บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในยุค ICT ทุกวันนี้นั้น ความจำเป็นในการใช้งานระบบสารสนเทศเป็นเรื่องสำคัญของทุกองค์กร เรียกได้ว่าระบบคอมพิวเตอร์ได้ถูกนำมาใช้ในการประมวลผล, การนำเสนอข้อมูล และอื่นๆ อีกมากมาย จนพนักงานในองค์กรต้องใช้งานคอมพิวเตอร์ในวันทำงานแทบทุกวันอย่างหลีกเลี่ยงไม่ได้

จากการที่องค์กรนำระบบสารสนเทศมาใช้ในชีวิตประจำวันของการทำงาน จึงมีความจำเป็นที่ต้องมีฝ่ายหรือบุคลากรที่จะมาตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology : IT) ซึ่งมักเรียกบุคลากรเหล่านี้ว่า "IT Auditor" หรือ "IS Auditor" ที่ย่อมาจาก “Information Systems Audit” โดยทั่วไปแล้วจะมีทั้ง Internal Audit (ฝ่ายตรวจสอบภายในองค์กรเอง) และ External Audit (ผู้ตรวจสอบที่มาจากองค์กรภายนอกที่เชื่อถือได้มาตรวจสอบองค์กรอีกที)

IT Audit เป็นคำที่มีความหมายค่อนข้างกว้าง ครอบคลุมการตรวจสอบประเภทต่างๆ หลายประเภท เช่น

- การตรวจสอบกระบวนการด้านเทคโนโลยีสารสนเทศ (IT Process Auditing) ซึ่งครอบคลุมตั้งแต่การวางแผนด้านเทคโนโลยีสารสนเทศ จนถึงการตรวจสอบและติดตามกิจกรรมต่างๆ ด้านเทคโนโลยีสารสนเทศ
- การตรวจสอบด้านเทคนิคของระบบสารสนเทศ (Technical Information Systems Auditing) ได้แก่ การตรวจสอบความปลอดภัย และการควบคุมโครงสร้าง หรือองค์ประกอบพื้นฐานของระบบสารสนเทศ (Information Systems Infrastructure) เช่น
  - ระบบสื่อสารข้อมูลและระบบโครงข่าย (Data Communications and Network Systems)
  - ระบบปฏิบัติการ (Operating Systems)
  - ระบบจัดการฐานข้อมูล (Database Management Systems)

- การตรวจสอบระบบงาน (Application Information Systems Auditing)
- การตรวจสอบการพัฒนาระบบ (Systems Development Auditing)
- การตรวจสอบการนำระบบมาใช้งานจริง (Systems Implementation Auditing)
- การตรวจสอบการปฏิบัติตามนโยบายรักษาความปลอดภัยระบบสารสนเทศของกิจการ กฎระเบียบ หรือมาตรฐานที่กำหนดไว้ (Compliance Information Systems Auditing)

ในการทำ IT Audit ใน “มุมของผู้สอบบัญชี” จะเน้นการทำ IT Audit เพื่อพิจารณาถึงความเพียงพอของการควบคุมด้านเทคโนโลยีสารสนเทศที่องค์กรกำหนดไว้ และการปฏิบัติตามการควบคุมนั้นเพื่อให้มั่นใจในความถูกต้อง น่าเชื่อถือของข้อมูลที่แสดงในงบการเงิน หรือหลักฐานที่ใช้ในการตรวจสอบ

สำหรับการทำ IT Audit ใน “มุมของผู้บริหาร” ไม่ควรเน้นเฉพาะการตรวจสอบการควบคุมสำหรับระบบเทคโนโลยีสารสนเทศที่องค์กรกำหนดไว้ เพื่อให้มั่นใจในความถูกต้องน่าเชื่อถือของข้อมูลที่แสดงในงบการเงิน หรือหลักฐานที่ใช้ในการตรวจสอบเท่านั้น แต่ควรจะครอบคลุมการตรวจสอบความเพียงพอและเหมาะสมของการรักษาความปลอดภัย และการควบคุมสำหรับระบบเทคโนโลยีสารสนเทศที่องค์กรกำหนดไว้ เพื่อให้มั่นใจว่าองค์กรจะสามารถบรรลุวัตถุประสงค์ทางธุรกิจขององค์กรที่กำหนดไว้จากการใช้ระบบเทคโนโลยีสารสนเทศนั้นด้วย

