

ระบบสนับสนุนการตรวจสอบการควบคุมภายในโดยใช้กรอบงานโคบิต



นายนพกฤษฎี อธิธิธีรเกียรติ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2550

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

A SYSTEM TO SUPPORT INTERNAL CONTROL AUDIT USING COBIT FRAMEWORK

Mr. Noppakit Itthiteerakriat

A Thesis Submitted in Partial Fulfillment of the Requirements  
for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2007

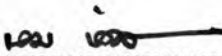
Copyright of Chulalongkorn University

500295

หัวข้อวิทยานิพนธ์                      ระบบสนับสนุนการตรวจสอบการควบคุมภายในโดยใช้กรอบงานโคบิต  
โดย    นายณพกฤษฎี อธิธิธีรเกียรติ  
สาขาวิชา                                    วิทยาศาสตร์คอมพิวเตอร์  
อาจารย์ที่ปรึกษา                          ผู้ช่วยศาสตราจารย์ ดร.ญาใจ ลิ้มปิยะกรณ์

---

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้หัวข้อวิทยานิพนธ์ฉบับนี้เป็น  
ส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาโทบริหารธุรกิจ


  
..... คนบดี คณะวิศวกรรมศาสตร์  
(รองศาสตราจารย์ ดร. บุญสม เลิศธีรวงค์)

คณะกรรมการสอบวิทยานิพนธ์

  
..... ประธานกรรมการ  
(ศาสตราจารย์ ดร.บุญเสริม กิจศิริกุล)

  
..... อาจารย์ที่ปรึกษา  
(ผู้ช่วยศาสตราจารย์ ดร.ญาใจ ลิ้มปิยะกรณ์)

  
..... กรรมการ  
(ผู้ช่วยศาสตราจารย์ ดร.เฉลิมเอก อินทนากรวินิต)

  
..... กรรมการ  
(อาจารย์ ดร.ภาสกร อภิรักษ์วรพินิต)

นพคุณฐิ อธิธิริเกียรติ : ระบบสนับสนุนการตรวจสอบการควบคุมภายในโดยใช้กรอบงานโคบิต (A SYSTEM TO SUPPORT INTERNAL CONTROL AUDIT USING COBIT FRAMEWORK) อ. ที่ปรึกษา : ผศ.ดร.ญาใจ ลิ้มปิยะกรณ์, 88 หน้า.

หลายองค์กรเริ่มตระหนักและให้ความสำคัญกับการตรวจสอบการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ซึ่งถือเป็นกระบวนการหนึ่งที่มีความสำคัญ ช่วยให้การดำเนินงานด้านไอทีภายในองค์กรให้เป็นไปตามวัตถุประสงค์หลักที่องค์กรได้กำหนดไว้ และช่วยลดความเสี่ยงที่เกิดจากช่องโหว่ต่างๆ ที่เกิดจากการนำเทคโนโลยีสารสนเทศเข้ามาใช้อำนวยความสะดวกการปฏิบัติงานขององค์กรอีกด้วย จากความสำคัญของกระบวนการดังกล่าว งานวิจัยนี้จึงได้ออกแบบกระบวนการการตรวจสอบการควบคุมภายในด้านไอทีที่ชัดเจนเข้าใจได้ง่าย โดยอ้างอิงจากโคบิต ซึ่งเป็นกรอบงานที่ได้รับการยอมรับแพร่หลายทั่วโลก รวมทั้งได้พัฒนาระบบอำนวยความสะดวกแก่ผู้ตรวจสอบเทคโนโลยีสารสนเทศ ให้สามารถปฏิบัติงานได้รวดเร็ว มีประสิทธิภาพ โดยระบบที่พัฒนาขึ้นมีหน้าที่การทำงานซึ่งครอบคลุมกระบวนการตรวจสอบ ได้แก่ การจัดการโครงการตรวจสอบ การวางแผนการตรวจสอบ การประเมินหัวข้อการควบคุมที่ใช้ในการตรวจสอบ การจัดการเอกสารการตรวจสอบ การจัดการประเด็นปัญหาที่ตรวจพบ การเรียกดูประวัติการตรวจสอบย้อนหลัง รวมถึงการจัดเก็บข้อมูลความเสี่ยงทั้งหมดภายในองค์กร ระบบที่พัฒนาขึ้นได้ถูกทดลองใช้โดยผู้ตรวจสอบเทคโนโลยีสารสนเทศของธนาคารพาณิชย์แห่งหนึ่ง ซึ่งใช้กรอบงานโคบิตสำหรับงานตรวจสอบการควบคุมภายในด้านไอทีของธนาคาร ผลการประเมินเป็นที่น่าพอใจ

