

249092

ห้องสมุดงานวิจัย สำนักงานคณะกรรมการวิจัยแห่งชาติ



249092



การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT  
INFORMATION TECHNOLOGY AUDITING BY COBIT

ภาพร กิโยคิดกชชัย

งานค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต  
สาขาวิชาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร บัณฑิตวิทยาลัย มหาวิทยาลัยสุรนารี

พ.ศ. 2553



606254340

# การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT



ภาพร ภิชัยดิษฐชัย

งานค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต  
สาขาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์

พ.ศ. 2553

# **Information Technology Auditing by COBIT**

**Paporn Piyayodilokchai**

**An Independent Study Submitted in Partial Fulfillment of the Requirements  
for the Degree of Master of Science (Computer and Communication Technology)**

**Department of Computer and Communication Technology**

**Graduate School, Dhurakij Pundit University**

**2010**



ใบรับรองงานค้นคว้าอิสระ  
บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์  
ปริญญา วิทยาศาสตร์มหาบัณฑิต

หัวข้องานค้นคว้าอิสระ การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT

เสนอโดย ภาพร ภิชโยคิลกษัย

สาขาวิชา เทคโนโลยีคอมพิวเตอร์และการสื่อสาร

อาจารย์ที่ปรึกษางานค้นคว้าอิสระ ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบงานค้นคว้าอิสระแล้ว

.....ประธานกรรมการ  
(รองศาสตราจารย์ ดร.ณรงค์ มั่งคั่ง)

.....กรรมการและอาจารย์ที่ปรึกษางานค้นคว้าอิสระ  
(ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์)

.....กรรมการ  
(อาจารย์ ดร.ประศาสน์ จันทราทิพย์)

บัณฑิตวิทยาลัยรับรองแล้ว

.....คณบดีบัณฑิตวิทยาลัย  
(รองศาสตราจารย์ ดร.ธนิกา จิตรน้อมรัตน์)

วันที่ 17 เดือน สิงหาคม พ.ศ. ๒๕๕3

หัวข้องานคั่นคว่ำอิสระ	การตรวจสอบระบบเทคโนโลยีสารสนเทศตาม แนวทางของ COBIT
ชื่อผู้เขียน	ภาพร ภัย โยคิลักษณ์
อาจารย์ที่ปรึกษางานคั่นคว่ำอิสระ	ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์
สาขาวิชา	เทคโนโลยีคอมพิวเตอร์และการสื่อสาร
ปีการศึกษา	2553

### บทคัดย่อ

249092

งานคั่นคว่ำอิสระ การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT เป็นการศึกษารวบรวมข้อมูลเกี่ยวกับเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ การตรวจสอบระบบเทคโนโลยีสารสนเทศ และ COBIT FRAMEWORK เพื่อนำกรอบมาตรฐานของ COBIT มาใช้เป็นแนวทางในการจัดทำแนวการตรวจสอบระบบเทคโนโลยีสารสนเทศตามโครงสร้างของมาตรฐาน COBIT บนพื้นฐานของกระบวนการทางธุรกิจ 4 กระบวนการหลัก (Domain) ได้แก่ การวางแผนและการจัดการองค์กร (PO : Planning and Organization) การจัดหาและติดตั้ง (AI : Acquisition and Implementation) การส่งมอบและบำรุงรักษา (DS : Delivery and Support) การติดตามผล (M : Monitoring)

แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT นั้น ผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถนำมาใช้เป็นเครื่องมือในการปฏิบัติงานตรวจสอบ และหัวหน้าหน่วยงานตรวจสอบสามารถใช้เป็นเครื่องมือในการสอบทานและควบคุมงาน ซึ่งทำให้การตรวจสอบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างครอบคลุมตามระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร และบรรลุวัตถุประสงค์ของการตรวจสอบ อย่างไรก็ตาม รายละเอียดของการนำไปปฏิบัติในกระบวนการต่าง ๆ ในมาตรฐาน COBIT ผู้ตรวจสอบจะต้องพิจารณาข้อมูลเพิ่มเติมจาก FRAMEWORK อื่น ๆ เช่น มาตรฐาน ISO/IEC 27001, ISO/IEC 17799, ISO/IEC 13335, ISO/IEC 15408 และ ITIL (IT Infrastructure Library) ตลอดจนเครื่องมือต่าง ๆ ที่ใช้สำหรับบริหารจัดการระบบเทคโนโลยีสารสนเทศ เช่น PRINCE 2, PMBOX, TickIT และ TOGAF 8.1

**Independent Study Title** Information Technology Auditing by COBIT  
**Author** Paporn Piyayodilokchai  
**Independent Study Advisor** Assistant Professor Dr.Pranot Boonchai-Apisit  
**Department** Computer and Communication Technology  
**Academic Year** 2010

### ABSTRACT

249092

Independent study Information Technology Auditing by COBIT , the data is gathered about the information technology, risk of the information technology, damage from use of the information technology, the information technology auditing and COBIT FRAMEWORK to cover the COBIT FRAMEWORK as the guideline to prepare the audit program for information technology auditing based on the structure of the COBIT FRAMEWORK on the 4 main business processes (Domain) i.e. PO : Planning and Organization, AI : Acquisition and Implementation, DS : Delivery and Support, M : Monitoring.

