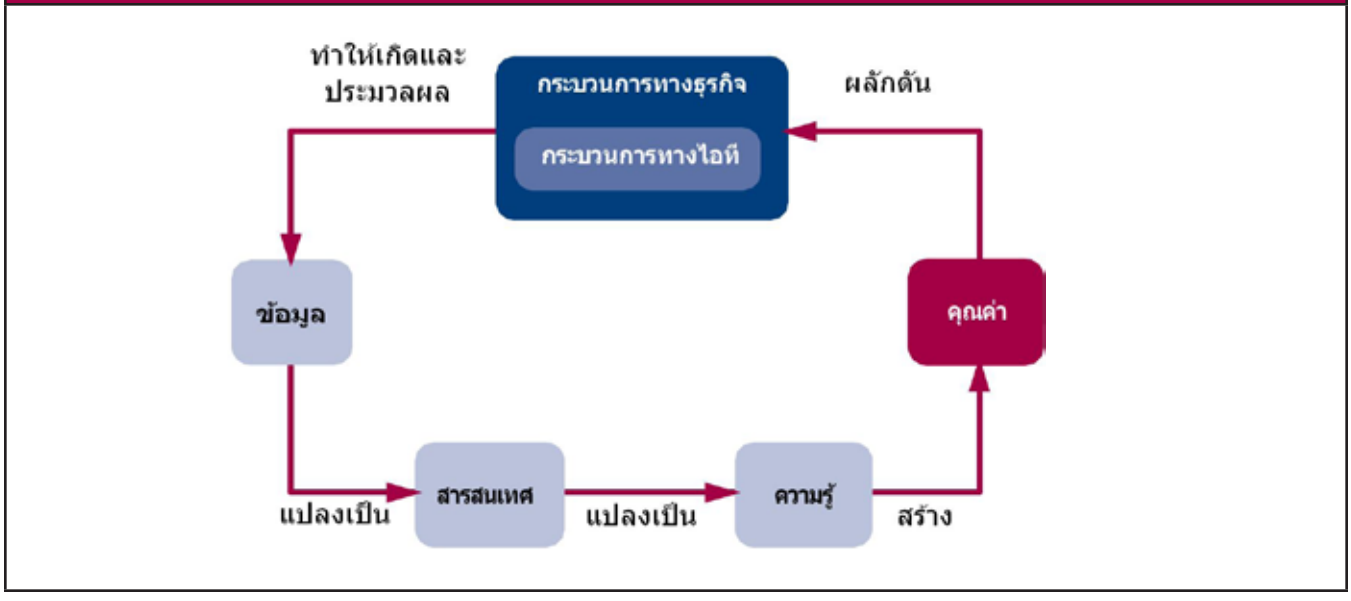
ปัจจัยเอื้อใน COBIT 5: สารสนเทศ

บทนำ—วัฏจักรของสารสนเทศ

ปัจจัยเอื้อด้านสารสนเทศใช้กับสารสนเทศทั้งหมดที่เกี่ยวข้องกับองค์กร ไม่เฉพาะแต่สารสนเทศที่เป็นอัตโนมัติเท่านั้น (automated information) อาจเป็นสารสนเทศแบบมีโครงสร้างหรือไม่มีโครงสร้าง เป็นแบบทางการหรือไม่เป็นทางการก็ได้

สารสนเทศอาจพิจารณาได้ว่าเป็นขั้นตอนหนึ่งใน 'วัฏจักรของสารสนเทศ' ขององค์กร ในวัฏจักรของสารสนเทศ (**รูปภาพที่ 35**) กระบวนการทางธุรกิจทำให้เกิดและประมวลผลข้อมูล แปลงข้อมูลให้เป็นสารสนเทศและความรู้ และท้ายสุดสร้างคุณค่าให้กับองค์กร ขอบเขตของปัจจัยเอื้อด้านสารสนเทศโดยหลักแล้วจะเกี่ยวข้องกับระยะที่เป็น 'สารสนเทศ' ในวัฏจักรของสารสนเทศ แต่ COBIT 5 ก็ได้ครอบคลุมถึงมุมมองในด้านข้อมูลและความรู้ด้วย

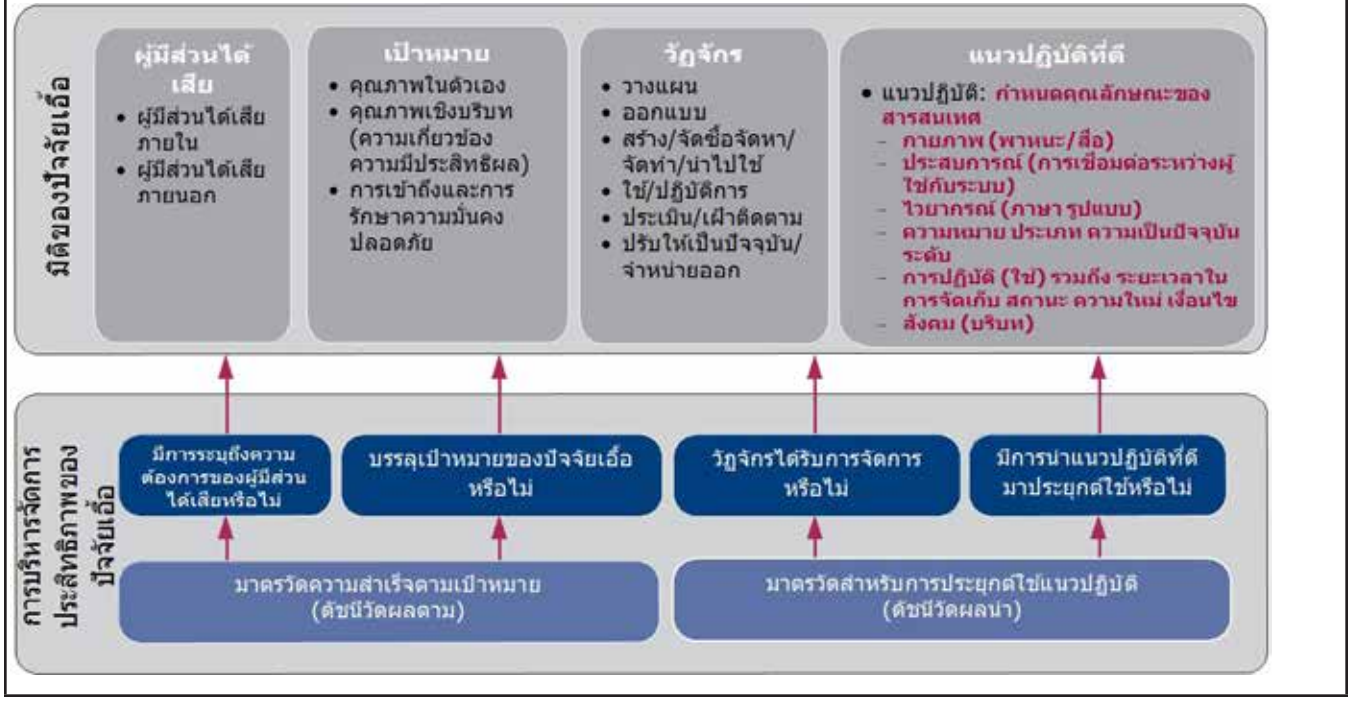
รูปภาพที่ 35—ข้อมูลคำนิยามของข้อมูลใน COBIT 5—วัฏจักรของสารสนเทศ



ปัจจัยเอื้อด้านสารสนเทศใน COBIT 5

ข้อมูลรายละเอียดเฉพาะของปัจจัยเอื้อด้านสารสนเทศ เปรียบเทียบกับคำอธิบายปัจจัยเอื้อทั่วไป แสดงไว้ใน**รูปภาพที่ 36**

รูปภาพที่ 36—ปัจจัยเอื้อใน COBIT 5: สารสนเทศ



ต้นแบบสารสนเทศ (Information Model) แสดงถึง

- **ผู้มีส่วนได้เสีย**—อาจจะมาจากภายในหรือภายนอกองค์กรก็ได้ รูปแบบทั่วไป (generic model) แนะนำด้วยว่า นอกจากการระบุถึงผู้มีส่วนได้เสียแล้ว ยังต้องกำหนดส่วนได้เสียของผู้มีส่วนได้เสียด้วย กล่าวคือ ทำไมพวกเขาต้องให้ความสนใจในสารสนเทศ

  สำหรับผู้มีส่วนได้เสียของสารสนเทศเป็นใครได้บ้างนั้น อาจเป็นไปได้ที่จะจัดกลุ่มของบทบาทหน้าที่ในการจัดการกับสารสนเทศที่แตกต่างกันไป เริ่มตั้งแต่ข้อเสนอที่ให้จัดกลุ่มอย่างละเอียด–เช่นที่แนะนำให้ใช้ข้อมูลหรือสารสนเทศที่เฉพาะเจาะจงสำหรับแต่ละบทบาทหน้าที่ เช่น สถาปนิก เจ้าของ ผู้บริการ (steward) ผู้ดูแลทรัพย์สิน/ผลประโยชน์ (trustee) ผู้ขาย ผู้รับผลประโยชน์ ผู้จัดการด้านคุณภาพ ผู้จัดการด้านการรักษาความมั่นคงปลอดภัย–ไปจนถึงข้อเสนอที่ให้จัดกลุ่มอย่างกว้างๆ –เช่น การแยกออกเป็นผู้สร้างสารสนเทศ ผู้เก็บรักษาสารสนเทศ และผู้บริโภคสารสนเทศ:
  – ผู้สร้างสารสนเทศ (information producer) มีหน้าที่ในการทำให้มีสารสนเทศเกิดขึ้น
  – ผู้เก็บรักษาสารสนเทศ (information custodian) มีหน้าที่ในการจัดเก็บและดูแลสารสนเทศ
  – ผู้บริโภคสารสนเทศ (information consumer) มีหน้าที่ในการใช้สารสนเทศ
  การจัดกลุ่มเหล่านี้ อิงกับกิจกรรมที่เกี่ยวข้องกับแหล่งที่มาของข้อมูล กิจกรรมขึ้นอยู่กับระยะ (phase) ในวัฏจักรของสารสนเทศ ดังนั้น เราสามารถนำมิติต่างๆ ในวัฏจักรของสารสนเทศตามที่ระบุไว้ในต้นแบบสารสนเทศมาใช้เพื่อให้ทราบได้ว่ากลุ่มบทบาทใดมีระดับของความละเอียดที่เหมาะสมกับต้นแบบสารสนเทศนั้น ซึ่งหมายความว่า บทบาทของผู้มีส่วนได้เสียด้านสารสนเทศสามารถระบุเป็นระยะในวัฏจักรของสารสนเทศ เช่น ผู้วางแผนด้านสารสนเทศ ผู้รับสารสนเทศ ผู้ใช้สารสนเทศ ในขณะเดียวกัน ก็หมายความว่ามิติของผู้มีส่วนได้เสียด้านสารสนเทศไม่ใช่มิติที่เป็นเอกเทศระยะต่างๆ ในวัฏจักรย่อมมีผู้มีส่วนได้เสียที่แตกต่างกันไป