องค์กรที่นำมาเป็นกรณีศึกษาในงานวิจัยครั้งนี้ เป็นองค์กรที่ประกอบธุรกิจทางการเงินด้านบัตรเครดิต และการให้สินเชื่อบุคคลที่ไม่ใช่สถาบันการเงิน (Non-bank) ที่มีการลงทุนด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนธุรกิจขององค์กรด้วยการ “Outsource” การพัฒนาระบบงานคอมพิวเตอร์และเทคโนโลยีสารสนเทศถูกดำเนินการโดยบริษัทภายนอก (Outsource) หลายรายคุณภาพและประสิทธิภาพของ Outsource หรือความซ้ำซ้อนและความหลากหลายของระบบงานอาจทำให้การปฏิบัติงานตามกระบวนการตรวจสอบระบบสารสนเทศที่กำหนดไว้ขององค์กร อาจพบปัญหาและอุปสรรคหลายประการที่จำเป็นจะต้องควบคุมความเสี่ยง อันเนื่องมาจากการเลือกใช้งานระบบเทคโนโลยีสารสนเทศนั้น

การควบคุมภายในซึ่งถือเป็นปัจจัยที่สำคัญมากอย่างหนึ่งของการดำเนินธุรกิจ เป็นองค์ประกอบหนึ่งของการกำกับดูแลกิจการที่ดี (Good Corporate Governance) โดย “Best Practices” หรือมาตรฐานที่ควรนำมาเป็นแนวทางในการเตรียมระบบสารสนเทศขององค์กรให้

พร้อมเข้าสู่ยุค IT Governance ที่นิยมใช้กันได้แก่ มาตรฐาน ISO / IEC17799, COBIT และ ITIL เป็นต้น

ดังนั้น เพื่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผล (Reasonable Assurance) ว่าองค์กรดำเนินงานอย่างมีประสิทธิภาพ และประสิทธิผล สามารถบรรลุเป้าหมายขององค์กร จึงมีความจำเป็นที่จะต้องนำมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้เพื่อความปลอดภัยขององค์กรและเพื่อให้สอดคล้องกับยุคของไอทีภิบาล (IT Governance) มุ่งสู่การเป็นบรรษัทภิบาล (Good Corporate Governance)

มาตรฐาน COBIT (Control Objectives for Information and Related Technology) มีจุดประสงค์ในการสร้างความมั่นใจว่า การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศนั้นสอดคล้องกับวัตถุประสงค์เชิงธุรกิจขององค์กร (Business Objectives) เพื่อให้เกิดการใช้ทรัพยากรอย่างมีประสิทธิผลอันจะส่งประโยชน์สูงสุดแก่องค์กร ช่วยให้เกิดความสมดุลระหว่างความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) และผลตอบแทนของการลงทุนในระบบสารสนเทศ (IT Return on Investment : IT ROI)

มาตรฐาน COBIT นั้นมีพื้นฐานมาจาก Framework ชั้นนำต่างๆ มากมาย ได้แก่ The Software Engineering Institute's Capability Maturity Model (CMM), ISO9000 และ The Information Technology Infrastructure Library (ITIL) ของประเทศอังกฤษ อย่างไรก็ตาม มาตรฐาน COBIT ก็ยังขาดในส่วนของ Guideline เพื่อใช้ในทางปฏิบัติ เนื่องจากมาตรฐาน COBIT เป็น Framework ที่เน้นในเรื่องของการควบคุม (Control) เป็นหลัก โดยมุ่งประเด็นในการบอกว่าองค์กรต้องการอะไรบ้าง (What) แต่ไม่มีรายละเอียดในแง่ของวิธีการที่นำไปสู่จุดนั้น (How) ซึ่งเหมาะกับผู้ตรวจสอบระบบสารสนเทศที่ต้องการนำมาตรฐาน COBIT มาใช้เพื่อทำเป็น Check Lists หรือ Audit Program

ปัจจุบันแนวคิดของมาตรฐาน COBIT กำลังเป็นที่นิยมในกลุ่มธุรกิจด้านการเงินและการธนาคาร ตัวอย่างเช่น ธนาคารแห่งประเทศไทย (ธปท.) และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ที่นำมาตรฐาน COBIT มาเป็นแนวทางในการออกข้อกำหนด และกฎข้อบังคับต่างๆ ที่ธนาคารพาณิชย์และบริษัทหลักทรัพย์ควรนำมาปฏิบัติ โดยขณะนี้ได้ออกประกาศเรื่องการควบคุมการปฏิบัติงานและแนวทางปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและการให้บริการการเงินทางอิเล็กทรอนิกส์ เพื่อเป็นแนวทางให้กับธนาคารพาณิชย์และบริษัทหลักทรัพย์ต่างๆ ในประเทศไทยแล้ว