ภาควิชา..... วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต..... *นพคุณฐิ อธิธิริเกียรติ*  
 สาขาวิชา.....วิทยาศาสตร์คอมพิวเตอร์.... ลายมือชื่ออาจารย์ที่ปรึกษา..... *al*  
 ปีการศึกษา 2550

# # 4971464121 : MAJOR COMPUTER SCIENCE

KEY WORD: INTERNAL CONTROL AUDIT / RISK ASSESSMENT / COBIT

NOPPAKIT ITTHITEERAKRIAT : A SYSTEM TO SUPPORT INTERNAL CONTROL AUDIT USING COBIT FRAMEWORK. THESIS ADVISOR : ASST. PROF. YACHAI LIMPIYAKORN, Ph.D., 88 pp.

Many organizations begin to be aware of the importance of Information Technology (IT) Internal Control Audit. IT Internal Control Audit is one of the essential processes that would enable IT operations to achieve an organization's objectives, in addition to mitigate any potential risks incurred from the vulnerability that are the consequences of deploying information technology to facilitate operations within an organization. This research, thus, designed a well-defined process of IT Internal Control Audit based on the worldclass CoBIT framework. Further, we developed a system to facilitate IT auditors for fast and efficient operations. The implemented system covers various audit processes including management of audit projects, audit planning, assessment of audit controls, management of audit documentation, issue handling, audit history listing, and organizational risk data storing. The system was evaluated by the IT Internal Control Audit of a particular commercial bank that uses CoBIT as the framework of its IT Internal Control Audit task. The evaluation results were satisfactory.

Department..... Computer Engineering.....Student's signature *Noppakit Itthiteerakriat*  
Field of study.....Computer Science.....Advisor's signature *Y. Limpiyakorn*  
Academic year....2007.....

## กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความอนุเคราะห์อย่างยิ่งของท่านผู้ช่วยศาสตราจารย์ ดร.ญาใจ ลิ้มปิยะภรณ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้สละเวลาให้ความรู้ให้คำปรึกษา ตรวจสอบ ให้คำแนะนำแนวทางการวิจัย และสนับสนุนเป็นอย่างดี จนทำให้การวิจัยในครั้งนี้สำเร็จออกมาด้วยดี

ขอขอบพระคุณ ศาสตราจารย์ ดร.บุญเสริม กิจศิริกุล ผู้ช่วยศาสตราจารย์ ดร.เฉลิมเอก อินทนากรวิวัฒน์ และอาจารย์ ดร.ภาสกร อภิรักษ์วรพิณิต กรรมการสอบวิทยานิพนธ์ ที่กรุณาเสียสละเวลา ให้คำแนะนำ ตรวจสอบ และแก้ไขวิทยานิพนธ์ฉบับนี้

ขอกราบขอบพระคุณ คุณพ่อ-คุณแม่ ที่ให้การสนับสนุนและเป็นกำลังใจที่ดีเสมอมา

ขอขอบคุณพี่ๆ บริษัทธนาคารกรุงศรีอยุธยา จำกัด ที่ให้โอกาส ให้คำปรึกษา และให้การสนับสนุนเป็นอย่างดี

ท้ายที่สุด ผู้วิจัยขอขอบคุณเพื่อนๆ ทุกๆ คน ที่คอยติดตามและให้กำลังใจ รวมถึงท่านอื่นๆ ที่มีได้กล่าวชื่อไว้ ณ ที่นี้ที่มีส่วนทำให้วิทยานิพนธ์สำเร็จได้ด้วยดี

## สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	ง
บทคัดย่อภาษาอังกฤษ.....	จ
กิตติกรรมประกาศ.....	ฉ
สารบัญ .....	ช
สารบัญภาพ.....	ฌ
สารบัญตาราง.....	ฎ
บทที่ 1 บทนำ.....	1
1.1 ความเป็นมาและความสำคัญของปัญหา.....	1
1.2 วัตถุประสงค์ของการวิจัย.....	2
1.3 ขอบเขตของการวิจัย .....	3
1.4 ขั้นตอนและวิธีดำเนินการวิจัย .....	3
1.5 ประโยชน์ที่คาดว่าจะได้รับ.....	4
1.6 ลำดับการจัดเรียงเนื้อหาในวิทยานิพนธ์.....	4
1.7 ผลงานที่ตีพิมพ์จากวิทยานิพนธ์.....	4
บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง.....	5
2.1 ทฤษฎีที่เกี่ยวข้อง .....	5
2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง .....	11
บทที่ 3 การออกแบบขั้นตอนการดำเนินงาน .....	12
3.1 การวางแผนการตรวจสอบประจำปี (Project Planning) .....	12
3.2 การประเมินความเสี่ยง (Risk Assessment) .....	12
3.3 การจัดการเอกสารที่ใช้ในการตรวจสอบ (Audit Document Management) .....	13
3.4 ประวัติการตรวจสอบของศูนย์สารสนเทศ (Audit History) .....	13
3.5 การจัดการประเด็นปัญหา (Issue Management) .....	14
3.6 การระบุความเสี่ยง (Risk Database).....	14
บทที่ 4 การพัฒนาระบบสนับสนุน .....	18
4.1 ความต้องการด้านหน้าที่ของระบบสนับสนุน.....	18
4.2 การออกแบบระบบสนับสนุน.....	20
บทที่ 5 การทดสอบระบบสนับสนุน.....	31

	๗
5.1 ขั้นตอนปฏิบัติและผลการทดสอบระบบสนับสนุนด้วยกรณีทดสอบ .....	31
5.2 สรุปผลการทดสอบ .....	34
บทที่ 6 สรุปผลการวิจัยและข้อเสนอแนะ .....	35
6.1 สรุปผลการวิจัย .....	35
6.2 ข้อจำกัด .....	35
6.3 แนวทางการวิจัยต่อ .....	35
รายการอ้างอิง .....	36
ภาคผนวก .....	37
ภาคผนวก ก. คำอธิบายยูสเคส .....	38
ภาคผนวก ข. พจนานุกรมข้อมูลของระบบฐานข้อมูล .....	53
ภาคผนวก ค. ตัวอย่างหน้าจอของส่วนต่อประสานผู้ใช้ .....	67
ประวัติผู้เขียนวิทยานิพนธ์ .....	88



## สารบัญภาพ

	หน้า
รูปที่ 1 ภาพรวมของกรอบงานโคบิต .....	9
รูปที่ 2 กรอบงานการวิเคราะห์ความเสี่ยง [4] .....	10
รูปที่ 3 การนิยามความเสี่ยงตามวิธีของ RISKIT [6] .....	11
รูปที่ 4 แผนภาพกิจกรรมของกระบวนการตรวจสอบการควบคุมภายใน .....	16
รูปที่ 5 แผนภาพกิจกรรมการตรวจสอบติดตามการแก้ไขข้อบกพร่อง .....	17
รูปที่ 6 แผนภาพยุทธศาสตร์การจัดฝึกอบรมองค์กร .....	20
รูปที่ 7 แผนภาพอีอาร์ของฐานข้อมูล .....	21
รูปที่ 8 ตัวอย่างหน้าจอการเข้าสู่ระบบ .....	67
รูปที่ 9 ตัวอย่างหน้าจอการทำงานหลัก .....	67
รูปที่ 10 ตัวอย่างหน้าจอการสร้างตรงการตรวจสอบ .....	68
รูปที่ 11 ตัวอย่างหน้าจอรายละเอียดแผนงาน .....	68
รูปที่ 12 ตัวอย่างหน้าจอการประเมินแผนงานตรวจสอบ .....	69
รูปที่ 13 ตัวอย่างหน้าจอผลการประเมินแผนงานตรวจสอบ .....	69
รูปที่ 14 ตัวอย่างหน้าจอการใส่รายละเอียดของแผนงานตรวจสอบ .....	70
รูปที่ 15 ตัวอย่างหน้าจอการกำหนดรายชื่อผู้ตรวจสอบ .....	70
รูปที่ 16 ตัวอย่างหน้าจอการแสดงการซ้ำกันของผู้ตรวจสอบ .....	71
รูปที่ 17 ตัวอย่างหน้าจอการวางแผนงานตรวจสอบ .....	71
รูปที่ 18 ตัวอย่างหน้าจอการเลือกสูตรการประเมินหัวข้อการควบคุม .....	72
รูปที่ 19 ตัวอย่างหน้าจอแสดงผลการประเมินหัวข้อการควบคุม .....	72
รูปที่ 20 ตัวอย่างหน้าจอการกำหนดบทบาทของผู้ตรวจสอบ .....	73
รูปที่ 21 ตัวอย่างหน้าจอการกำหนดหัวข้อการควบคุมให้ผู้ตรวจสอบ .....	73
รูปที่ 22 ตัวอย่างหน้าจอการเข้าถึงแผนงานตรวจสอบ .....	74
รูปที่ 23 ตัวอย่างหน้าจอการแสดงรายละเอียดหัวข้อการควบคุมที่ได้รับมอบหมาย .....	74
รูปที่ 24 ตัวอย่างหน้าจอการ ดาวโหลด เอกสารการตรวจสอบ .....	75
รูปที่ 25 ตัวอย่างหน้าจอการ อัปโหลด เอกสารการตรวจสอบ .....	75
รูปที่ 26 ตัวอย่างหน้าจอแสดงเงื่อนไขที่ใช้ในการค้นหาประเด็นปัญหา .....	76