  ในขณะที่บทบาทหน้าที่ที่เกี่ยวข้องขึ้นอยู่กับระยะต่างๆ ในวัฏจักรของสารสนเทศ ส่วนได้เสียสามารถเชื่อมโยงได้กับเป้าหมายของสารสนเทศ
- **เป้าหมาย**— เป้าหมายของสารสนเทศ แบ่งออกเป็น 3 มิติเชิงคุณภาพดังนี้
  คุณภาพในตัวเอง (Intrinsic quality)—ค่าของข้อมูลสอดคล้องกับค่าที่แท้จริงหรือค่าที่ถูกต้องเพียงใด รวมถึง
  – ความถูกต้อง—สารสนเทศมีความถูกต้องและเชื่อถือได้เพียงใด
  – ความเที่ยงตรง (Objectivity)—สารสนเทศมีความเป็นกลาง ไม่มีการบิดเบือน ไม่เอนเอียงเพียงใด
  – ความน่าเชื่อถือ (Believability)—สารสนเทศถือได้ว่ามีความถูกต้องและน่าเชื่อถือเพียงใด
  – ชื่อเสียง (Reputation)—สารสนเทศมาจากแหล่งข้อมูลหรือเนื้อหาที่น่าเชื่อถือได้มากน้อยเพียงใด
  คุณภาพเชิงบริบทและการนำเสนอ—สารสนเทศสามารถนำมาประยุกต์ใช้ในภารกิจของผู้ใช้สารสนเทศและนำเสนอในรูปแบบที่เข้าใจได้ง่ายและชัดเจนเพียงใด คุณภาพของสารสนเทศนั้นขึ้นอยู่กับบริบทของการใช้ ซึ่งรวมถึง
  – ความเกี่ยวเนื่อง (Relevancy)—สารสนเทศสามารถนำมาประยุกต์ใช้และเป็นประโยชน์ในภารกิจที่กำลังทำอยู่เพียงใด
  – ความครบถ้วน (Completeness)—สารสนเทศไม่ขาดหายและมีความลึกและกว้างเพียงพอสำหรับภารกิจที่กำลังทำอยู่เพียงใด
  – ความเป็นปัจจุบัน—สารสนเทศเป็นปัจจุบันอย่างเพียงพอต่อภารกิจที่กำลังทำอยู่เพียงใด
  – ปริมาณสารสนเทศที่เหมาะสม (Appropriate amount of information)—ปริมาณสารสนเทศเพียงพอสำหรับภารกิจที่กำลังทำอยู่เพียงใด
  – การนำเสนอที่สั้นกระชับ (Concise representation)—สารสนเทศนำเสนอด้วยความกระชับเพียงใด
  – การนำเสนอที่มีความสอดคล้องกัน (Consistent representation)—สารสนเทศนำเสนอในรูปแบบที่เหมือนกันเพียงใด
  – ความสามารถในการตีความ (Interpretability)—สารสนเทศใช้ภาษา สัญลักษณ์ และหน่วยนับที่เหมาะสม ด้วยนิยามที่ชัดเจนเพียงใด
  – ความเข้าใจได้—สารสนเทศทำความเข้าใจได้ง่ายเพียงใด
  – ความง่ายต่อการจัดดำเนินการ (manipulation)—สารสนเทศสามารถจัดดำเนินการและนำไปประยุกต์ใช้กับภารกิจต่างๆ ได้ง่ายมากน้อยเพียงใด
  คุณภาพด้านความมั่นคงปลอดภัยและการเข้าถึง (Security/accessibility quality)—สารสนเทศพร้อมใช้งานและสามารถได้รับมา (obtainable) เพียงใด ซึ่งรวมถึง
  – ความพร้อมใช้/และทันเวลา—สารสนเทศพร้อมใช้งานเมื่อต้องการ หรือเรียกใช้ได้ง่ายและรวดเร็วเพียงใด
  – การจำกัดการเข้าถึง—มีการจำกัดการเข้าถึงสารสนเทศให้เฉพาะกับผู้ที่ได้รับอนุญาตอย่างเหมาะสมเพียงใด

  ในภาคผนวก F ได้ให้รายละเอียดการเปรียบเทียบเกณฑ์ด้านคุณภาพของสารสนเทศใน COBIT 5 กับ COBIT 4.1 ยกตัวอย่างเช่น ความถูกต้องสมบูรณ์ (integrity) (ตามที่ระบุไว้ใน COBIT 4.1) อยู่ภายใต้เป้าหมายของสารสนเทศด้านความครบถ้วนและถูกต้อง (completeness and accuracy)
- **วัฏจักร**—ต้องพิจารณาถึงวัฏจักรของสารสนเทศอย่างครบวงจร และอาจจำเป็นต้องใช้วิธีปฏิบัติที่แตกต่างกันสำหรับสารสนเทศในแต่ละระยะของวัฏจักร ปัจจัยเอื้อด้านสารสนเทศใน COBIT 5 สามารถแบ่งออกเป็นระยะต่างๆ ได้ดังนี้
  – **วางแผน**— ระยะนี้ เป็นการเตรียมการสำหรับการจัดทำและใช้ข้อมูล กิจกรรมในระยะนี้อาจรวมถึงการกำหนดวัตถุประสงค์ การวางแผนสถาปัตยกรรมข้อมูล และการพัฒนามาตรฐานและคำนิยามต่างๆ ยกตัวอย่างเช่น คำนิยามของข้อมูล ขั้นตอนการปฏิบัติงานในการเก็บรวบรวมข้อมูล
  – **การออกแบบ**
  – **จัดทำ/จัดหา**—กิจกรรมของระยะนี้ อาจรวมถึงการจัดทำระเบียนข้อมูล (data record) การซื้อข้อมูล และการถ่ายโอนข้อมูลจากแฟ้มข้อมูลภายนอกเข้าสู่ระบบ

– **ใช้/ปฏิบัติการ ประกอบด้วย**
  • การจัดเก็บ—ในระยะนี้ สารสนเทศจะถูกจัดเก็บในรูปแบบของอิเล็กทรอนิกส์ หรือบนกระดาษ (หรือแม้แต่ในความทรงจำของบุคคล) กิจกรรมในระยะนี้อาจเกี่ยวข้องกับการจัดเก็บสารสนเทศในรูปแบบอิเล็กทรอนิก (เช่น แฟ้มข้อมูล ฐานข้อมูล คลังข้อมูล ที่เป็นอิเล็กทรอนิก) หรือบนกระดาษ (เช่น เอกสารที่เป็นกระดาษ)
  • แบ่งปัน—ในระยะนี้ สารสนเทศพร้อมที่เรียกใช้งานผ่านวิธีการในการแจกจ่ายข้อมูล กิจกรรมในช่วงนี้อาจรวมถึงกระบวนการในการนำสารสนเทศไปไว้ในที่ที่สามารถเข้าถึงและใช้งานได้ เช่น การแจกจ่ายเอกสารผ่านทางจดหมายอิเล็กทรอนิกส์ สำหรับสารสนเทศที่อยู่ในรูปแบบอิเล็กทรอนิก วัฏจักรในระยะนี้ส่วนใหญ่อาจทับซ้อนกับระยะของการจัดเก็บ เช่น การแบ่งปันข้อมูลผ่านทางการเข้าถึงฐานข้อมูลและเครื่องแม่ข่ายสำหรับแฟ้มข้อมูล/เอกสาร
  • ใช้—เป็นระยะที่ใช้สารสนเทศเพื่อให้บรรลุเป้าหมายที่ตั้งไว้ กิจกรรมในระยะนี้อาจรวมถึงการใช้งานสารสนเทศในทุกรูปแบบ (เช่น การตัดสินใจเชิงบริหาร การดำเนินกระบวนการที่เป็นอัตโนมัติ) และอาจรวมถึงกิจกรรมเช่น การเรียกและแปลงสารสนเทศจากรูปแบบหนึ่งไปเป็นอีกรูปแบบหนึ่งด้วย

จากมุมมองในหนังสือ Taking Governance Forward สารสนเทศเป็นปัจจัยเอื้อสำหรับการกำกับดูแลองค์กร ดังนั้น การใช้สารสนเทศตามที่ระบุไว้ในต้นแบบสารสนเทศนี้ อาจถือได้ว่าเป็นการใช้ด้วยจุดประสงค์เช่นเดียวกับการที่ผู้มีส่วนได้เสียด้านการกำกับดูแลจำเป็นต้องใช้สารสนเทศเพื่อปฏิบัติหน้าที่ ดำเนินกิจกรรมต่างๆ และมีปฏิสัมพันธ์ต่อกัน.

บทบาทหน้าที่ กิจกรรม และความสัมพันธ์เหล่านี้ได้นำมาแสดงไว้ใน**รูปภาพที่ 8** ปฏิสัมพันธ์ระหว่างผู้มีส่วนได้เสียจำเป็นต้องมีการไหลของสารสนเทศ (information flow) ซึ่งมีจุดประสงค์ตามที่ระบุไว้ในแบบแผน: เรื่องความรับผิดชอบในผลของงาน เรื่องการมอบอำนาจ เรื่องการเฝ้าติดตาม เรื่องการกำหนดทิศทาง เรื่องความสอดคล้องกัน เรื่องการปฏิบัติงาน และเรื่องการควบคุม
– การเฝ้าติดตาม—เป็นระยะที่ให้ความมั่นใจว่า ทรัพยากรด้านสารสนเทศยังคงสามารถทำงานได้อย่างถูกต้อง กล่าวคือ ยังคงทำประโยชน์ได้ กิจกรรมในระยะนี้อาจรวมถึงการเก็บรักษาสารสนเทศให้เป็นปัจจุบัน รวมทั้งกิจกรรมในการบริหารจัดการสารสนเทศอื่นๆ เช่น การทำให้ดีขึ้น การลบ การผนวกรวม และการขจัดความซ้ำซ้อนของสารสนเทศในคลังข้อมูล
– จำหน่ายออก—เป็นระยะที่ทรัพยากรด้านสารสนเทศจะถูกลบหรือทิ้งไปเมื่อไม่จำเป็นต้องใช้งานอีกต่อไป กิจกรรมในระยะนี้ อาจรวมถึงการจัดเก็บสารสนเทศที่ลบออกไปนี้ไว้ต่างหาก (archive) หรือการทำลายทิ้ง

• **แนวปฏิบัติที่ดี**—ความเข้าใจในแนวคิดของสารสนเทศอาจมีความหลากหลายแตกต่างกันไปตามสาขาวิชาต่างๆ เช่น เศรษฐศาสตร์ ทฤษฎีการสื่อสาร วิทยาศาสตร์คอมพิวเตอร์ การบริหารจัดการความรู้ และระบบสารสนเทศ ดังนั้น จึงไม่มีคำจำกัดความเกี่ยวกับสารสนเทศเพียงหนึ่งเดียวที่ตกลงใช้ร่วมกันได้ อย่างไรก็ตาม เราสามารถบอกถึงลักษณะของสารสนเทศได้ด้วยการระบุและอธิบายถึงคุณสมบัติของสารสนเทศ