1.2 วัตถุประสงค์งานวิจัย

1. เพื่อศึกษาแนวทางปฏิบัติการตรวจสอบระบบสารสนเทศตามมาตรฐาน COBIT (COBIT Framework)

2. เพื่อวิเคราะห์ประเด็นปัญหา และอุปสรรคของกระบวนการตรวจสอบระบบสารสนเทศ (IT Audit Process) ขององค์กรที่นำมาเป็นกรณีศึกษานำไปปฏิบัติงานอยู่ในปัจจุบัน

3. เพื่อประยุกต์มาตรฐาน COBIT มาใช้ขจัดปัญหาและอุปสรรคของกระบวนการตรวจสอบระบบสารสนเทศที่มีอยู่ให้เหมาะสม

1.3 ขอบเขตงานวิจัย

เพื่อให้งานวิจัยมีความชัดเจน ผู้วิจัยจึงได้กำหนดขอบเขตของการวิจัย ดังต่อไปนี้

1.3.1 ขอบเขตด้านเนื้อหา

งานวิจัยฉบับนี้เป็นการศึกษาปรับปรุงกระบวนการในการตรวจสอบระบบสารสนเทศเฉพาะการตรวจรับระบบงานในส่วนของการบริหารโครงการเทคโนโลยีสารสนเทศ (IT Project Management) โดยเริ่มจากการศึกษาแนวทางปฏิบัติการตรวจสอบระบบสารสนเทศ (IT Audit Methodologies) ตามมาตรฐาน COBIT และวิเคราะห์ประเด็นปัญหาและอุปสรรคของกระบวนการตรวจสอบระบบสารสนเทศ (IT Audit Process) ขององค์กรที่นำมาเป็นกรณีศึกษานำไปปฏิบัติงานอยู่ในปัจจุบัน แล้วนำมาตรฐาน COBIT มาประยุกต์ใช้ เพื่อขจัดปัญหาและอุปสรรคของกระบวนการตรวจสอบระบบสารสนเทศที่มีอยู่ให้เหมาะสม

1.3.2 ขอบเขตด้านระยะเวลา

งานวิจัยฉบับนี้ใช้ระยะเวลาในการศึกษา 11 เดือน ตั้งแต่เดือนพฤศจิกายน 2548 ถึงเดือนกันยายน 2549

1.4 ระเบียบวิธีวิจัย

งานวิจัยฉบับนี้เป็นการวิจัยในเชิงคุณภาพ (Qualitative Research) โดยทำการวิจัยทั้งแบบปฐมภูมิ (Primary Data) และแบบทุติยภูมิ (Secondary Data) ด้วยวิธีต่างๆ ดังนี้

1. รวบรวมข้อมูลที่เกี่ยวข้องกับมาตรฐาน COBIT จากเอกสารและแหล่งข้อมูลต่างๆ
2. วิเคราะห์ประเด็นปัญหาในกระบวนการตรวจสอบระบบสารสนเทศ (IT Audit Process) ขององค์กรที่นำมาเป็นกรณีศึกษานำไปปฏิบัติงานอยู่ในปัจจุบัน
3. การสัมภาษณ์ผู้เชี่ยวชาญด้านการตรวจสอบระบบสารสนเทศที่มีความรู้ ความเข้าใจในมาตรฐาน COBIT เพื่อสอบถามแนวทางปฏิบัติการตรวจสอบระบบสารสนเทศตามมาตรฐาน COBIT รวมทั้งปัจจัยสนับสนุน ปัญหาและอุปสรรคของการนำมาตรฐาน COBIT มาใช้ในองค์กร
4. การสัมภาษณ์ผู้บริหาร และผู้เกี่ยวข้องในกระบวนการตรวจสอบระบบสารสนเทศขององค์กรที่นำมาเป็นกรณีศึกษา เพื่อให้ทราบถึงปัญหาและอุปสรรค รวมทั้งความคิดเห็นต่อแนวทางในการขจัดปัญหาและอุปสรรค
5. วิเคราะห์ข้อมูลปฐมภูมิ (Primary Data) และข้อมูลทุติยภูมิ (Secondary Data) ที่ได้จากการรวบรวม มาประยุกต์ปรับปรุงกระบวนการตรวจสอบระบบสารสนเทศให้เหมาะสม