The audit program for the information technology auditing by COBIT, the auditor of the information technology could use it as the tool on the audit, and the chief of the audit unit could use as the tool for review and supervision. The audit of the information technology could be done to cover the risk of the information technology of the organization and to achieve the objectives of audit. However, the details of the application in the procedures of the COBIT FRAMEWORK, the auditor must consider additional data from other framework i.e. ISO/IEC 27001, ISO/IEC 17799, ISO/IEC 13335, ISO/IEC 15408 and ITIL (IT Infrastructure Library) as well as tools used for management of the information technology i.e. PRINCE 2, PMBOX, TickIT and TOGAF 8.1.

## กิตติกรรมประกาศ

งานค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงได้ด้วยความช่วยเหลือจากบุคคลมากมายที่ขอกล่าวถึงด้วยความขอบพระคุณ

ผู้เขียนขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์ ซึ่งได้ให้คำแนะนำและเสียสละเวลาอันมีค่าของท่านรับเป็นอาจารย์ที่ปรึกษางานค้นคว้าอิสระ และได้กรุณาแนะนำความรู้และสิ่งที่เป็นประโยชน์อย่างอเนกประการ ในการช่วยปรับปรุงงานค้นคว้าอิสระฉบับนี้ ผู้เขียนขอขอบพระคุณ รองศาสตราจารย์ ดร.ณรงค์ มั่งคั่ง ประธานกรรมการสอบงานค้นคว้าอิสระ และ อาจารย์ ดร.ประศาสน์ จันทราทิพย์ กรรมการผู้ทรงคุณวุฒิ ที่ได้สละเวลามาเป็นคณะกรรมการสอบงานค้นคว้าอิสระ ตลอดจนให้ข้อคิดเห็นอันเป็นประโยชน์ ในการทำให้งานค้นคว้าอิสระฉบับนี้ มีคุณค่ามากยิ่งขึ้น

ผู้เขียนขอกราบขอบพระคุณคุณยายและคุณปู่คุณย่าของหลาน ๆ ซึ่งให้การสนับสนุนและให้กำลังใจแก่ผู้เขียนตลอดมา โดยเฉพาะอย่างยิ่งคุณย่าที่ช่วยกรุณาดูแลหลาน ๆ ในช่วงระยะเวลาที่ผู้เขียนทำการศึกษาและจัดทำงานค้นคว้าอิสระฉบับนี้

ผู้เขียนขอขอบพระคุณท่านอาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้แก่ผู้เขียนท้ายสุด ผู้เขียนขอขอบคุณนายสุชาติ ภิชัยดิถกชัย สามีผู้เขียน ที่ได้ให้การสนับสนุนและให้กำลังใจผู้เขียนในทุก ๆ ด้านมาโดยตลอด และช่วยดูแลบุตร ซึ่งทำให้ผู้เขียนสามารถทุ่มเทเวลาในการศึกษาและจัดทำงานค้นคว้าอิสระฉบับนี้

ผู้เขียนหวังเป็นอย่างยิ่งว่า งานค้นคว้าอิสระฉบับนี้ จะเป็นประโยชน์กับผู้ที่ต้องการศึกษาด้านการตรวจสอบระบบเทคโนโลยีสารสนเทศ และหากมีข้อผิดพลาดประการใดในงานค้นคว้าอิสระฉบับนี้ ผู้เขียนต้องกราบขออภัยเป็นอย่างสูงมา ณ ที่นี้ด้วย

ภาพร ภิชัยดิถกชัย

สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	๗
บทคัดย่อภาษาอังกฤษ.....	๙
กิตติกรรมประกาศ.....	๑
สารบัญ.....	ฉ
สารบัญตาราง.....	๗
สารบัญภาพ.....	๘
บทที่	
1. บทนำ.....	1
1.1 ที่มาและความสำคัญของปัญหา.....	1
1.2 วัตถุประสงค์ของการวิจัย.....	3
1.3 ขอบเขตของการวิจัย.....	3
1.4 ประโยชน์ที่คาดว่าจะได้รับ.....	3
2. แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง.....	4
2.1 องค์กรหรือหน่วยงานที่ตรวจสอบ.....	4
2.2 ระบบสารสนเทศ.....	5
2.3 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ.....	9
2.4 ความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ.....	11
2.5 การตรวจสอบระบบเทคโนโลยีสารสนเทศ.....	13
2.6 COBIT FRAMEWORK.....	18
2.7 การควบคุมระบบสารสนเทศ.....	40
2.8 งานวิจัยที่เกี่ยวข้อง.....	45
3. ระเบียบวิธีวิจัย.....	51
3.1 ขั้นตอนการดำเนินการวิจัย.....	51
3.2 อุปกรณ์และเครื่องมือที่ใช้ในการวิจัย.....	51
3.3 ระยะเวลาในการดำเนินการวิจัย.....	52

สารบัญ (ต่อ)