แบบแผนดังต่อไปนี้ นำเสนอการจัดโครงสร้างสำหรับคุณลักษณะที่แตกต่างกันของสารสนเทศ ซึ่งประกอบด้วยการระบุถึงคุณลักษณะของสารสนเทศ 6 ระดับหรือชั้นพร้อมกับคำอธิบาย ระดับทั้ง 6 นี้แสดงถึงคุณลักษณะที่เชื่อมต่อกัน เริ่มตั้งแต่ในโลกกายภาพของสารสนเทศซึ่งคุณลักษณะจะเชื่อมโยงกับเทคโนโลยีและสื่อทางเทคโนโลยีเพื่อการเก็บรวมรวบ เก็บรักษา ประมวลผล แจกจ่าย และนำเสนอสารสนเทศ ไปจนถึงในโลกของสังคมที่มีการใช้สารสนเทศ ทำความเข้าใจ และกระทำการ

ชั้นและคุณลักษณะของสารสนเทศสามารถอธิบายได้ดังต่อไปนี้
• **ชั้นของโลกทางกายภาพ (Physical world layer)**—คือโลกที่ปรากฏการณ์ทั้งหมดซึ่งสามารถสังเกตเห็นได้จริงเกิดขึ้น
–พาหนะ/สื่อของสารสนเทศ—คุณลักษณะที่ระบุถึง พาหนะหรือสื่อทางกายภาพของสารสนเทศ ยกตัวอย่างเช่น กระดาษ สัญญาณไฟฟ้า คลื่นเสียง
• **ชั้นของประสบการณ์ (Empiric layer)**—การสังเกตการณ์เชิงประจักษ์ (empirical observation) ถึงสัญญาณที่ใช้ในการเข้ารหัสสารสนเทศ และความแตกต่างระหว่างกัน ตลอดจนความแตกต่างจากคลื่นรบกวน
– ช่องทางในการเข้าถึงสารสนเทศ—คุณลักษณะที่ระบุถึงช่องทางการเข้าถึงสารสนเทศ ยกตัวอย่างเช่น การเชื่อมต่อระหว่างผู้ใช้กับระบบ (user interfaces)
• **ชั้นของไวยกรณ์ (Syntactic layer)** —กฎและหลักการสำหรับการสร้างประโยคตามภาษาธรรมชาติและภาษาประดิษฐ์ (artificial language) ไวยกรณ์ (syntax) ในที่นี้หมายถึงรูปแบบของสารสนเทศ
– รหัส/ภาษา—คุณลักษณะที่ระบุถึงการแสดงภาษา/รูปแบบที่ใช้ในการเข้ารหัสสารสนเทศและกฎในการรวบรวมสัญลักษณ์ต่างๆ ของภาษาเพื่อให้จัดทำเป็นโครงสร้างของไวยกรณ์
• **ชั้นของความหมาย (Semantic layer)**—กฎและหลักการสำหรับการสร้างความหมายจากโครงสร้างของไวยกรณ์ ความหมาย (Semantic) ในที่นี้ ได้แก่ความหมายของสารสนเทศ
– ประเภทของสารสนเทศ—คุณลักษณะที่ระบุถึงชนิดของสารสนเทศ ได้แก่ สารสนเทศด้านการเงินและสารสนเทศที่ไม่ใช่ด้านการเงิน สารสนเทศที่มาจากภายในและสารสนเทศที่มาจากภายนอก ค่าจากการประมาณการ/คาดการณ์และค่าจากการสังเกต ค่าที่ได้จาการวางแผนและค่าที่เกิดขึ้นจริง
– ความเป็นปัจจุบันของสารสนเทศ—คุณลักษณะที่ระบุถึงช่วงเวลาในการอ้างถึงสารสนเทศ ได้แก่ สารสนเทศในอดีต ในปัจจุบัน และในอนาคต
– ระดับของสารสนเทศ—คุณลักษณะที่ระบุถึงระดับรายละเอียดของสารสนเทศ ยกตัวอย่าเช่น ยอดขายต่อปี ต่อไตรมาศ ต่อเดือน

- **ชั้นของการปฏิบัติ (Pragmatic layer)** —กฎและโครงสร้างที่ใช้สร้างโครงสร้างที่ใหญ่ขึ้นด้านภาษา เพื่อให้บรรลุถึงจุดประสงค์อย่างใดอย่างหนึ่งในการสื่อสารของมนุษย์ การปฏิบัติ (pragmatic) ในที่นี้หมายถึงการใช้สารสนเทศ
  - ระยะเวลาในการจัดเก็บ (Retention period) —คุณลักษณะที่ระบุว่า สารสนเทศจะจัดเก็บไว้นานเพียงใดก่อนจะถูกทำลายทิ้ง
  - สถานะของสารสนเทศ—คุณลักษณะที่ระบุว่าสารสนเทศใดเป็นสารสนเทศที่ใช้งานอยู่ หรือเป็นสารสนเทศในอดีต
  - ความใหม่ (Novelty) —คุณลักษณะที่ระบุว่า สารสนเทศนั้นสร้างให้เกิดความรู้ใหม่ หรือยืนยันความรู้ที่มีอยู่เดิม ได้แก่ สารสนเทศกับการยืนยัน
  - ข้อแม้ (Contingency)—คุณลักษณะที่ระบุถึงสารสนเทศที่จำเป็นต้องมีมาก่อนที่จะเกิดสารสนเทศนี้ (เพื่อให้ข้อมูลนี้ได้รับการพิจารณาว่าเป็นสารสนเทศ)
- **ชั้นของโลกทางสังคม (Social world layer)**— โลกที่สร้างขึ้นทางสังคมจากการใช้โครงสร้างด้านภาษาที่ระดับของการปฏิบัติด้านศาสตร์ในการใช้สัญลักษณ์และภาษา (semiotic) เช่น สัญญา กฎหมาย วัฒนธรรม
  - บริบท (Context) —คุณลักษณะที่ระบุถึงบริบทที่ทำให้สารสนเทศมีความหมาย ใช้ มีคุณค่า และอื่นๆ เช่น บริบทของวัฒนธรรม บริบทของแต่ละโดเมน

ข้อควรพิจาณาเพิ่มเติมเกี่ยวกับสารสนเทศ— การลงทุนในสารสนเทศและเทคโนโลยีที่เกี่ยวข้องตั้งอยู่บนพื้นฐานของเหตุผลทางธุรกิจ ซึ่งรวมถึงการวิเคราะห์ต้นทุน-ผลประโยชน์ ต้นทุนและผลประโยชน์ไม่ได้หมายถึงแค่ปัจจัยที่มีตัวตนและวัดผลได้เท่านั้น แต่ยังรวมถึงปัจจัยที่ไม่มีตัวตนด้วย เช่น ความได้เปรียบในการแข่งขัน ความพึงพอใจของลูกค้า และความไม่แน่นอนของเทคโนโลยี องค์กรจะได้รับประโยชน์จากการใช้สารสนเทศก็ต่อเมื่อได้นำทรัพยากรของสารสนเทศไปใช้หรือประยุกต์ใช้ ดังนั้น คุณค่าของสารสนเทศจึงเกิดขึ้นได้จากการนำไปใช้งานเท่านั้น (ใช้ภายในองค์กรหรือขาย) สารสนเทศไม่มีคุณค่าในตัวเอง คุณค่าจะเกิดขึ้นก็ต่อเมื่อใช้สารสนเทศในกิจกรรมที่สร้างคุณค่าเท่านั้น

ต้นแบบสารสนเทศนี้ เป็นรูปแบบใหม่และมีส่วนประกอบต่างๆ มากมาย โดยจะได้รับการพัฒนาเพิ่มเติมในเอกสารฉบับแยกต่างหาก เพื่อที่ให้ง่ายต่อการเรียกใช้สำหรับผู้ใช้งาน COBIT 5 และทำให้เห็นความเกี่ยวข้องได้ชัดเจนมากขึ้นในบริบทของกรอบดำเนินการของ COBIT 5 โดยรวม ตัวอย่างที่ 13 14 และ 15 เป็นตัวอย่างของความเป็นไปได้ในการนำต้นแบบสารสนเทศไปใช้งาน

ตัวอย่างที่ 13–การใช้ต้นแบบสารสนเทศสำหรับรายละเอียดคุณสมบัติของสารสนเทศ

เมื่อพัฒนาระบบงานใหม่ เราสามารถใช้ต้นแบบสารสนเทศเพื่อช่วยในการกำหนดรายละเอียดคุณสมบัติของระบบงานและรูปแบบของสารสนเทศหรือข้อมูลที่เกี่ยวข้อง

คุณลักษณะของสารสนเทศในต้นแบบสารสนเทศสามารถใช้เพื่อกำหนดรายละเอียดคุณสมบัติสำหรับระบบงานและกระบวนการทางธุรกิจที่จะใช้สารสนเทศ

ยกตัวอย่างเช่น การออกแบบและรายละเอียดคุณสมบัติของระบบใหม่จะต้องกำหนดถึง
- ชั้นของกายภาพ—จะจัดเก็บสารสนเทศไว้ที่ไหน
- ชั้นของประสบการณ์—จะเข้าถึงสารสนเทศได้อย่างไร
- ชั้นของไวยกรณ์—สารสนเทศจะมีโครงสร้างและการเข้ารหัสอย่างไร
- ชั้นของความหมาย—สารสนเทศเป็นข้อมูลประเภทใด สารสนเทศอยู่ในระดับใด
- ชั้นของการปฏิบัติ—ต้องการเก็บสารสนเทศไว้นานเท่าใด ยังมีสารสนเทศอื่นๆ อีกหรือไม่ที่จำเป็นต้องใช้เพื่อให้สารสนเทศเป็นประโยชน์และสามารถทำงานได้

เมื่อดูที่มิติของผู้มีส่วนได้เสียร่วมกับวัฏจักรของสารสนเทศ เราสามารถระบุได้ว่าใครที่จำเป็นต้องเข้าถึงข้อมูลประเภทใดบ้างในระยะใดภายใต้วัฏจักรของสารสนเทศ

เมื่อจะทดสอบระบบงาน ผู้ทดสอบสามารถใช้เกณฑ์ด้านคุณภาพของสารสนเทศในการพัฒนาชุดของกรณีทดสอบเพื่อให้มีความครอบคลุมได้

ตัวอย่างที่ 14–การใช้ต้นแบบสารสนเทศเพื่อกำหนดความคุ้มครองที่ต้องการ

กลุ่มบุคคลที่รักษาความมั่นคงปลอดภัยภายในองค์กรจะได้ประโยชน์จากมิติด้านคุณลักษณะของต้นแบบสารสนเทศ โดยแท้จริงแล้ว การรักษาความมั่นคงปลอดภัยจะต้องพิจารณาถึง
- ชั้นของกายภาพ—จะจัดเก็บสารสนเทศไว้ที่ไหน และจัดเก็บอย่างไร
- ชั้นของประสบการณ์—จะเข้าถึงสารสนเทศได้ทางช่องทางใดได้บ้าง
- ชั้นของความหมาย—สารสนเทศเป็นข้อมูลประเภทใด สารสนเทศเป็นข้อมูลในปัจจุบัน หรือเกี่ยวข้องกับอดีตหรือนาคต
- ชั้นของการปฏิบัติ—ต้องการเก็บสารสนเทศไว้นานเท่าใด เป็นข้อมูลในอดีตหรือเป็นข้อมูลที่ใช้อยู่ในการดำเนินงาน

การใช้คุณลักษณะเหล่านี้ จะช่วยให้ผู้ใช้สามารถกำหนดระดับของการคุ้มครองและกลไกในการคุ้มครองที่ต้องการได้