รูปที่ 27 ตัวอย่างหน้าจอบการแสดงรายละเอียดการค้นหาประเด็นปัญหา.....	76
รูปที่ 28 ตัวอย่างหน้าจอบการแสดงรายชื่อของประเด็นปัญหาที่ค้นหา.....	77
รูปที่ 29 ตัวอย่างหน้าจอบการเพิ่มละเอียดของประเด็นปัญหาใหม่.....	77
รูปที่ 30 ตัวอย่างหน้าจอบการค้นหาประเด็นปัญหาที่ต้องการแก้ไข.....	78
รูปที่ 31 ตัวอย่างหน้าจอบการแสดงรายละเอียดของเอกสารการตรวจสอบ.....	78
รูปที่ 32 ตัวอย่างหน้าจอบการแสดงรายชื่อความเสี่ยงแบ่งตามประเภทความเสี่ยง.....	79
รูปที่ 33 ตัวอย่างหน้าจอบการแสดงรายละเอียดข้อมูลความเสี่ยง.....	79
รูปที่ 34 ตัวอย่างหน้าจอบการแสดงข้อมูลความเสี่ยง.....	80
รูปที่ 35 ตัวอย่างหน้าจอบการหลักของการกำหนดค่าข้อมูล.....	80
รูปที่ 36 ตัวอย่างหน้าจอบข้อมูลหัวข้อการควบคุมตามกรอบงานโคบิต.....	81
รูปที่ 37 ตัวอย่างหน้าจอบข้อมูลเป้าหมายทางธุรกิจ.....	81
รูปที่ 38 ตัวอย่างหน้าจอบข้อมูลงานตรวจสอบ.....	82
รูปที่ 39 ตัวอย่างหน้าจอบข้อมูลประเภทงานตรวจสอบ.....	82
รูปที่ 40 ตัวอย่างหน้าจอบข้อมูลผู้ตรวจสอบ.....	83
รูปที่ 41 ตัวอย่างหน้าจอบข้อมูลตำแหน่งงานของผู้ตรวจสอบ.....	83
รูปที่ 42 ตัวอย่างหน้าจอบข้อมูลความสามารถของผู้ตรวจสอบ.....	84
รูปที่ 43 ตัวอย่างหน้าจอบข้อมูลผู้รับผิดชอบในการสั่งการ.....	84
รูปที่ 44 ตัวอย่างหน้าจอบข้อมูลผู้รับผิดชอบในการดำเนินการ.....	85
รูปที่ 45 ตัวอย่างหน้าจอบข้อมูลฝ่ายงาน.....	85
รูปที่ 46 ตัวอย่างหน้าจอบข้อมูลประเภทความเสี่ยง.....	86
รูปที่ 47 ตัวอย่างหน้าจอบข้อมูลความสูญเสียทางธุรกิจ.....	86
รูปที่ 48 ตัวอย่างหน้าจอบข้อมูลโอกาสเกิดความเสี่ยง.....	87
รูปที่ 49 ตัวอย่างหน้าจอบข้อมูลผู้มีส่วนเกี่ยวข้อง.....	87