	หน้า
4. ผลการศึกษา.....	53
4.1 การศึกษาเกี่ยวกับการตรวจสอบสารสนเทศ.....	53
4.2 แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT.....	61
4.3 กรณีตัวอย่างการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT.....	108
5. สรุปผลการวิจัย.....	134
5.1 สรุปผลการวิจัย.....	134
5.2 อภิปรายผลการศึกษา.....	135
5.3 ข้อเสนอแนะ.....	136
บรรณานุกรม.....	137
ประวัติผู้เขียน.....	142

สารบัญตาราง

ตารางที่	หน้า
2.1 ประเภทของระบบสารสนเทศ.....	7
2.2 ความต้องการทางธุรกิจด้านสารสนเทศ.....	18
3.1 ระยะเวลาในการดำเนินการวิจัย.....	52
4.1 ระดับความสามารถของการควบคุมหรือระดับพัฒนาการของการควบคุม (Internal Control Capability Continuum).....	58
4.2 PO1c: การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (Define a Strategic IT Plan).....	62
4.3 PO2 : การกำหนดโครงสร้างด้านสารสนเทศ (Define the Information Architecture).....	63
4.4 PO3 : การกำหนดทิศทางด้านเทคโนโลยี (Determine Technological Direction). 64	64
4.5 PO4 : การจัดโครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศและความสัมพันธ์กับ หน่วยงานอื่น (Define the IT Organization and Relationships).....	65
4.6 PO5 : การจัดการด้านการลงทุนในเทคโนโลยีสารสนเทศ (Manage the IT Investment).....	66
4.7 PO6 : การสื่อสารเป้าหมายและทิศทางภายในองค์กร (Communicate Management Aims and Direction ).....	67
4.8 PO7 : การจัดการทรัพยากรบุคคล (Manage Human Resources).....	67
4.9 PO8 : การปฏิบัติตามข้อกำหนดขององค์กรภายนอก (Ensure Compliance with External Requirements).....	68
4.10 PO9 : การประเมินความเสี่ยง (Assess Risks).....	69
4.11 PO10 : การจัดการโครงการ (Manage Projects).....	70
4.12 PO11 : การจัดการคุณภาพ (Manage Quality).....	71
4.13 AI1 : การเลือกเทคโนโลยีมาใช้ในการปฏิบัติงาน (Identify Automated Solutions).....	74
4.14 AI2 : การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์ (Acquire and Maintain Application Software).....	75

## สารบัญตาราง(ต่อ)

ตารางที่	หน้า
4.15 AI3 : การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี (Acquire and Maintain Technology Infrastructure).....	77
4.16 AI4 : ระเบียบปฏิบัติในการพัฒนาและบำรุงรักษา (Develop and Maintain Procedures).....	78
4.17 AI5 : การติดตั้งและรับรองระบบ (Install and Accredite Systems).....	79
4.18 AI6: การจัดการการเปลี่ยนแปลง (Manage Changes).....	81
4.19 DS1 : การกำหนดและการจัดการระดับการให้บริการ (Define and Manage Service Levels).....	83
4.20 DS2 : การจัดการการใช้บริการจากบุคคลภายนอก (Manage Third-Party Services).....	84
4.21 DS3 : การจัดการด้านประสิทธิภาพและความสามารถ (Manage Performance and Capacity).....	85
4.22 DS4 : ความต่อเนื่องในการให้บริการ (Ensure Continuous Service).....	87
4.23 DS5 : การรักษาความปลอดภัยระบบ (Ensure Systems Security).....	90
4.24 DS6 : การกำหนดและจัดสรรต้นทุน (Identify and Allocate Costs).....	92
4.25 DS7 : การให้ความรู้และฝึกอบรมผู้ใช้งาน (Educate and Train Users).....	94
4.26 DS8 : การให้ความช่วยเหลือและคำแนะนำแก่ผู้ใช้ระบบงานในองค์กร (Assist and Advise Customers).....	94
4.27 DS9 : การจัดการรายละเอียดทรัพย์สิน (Manage the Configuration).....	96
4.28 DS10 : การจัดการปัญหาและเหตุการณ์ที่เกิดขึ้น (Manage Problems and Incidents).....	98
4.29 DS11 : การจัดการข้อมูล (Manage Data).....	99
4.30 DS12 : การจัดการด้านสิ่งอำนวยความสะดวก (Manage Facilities).....	101
4.31 DS13 : การจัดการด้านการปฏิบัติการ (Manage Operations).....	102
4.32 M1 : การติดตามกระบวนการทำงาน (Monitor the Processes).....	104
4.33 M2 : การประเมินความเพียงพอของการควบคุมภายใน (Assess Internal Control Adequacy).....	105

## สารบัญตาราง(ต่อ)

ตารางที่	หน้า
4.34 M3 : การรับรองความเป็นอิสระ (Obtain Independent Assurance).....	106
4.35 M4 : ความเป็นอิสระในการตรวจสอบ (Provide for Independent Audit).....	107
4.36 ตัวอย่างการบันทึกข้อมูลจากการตรวจสอบ.....	110

สารบัญภาพ

ภาพที่	หน้า
2.1 COBIT Cube.....	21
2.2 กรอบมาตรฐาน COBIT.....	23