ดูที่อีกมิติหนึ่งในต้นแบบสารสนเทศ ผู้ประกอบวิชาชีพด้านการรักษาความมั่นคงปลอดภัยยังสามารถพิจารณาถึงระยะในวัฏจักรของสารสนเทศได้ด้วย เพราะสารสนเทศจำเป็นต้องได้รับความคุ้มครองทุกระยะในวัฏจักรของสารสนเทศ ที่จริงแล้ว การรักษาความมั่นคงปลอดภัยเริ่มจากระยะของการวางแผนสารสนเทศ และยังหมายรวมไปถึงกลไกต่างๆในการให้ความคุ้มครองสำหรับการจัดเก็บ การแบ่งปัน และการจำหน่ายออกซึ่งสารสนเทศ ต้นแบบสารสนเทศให้ความมั่นใจว่า ข้อมูลจะได้รับความคุ้มครองตลอดวัฏจักรของสารสนเทศ

ตัวอย่างที่ 15–การใช้ต้นแบบสารสนเทศในการกำหนดความง่ายของการใช้ข้อมูล
เมื่อดำเนินการสอบทานกระบวนการทางธุรกิจ (หรือระบบงาน) ต้นแบบสารสนเทศสามารถนำมาใช้เพื่อช่วยในการสอบทานสารสนเทศที่ได้รับการประมวลผลส่งมอบโดยกระบวนการและระบบสารสนเทศต่างๆ เกณฑ์ด้านคุณภาพสามารถนำมาใช้ในการประเมินว่าสารสนเทศมีความพร้อมใช้เพียงใด—ว่าสารสนเทศครบถ้วน พร้อมใช้ในเวลาที่ต้องการ ถูกต้องตามความเป็นจริง มีความเกี่ยวเนื่อง พร้อมใช้ในปริมาณที่เหมาะสมหรือไม่เพียงใด เราอาจสามารถพิจารณาเกณฑ์การเข้าถึง (accessibility criteria) ได้ด้วย—ว่าข้อมูลสามารถเข้าถึงได้เมื่อต้องการและได้รับความคุ้มครองอย่างเหมาะสมหรือไม่ การสอบทานอาจขยายเพิ่มเติมให้รวมถึงเกณฑ์ในการแสดงผล ยกตัวอย่างเช่น สารสนเทศที่ง่ายต่อการทำความเข้าใจ ตีความ ใช้งาน และจัดดำเนินการ (manipulate) การสอบทานที่ใช้เกณฑ์ด้านคุณภาพของสารสนเทศจากต้นแบบสารสนเทศจะให้ภาพที่ครอบคลุมและครบถ้วนแก่องค์กรในเรื่องคุณภาพของสารสนเทศในปัจจุบันภายใต้กระบวนการทางธุรกิจ

หน้านี้เป็นหน้าว่าง

ปัจจัยเอื้อใน COBIT 5: บริการ โครงสร้างพื้นฐาน และระบบงาน

ความสามารถในการให้บริการ หมายถึงทรัพยากรต่างๆ เช่น ระบบงานและโครงสร้างพื้นฐาน ที่ใช้ประโยชน์สำหรับการส่งมอบบริการที่เกี่ยวข้องกับไอที

รายละเอียดเฉพาะสำหรับปัจจัยเอื้อด้านความสามารถในการให้บริการ เปรียบเทียบกับคำอธิบายสำหรับปัจจัยเอื้อทั่วไป (generic enabler) แสดงไว้ใน**รูปภาพที่ 37**

รูปแบบของบริการ โครงสร้างพื้นฐาน และระบบงาน แสดงถึง

- **ผู้มีส่วนได้เสีย**—ความสามารถในการให้บริการ (ใช้ในความหมายที่รวมถึงบริการ โครงสร้างพื้นฐาน และระบบงาน) มีผู้มีส่วนได้เสียที่อาจจะมาจากภายในหรือภายนอกก็ได้ บริการอาจจะส่งมอบโดยหน่วยงานภายในหรือภายนอกก็ได้—หน่วยงานด้านไอทีภายใน ผู้จัดการด้านปฏิบัติการ ผู้ให้บริการภายนอก ผู้ใช้บริการอาจอยู่ภายในองค์กร— ผู้ใช้งานทางธุรกิจหรืออยู่ภายนอกองค์กร—พันธมิตรทางธุรกิจ ลูกค้า ผู้ขาย ส่วนได้เสียของผู้มีส่วนได้เสียแต่ละคนจะต้องได้รับการระบุและให้ความสนใจไม่ว่าจะเป็นในเรื่องของการส่งมอบบริการที่เหมาะสม หรือการได้รับบริการที่ร้องขอจากผู้ให้บริการ
- **เป้าหมาย**—เป้าหมายของระดับความสามารถในการให้บริการ จะแสดงออกมาในแง่ของบริการ—ระบบงาน โครงสร้างพื้นฐาน เทคโนโลยี—และระดับการให้บริการ โดยพิจารณาถึงบริการและระดับการให้บริการที่ประหยัดที่สุดสำหรับองค์กร เน้นอีกครั้งว่าเป้าหมายจะต้องเกี่ยวข้องกับบริการและการให้บริการ รวมทั้งผลลัพธ์ของการให้บริการ กล่าวคือ การมีส่วนในการสนับสนุนให้กระบวนการทางธุรกิจประสบความสำเร็จ
- **วัฏจักร**—ความสามารถในการให้บริการมีวัฏจักร ความสามารถในการให้บริการในอนาคตหรือที่วางแผนไว้มักจะอธิบายไว้ใน สถาปัตยกรรมเป้าหมาย ซึ่งครอบคลุมถึงส่วนประกอบย่อย (building blocks) เช่น ระบบงานในอนาคต และรูปแบบเป้าหมายของโครงสร้างพื้นฐาน และยังอธิบายถึงความเชื่อมโยงและความสัมพันธ์ระหว่างส่วนประกอบย่อยเหล่านี้

รูปภาพที่ 37—ปัจจัยเอื้อใน COBIT 5: บริการ โครงสร้างพื้นฐาน และระบบงาน

ความสามารถในการให้บริการในปัจจุบันที่ใช้งานหรือปฏิบัติการเพื่อการส่งมอบบริการด้านไอทีได้อธิบายไว้ในสถาปัตยกรรมที่เป็นเกณฑ์พื้นฐาน (baseline architecture) ทั้งนี้ ขึ้นอยู่กับกรอบเวลาของสถาปัตยกรรมเป้าหมาย สถาปัตยกรรมในช่วงระหว่างการปรับเปลี่ยน (transition architecture) อาจต้องได้รับการกำหนดขึ้นเพื่อแสดงให้องค์กรเห็นถึงสถานะที่เป็นส่วนเพิ่มระหว่างสถาปัตยกรรมเป้าหมายกับเกณฑ์พื้นฐาน

- **แนวปฏิบัติที่ดี**—แนวปฏิบัติที่ดีสำหรับความสามารถในการให้บริการ รวมถึง
  - คำนิยามของหลักการด้านสถาปัตยกรรม—หลักการด้านสถาปัตยกรรมเป็นแนวทางในภาพรวมที่ใช้กำกับดูแลการนำไปใช้งาน และการใช้ทรัพยากรที่เกี่ยวข้องกับไอทีในองค์กร ตัวอย่างของหลักการด้านสถาปัตยกรรมประกอบด้วย
    - **การนำไปใช้อีก (reuse)**—ส่วนประกอบของสถาปัตยกรรมที่ใช้ร่วมกัน ควรนำไปเป็นส่วนหนึ่งของสถาปัตยกรรมเป้าหมายหรือสถาปัตยกรรมที่อยู่ระหว่างการปรับเปลี่ยน เพื่อใช้ในการออกแบบและนำกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ (solution) ไปใช้งาน
    - **ซื้อหรือสร้าง**—กระบวนการการแก้ไขปัญหาแบบเบ็ดเสร็จ (solution) ควรจะซื้อ ยกเว้นแต่ถ้ามีการตัดสินใจที่สมเหตุผลที่จะพัฒนาขึ้นใช้เองเป็นการภายใน
    - **ความเรียบง่าย**—สถาปัตยกรรมขององค์กรควรออกแบบให้เรียบง่ายและดูแลได้ง่ายเท่าที่จะเป็นไปได้ในขณะที่ยังคงตอบสนองความต้องการขององค์กร
    - **ความคล่องตัว**—สถาปัตยกรรมองค์กรควรมีความคล่องตัวเพื่อตอบสนองต่อการเปลี่ยนแปลงความต้องการของธุรกิจอย่างมีประสิทธิภาพและประสิทธิผล
    - **การเปิดรับ (Openness)**—สถาปัตยกรรมองค์กรควรใช้ประโยชน์จากมาตรฐานอุตสาหกรรมแบบเปิด (open industry standard)
  - นิยามขององค์กรสำหรับสถาปัตยกรรมที่เหมาะสมที่สุด มองไปที่การตอบสนองต่อความต้องการของผู้มีส่วนได้เสียที่มีความหลากหลาย มีรูปแบบ บัญชีรายชื่อ (catalogues) และมาตรวัดต่างๆ ที่ใช้อธิบายถึงสถาปัตยกรรมที่เป็นเกณฑ์พื้นฐาน สถาปัตยกรรมเป้าหมาย หรือสถาปัตยกรรมในระหว่างการปรับเปลี่ยน ยกตัวอย่างเช่น สถาปัตยกรรมระบบงานอาจอธิบายโดยใช้แผนภาพการเชื่อมต่อกันของระบบงาน (application interface diagram) ซึ่งแสดงถึงระบบงานต่างๆ ที่ใช้งานอยู่ (หรือที่วางแผนไว้) และการเชื่อมต่อระหว่างกัน
  - มีคลังเก็บสถาปัตยกรรม (architecture repository) ที่ใช้จัดเก็บผลลัพธ์ของสถาปัตยกรรมประเภทต่างๆ รวมถึง หลักการและมาตรฐานของสถาปัตยกรรม ต้นแบบอ้างอิงของสถาปัตยกรรม และผลงานที่ส่งมอบอื่นๆ ของสถาปัตยกรรม และที่ใช้กำหนดส่วนประกอบย่อย (building blocks) ของบริการ เช่น
    - ระบบงาน ที่ทำหน้าที่งานให้แก่ธุรกิจ
    - โครงสร้างพื้นฐานด้านเทคโนโลยี รวมถึง ฮาร์ดแวร์ ซอฟต์แวร์ระบบ และโครงสร้างพื้นฐานด้านเครือข่าย
    - โครงสร้างพื้นฐานทางกายภาพ
  - ระดับการให้บริการที่ต้องกำหนดขึ้น และผู้ให้บริการต้องปฏิบัติตาม