## สารบัญตาราง

	หน้า
ตารางที่ 1 ความต้องการด้านหน้าที่ .....	18
ตารางที่ 2 การทดสอบตามความต้องการด้านหน้าที่.....	31
ตารางที่ 3 คำอธิบายยูสเคสจัดการโครงการตรวจสอบ .....	38
ตารางที่ 4 คำอธิบายยูสเคสอนุมัติโครงการตรวจสอบ .....	39
ตารางที่ 5 คำอธิบายยูสเคสเปิดแผนงานตรวจสอบ .....	40
ตารางที่ 6 คำอธิบายยูสเคสปิดแผนงานตรวจสอบ.....	41
ตารางที่ 7 คำอธิบายยูสเคสปิดโครงการตรวจสอบ.....	42
ตารางที่ 8 คำอธิบายยูสเคสวางแผนการตรวจสอบ .....	43
ตารางที่ 9 คำอธิบายยูสเคสประเมินแผนงานตรวจสอบ .....	44
ตารางที่ 10 คำอธิบายยูสเคสประเมินหัวข้อการควบคุม .....	45
ตารางที่ 11 คำอธิบายยูสเคสกำหนดบทบาทผู้ตรวจสอบ.....	45
ตารางที่ 12 คำอธิบายยูสเคสกำหนดหัวข้อการควบคุมให้ผู้ตรวจสอบ .....	46
ตารางที่ 13 คำอธิบายยูสเคสจัดการเอกสารการตรวจสอบ .....	47
ตารางที่ 14 คำอธิบายยูสเคสตรวจสอบรหัสผ่าน.....	48
ตารางที่ 15 คำอธิบายยูสเคสจัดการประเด็นปัญหา .....	48
ตารางที่ 16 คำอธิบายยูสเคสเรียกดูประวัติการตรวจสอบ .....	49
ตารางที่ 17 คำอธิบายยูสเคสจัดการข้อมูลความเสี่ยง .....	50
ตารางที่ 18 คำอธิบายยูสเคสจัดการผู้ใช้งานระบบ .....	51
ตารางที่ 19 ตาราง TB_ACTIONOWNER.....	53
ตารางที่ 20 ตาราง TB_AUASSESSMENT.....	53
ตารางที่ 21 ตาราง TB_AUDITOR.....	54
ตารางที่ 22 ตาราง TB_AUDITORINPROJECT .....	55
ตารางที่ 23 ตาราง TB_AUDITORSKILL .....	55
ตารางที่ 24 ตาราง TB_AUDITUNIVERSE .....	56
ตารางที่ 25 ตาราง TB_AUDITUTYPE.....	57
ตารางที่ 26 ตาราง TB_CONTROL .....	57

ตารางที่ 27 ตาราง TB_CONTROLASSESSMENT .....	58
ตารางที่ 28 ตาราง TB_CONTROLINPROJECT .....	58
ตารางที่ 29 ตาราง TB_DEPARTMENT .....	59
ตารางที่ 30 ตาราง TB_GOAL.....	59
ตารางที่ 31 ตาราง TB_HISTORYTREE .....	60
ตารางที่ 32 ตาราง TB_ISSUEDETAIL .....	60
ตารางที่ 33 ตาราง TB_ISSUEOWNER .....	61
ตารางที่ 34 ตาราง TB_JOBTITLE.....	61
ตารางที่ 35 ตาราง TB_LOSS.....	62
ตารางที่ 36 ตาราง TB_PROBABILITY .....	62
ตารางที่ 37 ตาราง TB_PROJECTMASTER .....	63
ตารางที่ 38 ตาราง TB_PROJECTDETAIL .....	63
ตารางที่ 39 ตาราง TB_RISK.....	64
ตารางที่ 40 ตาราง TB_RISKTYPE .....	65
ตารางที่ 41 ตาราง TB_STAKEHOLDER .....	65
ตารางที่ 42 ตาราง TB_USER.....	65