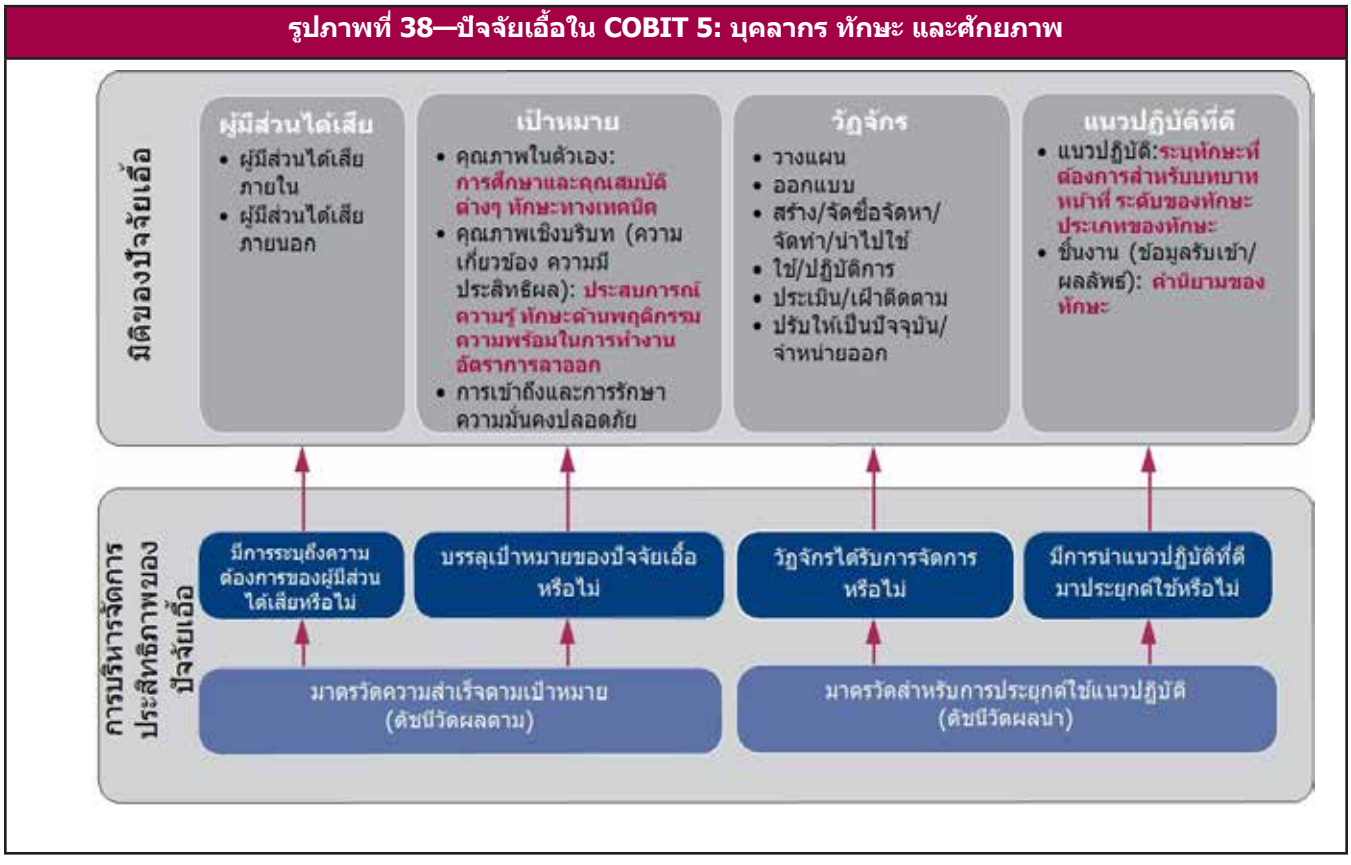
  ยังมีแนวปฏิบัติที่ดีจากภายนอกอื่นๆ สำหรับกรอบดำเนินงานด้านสถาปัตยกรรมและความสามารถในการให้บริการที่สามารถนำมาใช้ได้ ซึ่งรวมถึงแนวทาง แม่แบบ (template) หรือมาตรฐานต่างๆ ที่สามารถนำมาใช้เพื่อร่นระยะเวลาในการจัดทำผลงานด้านสถาปัตยกรรมที่จะต้องส่งมอบ ยกตัวอย่างเช่น
  - TOGAF[16] ให้ต้นแบบอ้างอิงด้านเทคนิคและต้นแบบอ้างอิงด้านโครงสร้างพื้นฐานของสารสนเทศเชิงบูรณาการ (integrated information infrastructure reference model)
  - ITIL ให้แนวทางที่ครอบคลุมในการออกแบบและปฏิบัติการสำหรับการให้บริการ
- **ความสัมพันธ์กับปัจจัยเอื้ออื่นๆ —ความเชื่อมโยงกับปัจจัยเอื้ออื่นๆ รวมถึง**
  - สารสนเทศเป็นส่วนหนึ่งของความสามารถในการให้บริการ และกระบวนการใช้ประโยชน์จากความสามารถในการให้บริการเพื่อส่งมอบบริการทั้งภายในและภายนอก
  - มุมมองด้านวัฒนธรรมและพฤติกรรมก็มีความเกี่ยวข้อง โดยจำเป็นต้องสร้างวัฒนธรรมที่เน้นการให้บริการ (service oriented culture)
  - ข้อมูลรับเข้าและผลลัพธ์ของแนวปฏิบัติในการบริหารจัดการ (management practice) และกิจกรรมต่างๆ ภายใน COBIT 5 ควรรวมถึงความสามารถในการให้บริการ ซึ่งใช้เป็นข้อมูลรับเข้าหรือส่งมอบเป็นผลลัพธ์

[16] www.opengroup.org/togaf

ปัจจัยเอื้อใน COBIT 5: บุคลากร ทักษะ และศักยภาพ

รายละเอียดเฉพาะสำหรับปัจจัยเอื้อด้านบุคลากร ทักษะ และศักยภาพ เปรียบเทียบกับคำอธิบายปัจจัยเอื้อทั่วไป (generic enabler) แสดงไว้ใน**รูปภาพที่ 38**

รูปภาพที่ 38—ปัจจัยเอื้อใน COBIT 5: บุคลากร ทักษะ และศักยภาพ



รูปแบบของบุคลากร ทักษะ และศักยภาพ แสดงถึง

- **ผู้มีส่วนได้เสีย**—ทักษะและศักยภาพอาจมีผู้มีส่วนได้เสียอยู่ภายในองค์หรือองค์กรก็ได้ ผู้มีส่วนได้เสียต่างๆ สวมบทบาทที่แตกต่างกัน—ผู้จัดการทางธุรกิจ ผู้จัดการโครงการ พันธมิตรทางธุรกิจ คู่แข่ง ผู้สรรหาบุคลากรใหม่ ผู้ฝึกอบรม ผู้พัฒนาระบบ ผู้เชี่ยวชาญทางเทคนิคด้านไอที และอื่นๆ —และแต่ละบทบาทจำเป็นต้องมีชุดของทักษะที่แตกต่างกัน
- **เป้าหมาย**—เป้าหมายสำหรับทักษะและศักยภาพเกี่ยวข้องกับระดับการศึกษาและคุณสมบัติ ทักษะด้านเทคนิค ระดับของประสบการณ์ ความรู้ และทักษะด้านพฤติกรรม ซึ่งเป็นสิ่งที่จำเป็นต้องมีเพื่อให้กิจกรรมต่างๆ ของกระบวนการและการปฏิบัติตามบทบาทหน้าที่ต่างๆ ขององค์กรประสบความสำเร็จ เป้าหมายสำหรับบุคลากรยังรวมถึงอัตรากำลังและอัตราการลาออกที่เหมาะสม
- **วัฏจักร**—ทักษะและศักยภาพมีวัฏจักร องค์กรต้องทราบทักษะพื้นฐานในปัจจุบันและวางแผนไปสู่ระดับที่ต้องการ ทักษะได้รับอิทธิผลส่วนหนึ่งจากกลยุทธ์และเป้าหมายขององค์กร ทักษะจำเป็นต้องได้รับการพัฒนาขึ้นมา (เช่น ผ่านทางการฝึกอบรม) หรือการจัดหา (เช่น ผ่านทางการสรรหาพนักงานใหม่) แล้วจัดสรรให้กับบทบาทต่างๆ ภายใต้โครงสร้างการจัดองค์กร ทักษะอาจจำเป็นต้องยกเลิกไป ยกตัวอย่างเช่น เมื่อกิจกรรมนั้นเปลี่ยนกรทำงานเป็นแบบอัตโนมัติ หรือให้หน่วยงานภายนอกมาดำเนินการแทน
  - องค์กรต้องประเมินทักษะพื้นฐานอย่างสม่ำเสมอ เช่น ปีละครั้ง เพื่อให้เข้าใจถึงวิวัฒนาการที่เกิดขึ้น ซึ่งจะเป็นข้อมูลที่ใช้ในกระบวนการวางแผนสำหรับงวดต่อไป
  - การประเมินนี้ยังช่วยป้อนข้อมูลเข้าสู่กระบวนการให้รางวัลและการยอมรับ (recognition) สำหรับการบริหารทรัพยากรบุคคล
- **แนวปฏิบัติที่ดี**—แนวปฏิบัติที่ดีสำหรับทักษะและศักยภาพ ได้รวมเอาการระบุถึงความจำเป็นที่จะต้องมีทักษะที่ต้องการสำหรับแต่ละบทบาทหน้าที่ของผู้มีส่วนได้เสียต่างๆ โดยอธิบายถึงระดับของทักษะที่แตกต่างกันในประเภทต่างๆ ของทักษะ ควรมีคำนิยามของคำว่าทักษะสำหรับในแต่ละระดับและประเภทของทักษะที่เหมาะสม ตัวอย่างประเภทของทักษะสำหรับกิจกรรมที่เกี่ยวข้องกับไอที ได้แก่ การบริหารจัดการสารสนเทศ การวิเคราะห์ธุรกิจ
  - แนวปฏิบัติที่ดีอื่นๆ
    - มีแนวปฏิบัติที่ดีจากแหล่งภายนอก เช่น กรอบการดำเนินงานด้านทักษะสำหรับยุคของสารสนเทศ (skills framework for the information age) หรือ SFIA[17] ซึ่งให้คำนิยามของคำว่าทักษะไว้อย่างครอบคลุม
    - ตัวอย่างประเภทของทักษะที่เป็นไปได้ เทียบกับกระบวนการของ COBIT 5 ในโดเมนต่างๆ แสดงไว้ใน**รูปภาพที่ 39**

[17] www.sfia.org.uk

รูปภาพที่ 39—ประเภทของทักษะใน COBIT 5	
กระบวนการในโดเมนต่างๆ	**ตัวอย่างประเภทของทักษะ**
ประเมิน สั่งการ และเฝ้าติดตาม (EDM)	• การกำกับดูแลไอทีระดับองค์กร
จัดวางแนว จัดทำแผน และจัดระบบ (APO)	• การจัดทำนโยบายด้านไอที • กลยุทธ์ด้านไอที • สถาปัตยกรรมองค์กร • นวัตกรรม • การบริหารการเงิน • การบริหารจัดการกลุ่ม (ของโครงการหรือเงินลงทุน)
จัดสร้าง จัดหา และนำไปใช้ (BAI)	• การวิเคราะห์ธุรกิจ • การบริหารโครงการ • การประเมินการใช้งาน (ใช้และเรียนรู้ได้ง่าย) • การให้คำนิยามและการบริหารจัดการความต้องการ • การจัดทำโปรแกรม • การยศาสตร์ของระบบ (System ergonomics) • การเลิกใช้งานซอฟต์แวร์ (Software decommissioning) • การบริหารจัดการขีดความสามรถ (Capacity management)
ส่งมอบ บริการ และสนับสนุน (DSS)	• การบริหารจัดการความพร้อมใช้ • การบริหารจัดการปัญหา • การบริหารจัดการหน่วยบริหาร (Service desk) และเหตุการณ์ผิดปกติ • การบริหารจัดการความมั่นคงปลอดภัย • ปฏิบัติการด้านไอที • การบริหารจัดการฐานข้อมูล
เฝ้าติตตาม วัดผล และประเมิน (MEA)	• การสอบทานการปฏิบัติตาม (กฎหมายหรือกฎระเบียบข้อบังคับ) • การเฝ้าติดตามประสิทธิภาพในการดำเนินงาน • การตรวจสอบการควบคุม

- **ความสัมพันธ์กับปัจจัยเอื้ออื่นๆ**—ความเชื่อมโยงกับปัจจัยเอื้ออื่นๆ รวมถึง
  - ทักษะและศักยภาพเป็นสิ่งจำเป็นสำหรับการปฏิบัติกิจกรรมต่างๆ ของกระบวนการและตัดสินใจตามโครงสร้างการจัดองค์กร ในทางกลับกัน บางกระบวนการเน้นที่การสนับสนุนวัฏจักรของทักษะและศักยภาพ
  - มีการเชื่อมโยงกับวัฒนธรรม จริยธรรม และพฤติกรรม กับทักษะด้านพฤติกรรม ซึ่งได้แก่การผลักดันพฤติกรรมบุคคลและพฤติกรรมบุคคลนี้ก็ได้รับอิทธิพลจากจริยธรรมส่วนบุคคลและจริยธรรมองค์กร
  - คำนิยามของคำว่าทักษะก็คือสารสนเทศ ซึ่งจำเป็นต้องได้รับการพิจารณาตามแนวปฏิบัติที่ดีสำหรับปัจจัยเอื้อด้านสารสนเทศ

ภาคผนวก H
อภิธานศัพท์

คำศัพท์อังกฤษ	คำศัพท์ไทย	คำนิยาม
accountability	ผู้รับผิดชอบในผลงาน (RACI)	บุคคล กลุ่มบุคคล หรือหน่วยงานที่รับผิดชอบในผลสุดท้ายของเรื่อง กระบวนการ หรือขอบเขตงานอย่างใดอย่างหนึ่ง ในตาราง RACI จะใช้ตอบคำถาม: ใครเป็นผู้รับผิดชอบต่อความสำเร็จของงาน
Accountability of governance	ความรับผิดชอบในผลงานของการกำกับดูแล	การกำกับดูแลทำให้มั่นใจว่าองค์กรจะบรรลุวัตถุประสงค์ โดยการประเมินความต้องการของผู้มีส่วนได้เสีย เงื่อนไข และทางเลือก; กำหนดทิศทางผ่านทางการจัดลำดับความสำคัญและการตัดสินใจ; และเฝ้าติดตามประสิทธิภาพในการดำเนินงาน การปฏิบัติตามกฎระเบียบข้อบังคับ และความคืบหน้าของงานเปรียบเทียบกับแผน ในองค์กรส่วนใหญ่ การกำกับดูแลเป็นหน้าที่ความรับผิดชอบของคณะกรรมการบริหารภายใต้การนำของประธานกรรมการ
Activity	กิจกรรม	ใน COBIT หมายถึงการกระทำหลักที่ใช้ในการดำเนินกระบวนการ แนวทางเพื่อบรรลุแนวปฏิบัติในการบริหารจัดการเพื่อให้ประสบความสำเร็จในการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร กิจกรรม • อธิบายถึงกลุ่มของการกระทำที่จำเป็นและเพียงพอในขั้นตอนของการนำไปใช้ (implementation step) เพื่อให้สามารถบรรลุแนวปฏิบัติในการกำกับดูแลหรือแนวปฏิบัติในการบริหารจัดการ • พิจารณาถึงข้อมูลรับเข้า (input) และผลลัพธ์ของกระบวนการ • ตั้งอยู่บนพื้นฐานของมาตรฐานและแนวปฏิบัติที่ดี ซึ่งเป็นที่ยอมรับกันโดยทั่วไป • สนับสนุนการจัดให้มีบทบาทหน้าที่และความรับผิดชอบที่ชัดเจน • ไม่ใช่สิ่งที่ตายตัว และจำเป็นต้องนำไปปรับใช้และพัฒนาให้เป็นกระบวนการเฉพาะที่เหมาะสมกับองค์กร
Alignment	ความสอดคล้อง	ภาวะที่ปัจจัยเอื้อในการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรสนับสนุนเป้าหมายและกลยุทธ์ขององค์กร
Application architecture	สถาปัตยกรรมระบบงาน	คำอธิบายถึงกลุ่มทางตรรกะ (logical group) ของความสามารถ (capability) ซึ่งใช้จัดการวัตถุต่างๆ ที่จำเป็นในการประมวลสารสนเทศและสนับสนุนวัตถุประสงค์ขององค์กร
Architecture board	คณะกรรมการบริหารด้านสถาปัตยกรรม	กลุ่มของผู้มีส่วนได้เสียและผู้เชี่ยวชาญที่รับผิดชอบในผลงานสำหรับการให้แนวทางในเรื่องและในการตัดสินใจที่เกี่ยวข้องกับสถาปัตยกรรมองค์กร ตลอดจนสำหรับการกำหนดนโยบายและมาตรฐานด้านสถาปัตยกรรม
Authentication	การพิสูจน์ตัวตน	การกระทำเพื่อพิสูจน์ตัวตนและสิทธิ์ของผู้ใช้ ในการเข้าถึงสารสนเทศบนระบบคอมพิวเตอร์ หมายเหตุ: การให้ความเชื่อมั่น: การพิสูจน์ตัวตนออกแบบมาเพื่อป้องกันการลงชื่อเข้าใช้ระบบโดยมิชอบ และยังอาจหมายถึงการพิสูจน์ความถูกต้องของข้อมูลด้วย
Authentication Baseline architecture	สถาปัตยกรรมที่เป็นเกณฑ์พื้นฐาน	คำอธิบายที่มีอยู่ของพื้นฐานการออกแบบส่วนประกอบของระบบธุรกิจ ก่อนที่จะเข้าสู่วัฏจักรของการสอบทานสถาปัตยกรรมและออกแบบใหม่ (redesign)
Benefit realization	การได้รับผลประโยชน์	เป็นหนึ่งในวัตถุประสงค์ของการกำกับดูแล การนำมาซึ่งผลประโยชน์ใหม่ๆ สำหรับองค์กร การดำรงรักษาและเพิ่มพูนผลประโยชน์ในรูปแบบที่เป็นอยู่ และการกำจัดการริเริ่มดำเนินการ (initiatives) และสินทรัพย์ที่ไม่สร้างคุณค่าพอ
Business continuity	ความต่อเนื่องในการดำเนินธุรกิจ	ป้องกัน ลดโอกาส และกู้คืนสภาพจากการหยุดชะงัก ในความหมายของ 'การวางแผนกลับคืนสู่การดำเนินธุรกิจ (business resumption planning)' 'การวางแผนฟื้นฟูระบบจากภัยพิบัติ (disaster recovery planning)' และ 'การวางแผนรับมือสถานการณ์ฉุกเฉิน (contingency planning)' อาจนำมาใช้ในบริบทนี้ ซึ่งจะเน้นที่มุมมองในด้านการกู้คืนสภาพ (recovery) ของความต่อเนื่อง และด้วยสาเหตุนี้ จึงควรพิจารณาถึงมุมมองในด้าน 'ความสามารถในการกลับคืนสู่สภาพเดิม (resilience)' ด้วย
Business goal	เป้าหมายทางธุรกิจ	การแปลความหมายของพันธกิจขององค์กรจากถ้อยแถลงเจตจำนง (statement of intention) มาเป็นเป้าและผลของประสิทธิภาพในการดำเนินงาน
Business process control	การควบคุมกระบวนการทางธุรกิจ	นโยบาย ขั้นตอนการปฏิบัติงาน แนวปฏิบัติ และโครงสร้างการจัดองค์กรที่ออกแบบมาเพื่อให้ความเชื่อมั่นได้พอควรว่ากระบวนการทางธุรกิจจะสามารถบรรลุเป้าหมาย

คำศัพท์อังกฤษ	คำศัพท์ไทย	คำนิยาม
Chargeback	การคิดค่าใช้จ่ายกลับคืน	การคิดค่าใช้จ่ายกลับคืนไปให้หน่วยงานในบริษัทที่ก่อให้เกิดค่าใช้จ่ายนี้ขึ้นมา หมายเหตุ: การคิดค่าใช้จ่ายกลับคืน (chargeback) มีความสำคัญเพราะหากไม่มีนโยบายดังกล่าวแล้ว อาจจะเกิดมุมมองที่คลาดเคลื่อนสำหรับความสามารถในการกำไรที่แท้จริงของสินค้าและบริการได้ หากค่าใช้จ่ายหลักถูกละเลยหรือคำนวณตามอำเภอใจ
COBIT	COBIT	1. COBIT 5: เดิมเป็นที่รู้จักในชื่อเต็มว่า Control objectives for information and related technology (COBIT) ปัจจุบันใช้อักษรย่อและเป็นการทบทวนรอบที่ 5 COBIT 5 เป็นกรอบการดำเนินงานด้านการกำกับดูแลและการบริหารจัดการด้านสารสนเทศและเทคโนโลยี (ไอที) ระดับองค์กรที่สมบูรณ์และเป็นที่ยอมรับในระดับสากล ซึ่งสนับสนุนผู้บริหารทุกระดับขององค์กรในการกำหนดและบรรลุเป้าหมายทางธุรกิจและเป้าหมายด้านไอที COBIT อธิบายถึงหลักการ 5 ประการและปัจจัยเอื้อ 7 ประเภทที่สนับสนุนองค์กรในการพัฒนาและนำไปใช้ซึ่งแนวปฏิบัติที่ดีด้านการกำกับดูแลและการบริหารจัดการที่เกี่ยวข้องกับไอที รวมถึงการพัฒนาอย่างต่อเนื่องและการเฝ้าติดตาม หมายเหตุ: ใน COBIT รุ่นก่อนหน้านี้ จะเน้นในด้านวัตถุประสงค์ของการควบคุม (control objective) ที่เกี่ยวข้องกับกระบวนการด้านไอที การบริหารจัดการและการควบคุมกระบวนการด้านไอที และการกำกับดูแลด้านไอที การประยุกต์และนำกรอบดำเนินงาน COBIT มาใช้ได้รับการสนับสนุนจากผลิตภัณฑ์ในชุดของ COBIT ที่ได้รับพัฒนาออกมาใหม่อยู่เรื่อยๆ (ดูข้อมูลจาก www.isaca.org/cobit) 2. COBIT 4.1 และรุ่นก่อนหน้านี้: เดิมเป็นที่รู้จักในชื่อเต็มว่า Control objectives for information and related technology (COBIT) ซึ่งเป็นกรอบการดำเนินงานสำหรับไอทีที่สมบูรณ์และเป็นที่ยอมรับในระดับสากล ซึ่งสนับสนุนผู้บริหารและผู้บริหารระดับสูงทั้งทางธุรกิจและด้านไอทีในการกำหนดเป้าหมายทางธุรกิจและเป้าหมายที่เกี่ยวข้องกับไอที และบรรลุเป้าหมายเหล่านี้โดยให้ต้นแบบในการกำกับดูแล การบริหารจัดการ การควบคุม และการให้ความเชื่อมั่นด้านไอทีอย่างครอบคลุม COBIT อธิบายถึงกระบวนการด้านไอทีและวัตถุประสงค์การควบคุมที่เกี่ยวข้อง แนวทางในการบริหารจัดการ (กิจกรรรม ความรับผิดชอบในผลงาน ความรับผิดชอบตามหน้าที่ และมาตรวัดประสิทธิภาพในการดำเนินงาน) และต้นแบบของระดับวุฒิภาวะ (maturity model) COBIT สนับสนุนผู้บริหารขององค์กรในการพัฒนา การนำไปใช้ การปรับปรุงอย่างต่อเนื่อง และการเฝ้าติดตามแนวปฏิบัติที่ดีที่เกี่ยวข้องกับไอที หมายเหตุ: การรับกรอบดำเนินงาน COBIT มาใช้ได้รับการสนับสนุนจากแนวทางสำหรับผู้บริหารและผู้บริหารระดับสูง (ใน บทสรุปสำหรับคณะกรรมการบริหารเพื่อการกำกับดูแลไอที พิมพ์ครั้งที่ 2 - board briefing on IT governance 2 edition) สำหรับผู้นำการกำกับดูแลด้านไอทีไปใช้งาน (IT governance implementers) (ใน COBIT Quickstart, 2nd Edition; IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition; และใน COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance) และสำหรับผู้ประกอบวิชาชีพด้านการให้ความเชื่อมั่นและการตรวจสอบด้านไอที (ใน IT Assurance Guide Using COBIT) นอกจากนี้ ยังมีแนวทางที่สนับสนุนการประยุกต์ใช้สำหรับข้อกำหนดด้านกฎหมายและกฎระเบียบข้อบังคับ (ยกตัวอย่างเช่น IT Control Objectives for Sarbanes-Oxley และ IT Control Objectives for Basel II) และที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ (ใน COBIT Security Baseline) ได้มีการแสดง COBIT เทียบกับกรอบดำเนินงานและมาตรฐานอื่นๆ เพื่อให้เห็นภาพของความครอบคลุมอย่างสมบูรณ์ในวัฏจักรของการบริหารจัดการด้านไอที และสนับสนุนการใช้ COBIT ในองค์กรที่ใช้กรอบดำเนินงานและมาตรฐานที่เกี่ยวกับไอทีที่หลากหลาย
Competence	ความสามารถ/ศักยภาพ	ความสามารถในการปฏิบัติภารกิจ การกระทำ และหน้าที่งานให้สำเร็จ

คำศัพท์อังกฤษ	คำศัพท์ไทย	คำนิยาม
Consulted party (RACI)	ผู้ให้คำปรึกษา (RACI)	หมายถึงบุคคลที่ให้ความเห็นเกี่ยวกับกิจกรรม (การสื่อสาร 2 ทาง) ในตาราง RACI จะใช้ตอบคำถาม: ใครเป็นผู้ให้ข้อมูล เป็นบทบาทหน้าที่หลักที่ให้ข้อมูล (input) โปรดสังเกตว่าจะขึ้นอยู่กับผู้มีความรับผิดชอบในผลงานและผู้มีความรับผิดชอบตามหน้าที่ที่จะรับสารสนเทศมาจากส่วนงานหรือพันธมิตรภายนอกอื่นๆ ด้วย อย่างไรก็ตาม ข้อมูล (input) ที่รับมาจากบทบาทต่างๆที่มีอยู่ในรายการจะได้รับการพิจารณา และต้องมีการดำเนินการที่เหมาะสมในการแจ้งเรื่องตามระดับ (escalation) ถ้าจำเป็น
Context	บริบท	กลุ่มของปัจจัยทั้งภายในและภายนอกโดยรวมที่อาจมีอิทธิพลหรือมีส่วนในการกำหนดว่าองค์กร หน่วยงาน กระบวนการ หรือบุคคลจะมีการกระทำอย่างไร หมายเหตุ: บริบทประกอบด้วย • บริบททางเทคโนโลยี—ปัจจัยด้านเทคโนโลยีที่มีผลต่อความสามารถขององค์กรในการสร้างคุณค่าจากข้อมูล • บริบททางข้อมูล—ข้อมูลมีความถูกต้อง พร้อมใช้งาน เป็นปัจจุบัน และมีคุณภาพ • ทักษะและความรู้—ประสบการณ์ทั่วไป และทักษะด้านการวิเคราะห์ ด้านเทคนิค และด้านธุรกิจ • บริบทด้านโครงสร้างการจัดองค์กรและวัฒนธรรม—ปัจจัยด้านการเมือง และองค์กรชอบที่จะใช้ข้อมูลมากกว่าใช้สัญชาติญาณหรือไม่ • บริบทด้านกลยุทธ์—วัตถุประสงค์ด้านกลยุทธ์ขององค์กร
Control	การควบคุม	วิธีในการบริหารความเสี่ยง รวมถึงนโยบาย ขั้นตอนการปฏิบัติงาน แนวทาง แนวปฏิบัติ หรือโครงสร้างการจัดองค์กร ซึ่งอาจเป็นด้านการจัดการดูแล (administrative) ด้านเทคนิค ด้านการบริหาร หรือด้านกฎหมาย และยังใช้ในความหมายเดียวกันกับการปกป้อง (safeguard) หรือมาตรการรับมือ (countermeasure)
Culture	วัฒนธรรม	แบบแผน (pattern) ของพฤติกรรม ความเชื่อ สมมติฐาน ทัศนคติ และวิธีในการทำสิ่งต่างๆ
Driver	ปัจจัยขับเคลื่อน/ปัจจัยผลักดัน	ปัจจัยภายนอกหรือปัจจัยภายใน ที่ริเริ่มดำเนินการหรือส่งผลให้องค์กรหรือบุคคลกระทำการหรือเกิดการเปลี่ยนแปลง
enterprise goal	เป้าหมายองค์กร	ดู เป้าหมายของธุรกิจ (business goal)
Enterprise governance	การกำกับดูแลองค์กร	กลุ่มของหน้าที่ความรับผิดชอบและแนวปฏิบัติที่ดำเนินการโดยคณะกรรมการบริหารและผู้บริหารระดับสูง โดยมีเป้าหมายในการให้ทิศทางเชิงกลยุทธ์ ทำให้เกิดความมั่นใจว่าจะบรรลุวัตถุประสงค์ แน่ใจได้ว่าความเสี่ยงได้รับการบริหารจัดการอย่างเหมาะสม และตรวจสอบว่ามีการใช้ทรัพยากรขององค์กรอย่างมีความรับผิดชอบ และยังอาจหมายถึงมุมมองด้านการกำกับดูแลที่เน้นองค์กรโดยรวม ซึ่งเป็นมุมมองในภาพรวมระดับสูงสุดของการกำกับดูแลซึ่งทุกมุมมองอื่นทั้งหมดจะต้องสอดคล้องกับมุมมองนี้
Full economic life cycle	ตลอดอายุการใช้งานที่เหมาะสม	ช่วงระยะเวลาที่คาดว่าจะได้รับผลประโยชน์ทางธุรกิจอย่างเป็นนัยสำคัญ และ/หรือช่วงระยะเวลาที่คาดว่าจะเกิดค่าใช้จ่ายอย่างเป็นนัยสำคัญ (รวมถึงการลงทุน ต้นทุนในการดำเนินธุรกิจ และต้นทุนในการเลิกธุรกิจ) จากการลงทุนในชุดโครงการ (programme)
Good practice	แนวปฏิบัติที่ดี	กิจกรรมหรือกระบวนการที่ได้รับการพิสูจน์แล้วว่า เมื่อองค์กรต่างๆนำมาใช้งานแล้วจะประสบความสำเร็จ และสามารถทำให้เกิดผลลัพธ์ที่เชื่อถือได้
Governance	การกำกับดูแล	การกำกับดูแลช่วยให้มั่นใจได้ว่า ความต้องการ เงื่อนไข และทางเลือกต่างๆ ของผู้มีส่วนได้เสียได้รับการประเมินเพื่อพิจารณาถึงการบรรลุวัตถุประสงค์ที่มีความสมดุลและเห็นพ้องต้องกันขององค์กร; การกำหนดทิศทางผ่านทางการจัดลำดับความสำคัญและการตัดสินใจ; และการเฝ้าติดตามประสิทธิภาพในการดำเนินงานและการปฏิบัติตามทิศทางและวัตถุประสงค์ที่เห็นพ้องต้องกัน
Governance/ management practice	แนวปฏิบัติในการกำกับดูแล/การบริหารจัดการ	สำหรับแต่ละกระบวนการของ COBIT แนวปฏิบัติในการกำกับดูแลและการบริหารจัดการ จะให้ข้อกำหนดในภาพรวมที่ครบชุดสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่มีประสิทธิผลและนำไปปฏิบัติได้จริง แนวปฏิบัติในการกำกับดูแล/การบริหารจัดการนี้เป็นคำแถลงการณ์กระทำ (statements of actions) จากหน่วยงานกำกับดูแลและผู้บริหาร
Governance enabler	ปัจจัยเอื้อด้านการกำกับดูแล	สิ่ง (ทั้งจับต้องได้และจับต้องไม่ได้) ที่ช่วยให้เกิดการกำกับดูแลที่มีประสิทธิผล

คำศัพท์อังกฤษ	คำศัพท์ไทย	คำนิยาม
Governance framework	กรอบการดำเนินงานด้านการกำกับดูแล	กรอบการดำเนินงานเป็นโครงสร้างแนวคิดพื้นฐานที่ใช้ในการแก้ไขหรือจัดการประเด็นปัญหาที่มีความซับซ้อน เป็นปัจจัยเอื้อสำหรับการกำกับดูแล เป็นกลุ่มของแนวคิด ข้อสมมุติฐาน และแนวปฏิบัติที่ใช้กำหนดวิธีปฏิบัติหรือทำความเข้าใจในบางเรื่อง ตลอดจนกำหนดความสัมพันธ์ระหว่างหน่วยงานต่างๆที่มีส่วนร่วม บทบาทหน้าที่ของผู้ที่มีส่วนร่วม และขอบเขต (อะไรที่รวมและไม่รวมอยู่ในระบบการกำกับดูแล) ตัวอย่าง: COBIT และการควบคุมภายใน—กรอบการดำเนินงานแบบบูรณาการของ COSO
Governance of enterprise IT	การกำกับดูแลไอทีระดับองค์กร	มุมมองของการกำกับดูแลที่ให้ความมั่นใจว่า สารสนเทศและเทคโนโลยีที่เกี่ยวข้องสนับสนุนและเอื้อต่อกลยุทธ์ขององค์กรและช่วยให้องค์กรบรรลุวัตถุประสงค์ และยังรวมถึงหน้าที่ในการกำกับดูแลด้านไอที กล่าวคือ การทำให้มั่นใจว่าความสามารถด้านไอทีเกิดขึ้นได้อย่างมีประสิทธิภาพและประสิทธิผล
Information	สารสนเทศ	เป็นสินทรัพย์เช่นเดียวกับสินทรัพย์ทางธุรกิจที่สำคัญอื่นๆ ขององค์กร เป็นที่สิ่งจำเป็นต่อการดำเนินธุรกิจขององค์กร อาจอยู่ในรูปแบบที่แตกต่างกัน เช่น สิ่งพิมพ์หรือข้อความที่เขียนบนกระดาษ เก็บในรูปแบบของอิเล็กทรอนิก ส่งทางไปรษณีย์หรือทางอิเล็กทรอนิกส์ แสดงบนฟิล์ม หรือคำพูดในการสนทนา
Informed party (RACI)	ผู้ที่ได้รับแจ้งให้รับทราบ (RACI)	หมายถึงผู้ที่บุคคลต่างๆจะให้ข้อมูลเกี่ยวกับความก้าวหน้าของงานหรือกิจกรรม (การสื่อสารทางเดียว) ในตาราง RACI จะใช้ตอบคำถาม: ใครเป็นผู้ได้รับสารสนเทศ เป็นบทบาทหน้าที่ที่จะได้รับแจ้งให้ทราบถึงความสำเร็จของงานและ/หรือการส่งมอบงาน ทั้งนี้ แน่นอนอยู่แล้วว่าบทบาทหน้าที่ซึ่ง 'รับผิดชอบในผลงาน' ควรจะได้รับสารสนเทศอย่างเหมาะสมอยู่เสมอเพื่อให้สามารถควบคุมดูแลการทำงานได้ เช่นเดียวกับบทบาทหน้าที่ซึ่ง 'รับผิดชอบตามหน้าที่' ที่ควรได้รับสารสนเทศในส่วนที่ตนรับผิดชอบ
Inputs and outputs	ข้อมูลรับเข้าและผลลัพธ์	ชิ้นงานนหรือสิ่งที่จัดทำขึ้นของกระบวนการที่ถือได้ว่ามีจำเป็นในการสนับสนุนการดำเนินกระบวนการ โดยเอื้อต่อการตัดสินใจที่สำคัญ ให้ข้อมูลและร่องรอยสำหรับการตรวจสอบกิจรรมต่างๆของกระบวนการ และเอื้อต่อการติดตามเหตุการณ์ผิดปกติที่เกิดขึ้น โดยระบุที่ระดับของแนวปฏิบัติในการบริหารจัดการ (management practice) และอาจรวมถึงชิ้นงานบางอย่างที่ใช้ภายในกระบวนการเท่านั้นและมักจะเป็นข้อมูลรับเข้า (input) ที่สำคัญของกระบวนการอื่น ข้อมูลรับเข้า (input) และผลลัพธ์ที่ระบุไว้ใน COBIT 5 ไม่ควรถือว่ามีเพียงรายการเหล่านั้นเท่านั้น เพราะอาจมีการกำหนดกระแสสารสนเทศ (information flow) เพิ่มเติมขึ้นได้อีก ขึ้นอยู่กับสภาพแวดล้อมขององค์กรและกรอบการดำเนินงานของกระบวนการ
Investment portfolio	กลุ่มของการลงทุน	กลุ่มของการลงทุนที่กำลังได้รับการพิจารณาหรือกำลังดำเนินการอยู่
IT application	ระบบงานด้านไอที	เป็นหน้าที่งานทางอิเล็กทรอนิกที่เป็นส่วนของกระบวนการทางธุรกิจ ซึ่งดูแลโดยหรือได้รับการสนับสนุนจากหน่วยงานด้านไอที
IT goal	เป้าหมายด้านไอที	ข้อความที่อธิบายถึงผลลัพธ์ที่ต้องการของไอทีระดับองค์กรเพื่อสนับสนุนเป้าหมายขององค์กร ผลลัพธ์อาจเป็นสิ่งที่จัดทำขึ้นมา การเปลี่ยนแปลงสถานะอย่างเป็นนัยสำคัญ หรือการปรับปรุงความสามารถอย่างเป็นนัยสำคัญ
IT service	การให้บริการด้านไอที	การให้บริการโครงสร้างพื้นฐานและระบบงานด้านไอทีกับลูกค้าในแต่ละวันและการสนับสนุนผู้ใช้งาน ตัวอย่างรวมถึง หน่วยบริการ (service desk) การจัดหาและย้ายอุปกรณ์ และการให้สิทธิ์เพื่อรักษาความมั่นคงปลอดภัย
Management	ผู้บริหาร	ผู้บริหารวางแผน จัดสร้าง ดำเนินการ และเฝ้าติดตามกิจกรรมต่างๆให้สอดคล้องกับทิศทางที่กำหนดมาจากหน่วยงานกำกับดูแลเพื่อให้บรรลุวัตถุประสงค์ขององค์กร
Model	ต้นแบบ/รูปแบบ	วิธีที่ใช้อธิบายถึงกลุ่มขององค์ประกอบและความสัมพันธ์ระหว่างองค์ประกอบเหล่านั้นเพื่ออธิบายถึงการทำงานหลักของวัตถุ ระบบ หรือแนวคิดอย่างใดอย่างหนึ่ง
Metric	มาตรวัด	หน่วยวัดเชิงปริมาณที่ใช้วัดความสำเร็จของกระบวนการตามเป้าหมายที่กำหนด มาตรวัดควรจะ SMART-ชี้เฉพาะ (Specific) วัดผลได้ (Measurable) ทำงานได้ (Actionable) เกี่ยวเนื่อง (Relevant) และทันเวลา (Timely) แนวทางสำหรับมาตรวัดที่สมบูรณ์จะต้องระบุถึงหน่วยที่ใช้ ความถี่ในการวัด ค่าเป้าหมายที่ต้องการ(ถ้าเหมาะสม) และยังรวมถึงขั้นตอนที่จะต้องดำเนินการในการวัดผล และขั้นตอนในการตีความผลการประเมิน

คำศัพท์อังกฤษ	คำศัพท์ไทย	คำนิยาม
Objective	วัตถุประสงค์	คำแถลงถึงผลลัพธ์ที่ต้องการ
Organisational structure	โครงสร้างการจัดองค์กร	ปัจจัยเอื้อสำหรับการกำกับดูแลและการบริหารจัดการ รวมถึงองค์กรและโครงสร้างขององค์กร ลำดับและสายการบังคับบัญชา ตัวอย่าง: คณะกรรมการอำนวยการ (Steering Committee)
Output	ผลลัพธ์	ดูใน ข้อมูลรับเข้าและผลลัพธ์ (inputs and outputs)
Owner	เจ้าของ	บุคคลหรือกลุ่มที่ถือหรือได้รับสิทธิและมีความรับผิดชอบต่อองค์องค์กร ต่อหน่วยงาน (entity) หรือต่อสินทรัพย์ขององค์กร เช่น เจ้าของกระบวนการ เจ้าของระบบ
Policy	นโยบาย	ความตั้งใจและทิศทางในภาพรวมที่ผู้บริหารแสดงออกมาอย่างเป็นทางการ
Principle	หลักการ	ปัจจัยเอื้อสำหรับการกำกับดูแลและการบริหารจัดการ ประกอบด้วยค่านิยามและข้อสมมติฐานขั้นพื้นฐานที่องค์กรยึดถืออยู่ ความเชื่อที่ชี้นำและกำหนดขอบเขตการตัดสินใจขององค์กร การสื่อสารทั้งภายในและภายนอกองค์กร และการดูแลรักษา (steward-ship)—การดูแลสินทรัพย์ที่ผู้อื่นเป็นเจ้าของ ตัวอย่าง: กฎบัตรจริยธรรม (ethic charter) กฎบัตรความรับผิดชอบต่อสังคม (social responsibility charter)
Process	กระบวนการ	โดยทั่วไปหมายถึงกลุ่มของแนวปฏิบัติที่ได้รับอิทธิพลจากนโยบายและกระบวนการขององค์กรซึ่งรับข้อมูลมาจากแหล่งต่างๆ (ซึ่งรวมถึงกระบวนการอื่นๆ) จัดดำเนินการ (manipulate) ข้อมูลที่รับเข้าและจัดทำผลลัพธ์ (เช่น ผลิตภัณฑ์ บริการ) หมายเหตุ: กระบวนการมีเหตุผลทางธุรกิจที่สมเหตุสมผลสำหรับการมีอยู่ มีเจ้าของผู้รับผิดชอบในผลงาน (accountable owner) มีบทบาทหน้าที่ความรับผิดชอบที่ชัดเจนในการปฏิบัติงาน และมีวิธีการสำหรับการวัดผลการปฏิบัติงาน
Process (capability) attribute	คุณลักษณะ (ความสามารถ) ของกระบวนการ	ISO/IEC 15504: เป็นลักษณะความสามารถของกระบวนการ (process capability) ที่วัดผลได้ ซึ่งประยุกต์ใช้กับกระบวนการใดๆ ก็ได้
Process capability	ความสามารถของกระบวนการ	ISO/IEC 15504: เป็นลักษณะความสามารถของกระบวนการที่ช่วยให้บรรลุเป้าหมายทางธุรกิจในปัจจุบันหรือที่ประมาณไว้
Process goal	เป้าหมายของกระบวนการ	ข้อความที่อธิบายถึงผลลัพธ์ที่ต้องการจากกระบวนการ ผลลัพธ์อาจเป็นสิ่งที่จัดทำขึ้นมา การเปลี่ยนสถานะอย่างเป็นนัยสำคัญ หรือการปรับปรุงความสามารถของกระบวนการอื่นๆ อย่างเป็นนัยสำคัญ
Programme and project management office (PMO)	สำนักงานบริหารโครงการและชุดโครงการ	เป็นหน้าที่งานที่รับผิดชอบในการสนับสนุนผู้บริหารชุดโครงการ (programmes) และโครงการ ในการรวบรวม ประเมิน และรายงานสารสนเทศที่เกี่ยวกับการดำเนินงานตามชุดโครงการและโครงการต่างๆที่ประกอบอยู่ในชุดโครงการนั้นๆ
Services	บริการ	ดู การให้บริการด้านไอที (IT service)
Skill	ทักษะ	ความสามารถในการเรียนรู้เพื่อบรรลุผลลัพธ์ที่ตั้งไว้
Stakeholder	ผู้มีส่วนได้เสีย	ผู้ที่รับผิดชอบในหน้าที่ต่อความคาดหวังหรือผลประโยชน์อื่นๆ บางประการขององค์กร—เช่น ผู้มีส่วนได้เสีย ผู้ใช้งาน รัฐบาล ผู้ขาย ลูกค้า และสารธารณชน
System of internal control	ระบบการควบคุมภายใน	นโยบาย มาตรฐาน แผนงานและขั้นตอนการปฏิบัติงาน และโครงสร้างการจัดองค์กรที่ออกแบบมาเพื่อให้ความเชื่อมั่นได้พอควรว่า จะบรรลุวัตถุประสงค์ขององค์กร และเหตุการณ์ที่ไม่พึงปรารถนาจะได้รับการป้องกัน ตรวจพบและแก้ไข
Value creation	การสร้างคุณค่า	วัตถุประสงค์หลักด้านการกำกับดูแลขององค์กร จะบรรลุเมื่อสามารถสร้างสมดุลระหว่างวัตถุประสงค์พื้นฐาน 3 ข้อ (การได้รับผลประโยชน์ ความเสี่ยงที่เหมาะสม และทรัพยากรที่ให้ประโยชน์สูงสุด)

หน้านี้เป็นหน้าว่าง