1.5 แผนงานวิจัย

1.5.1 รายละเอียดงานวิจัย

ในการดำเนินงานวิจัยครั้งนี้ สามารถกำหนดเป็นกิจกรรมในแต่ละขั้นตอนของการศึกษา พร้อมทั้งระบุขอบเขตของระยะเวลา เพื่อเป็นกรอบในการดำเนินงานวิจัย ดังตารางที่ 1.1

ตารางที่ 1.1

ขั้นตอน กิจกรรม และระยะเวลาในการดำเนินงานวิจัย

ขั้นตอน	กิจกรรม	ระยะเวลา
1	<u>เตรียมหัวข้องานค้นคว้าอิสระ</u>	<u>7 พ.ย. – 31 ธ.ค. 48</u>
	1.1 ศึกษาแนวความคิดและข้อมูลที่เกี่ยวข้อง	7 – 19 พ.ย. 48
	1.2 บูรณาการองค์ความรู้และแนวคิดในการวิจัย	20 พ.ย. – 9 ธ.ค. 48
	1.3 เขียนเค้าโครงงานวิจัย	10 – 16 ธ.ค. 48
	1.4 เสนอหัวข้อและเค้าโครงงานวิจัยให้อาจารย์ที่ปรึกษาพิจารณาอนุมัติ	17 – 24 ธ.ค. 48
	1.5 เสนอหัวข้อและเค้าโครงงานวิจัยให้กับวิทยาลัยฯ	25 – 31 ธ.ค. 48
2	<u>วางแผนงานวิจัย</u>	<u>1 ม.ค. – 10 ก.พ. 49</u>
	2.1 พัฒนาแนวคิดและรูปแบบงานวิจัย	1 – 20 ม.ค. 49
	2.2 จัดทำรายละเอียดขั้นตอนและระเบียบวิธีวิจัย	21 ม.ค. – 10 ก.พ. 49
3	<u>เสนอรายงานวิจัยส่วนแรก</u>	<u>11 ก.พ. – 16 พ.ค. 49</u>
	3.1 จัดทำรายงานวิจัยฉบับร่างส่วนแรก 3 บท	11 ก.พ. – 10 มี.ค. 49
	3.2 เสนอรายงานวิจัยฉบับร่างส่วนแรกให้อาจารย์ที่ปรึกษาพิจารณา	11 มี.ค. – 2 เม.ย. 49
	3.3 สอบวัดผลความก้าวหน้า (Progress Examination)	3 เม.ย. – 6 พ.ค. 49
	3.4 ปรับปรุง / แก้ไขรายงานวิจัยฉบับร่างส่วนแรกตามคำแนะนำของคณะกรรมการสอบงานวิจัย	7 – 16 พ.ค. 49
4	<u>ดำเนินงานวิจัย</u>	<u>17 พ.ค. – 31 ก.ค. 49</u>
	4.1 การเก็บรวบรวมข้อมูลทุติยภูมิจากเอกสาร หนังสือ บทความวิชาการ และสิ่งพิมพ์อื่นๆ ที่เกี่ยวข้อง ตลอดจนข้อมูลที่ได้จากแหล่งข้อมูลทางอินเทอร์เน็ต	17 พ.ค. – 30 มิ.ย. 49
	4.2 การเก็บรวบรวมข้อมูลปฐมภูมิจากการสัมภาษณ์ผู้เชี่ยวชาญ, ผู้บริหารสายงานตรวจสอบภายในและผู้เกี่ยวข้องขององค์กรที่นำมาเป็นกรณีศึกษา	1 – 31 ก.ค. 49

ตารางที่ 1.1 (ต่อ)

ขั้นตอน กิจกรรม และระยะเวลาในการดำเนินงานวิจัย

ขั้นตอน	กิจกรรม	ระยะเวลา
5	<u>สรุปผลงานวิจัย</u>	<u>1 ส.ค. – 15 ก.ย. 49</u>
	5.1 วิเคราะห์ข้อมูลการวิจัย	1 – 31 ส.ค. 49
	5.2 สรุปผลการวิจัย	1 – 15 ก.ย. 49
6	<u>เสนอรายงานวิจัยฉบับสมบูรณ์</u>	<u>16 ก.ย. 49 – 14 ม.ค. 50</u>
	6.1 จัดทำรายงานวิจัยฉบับสมบูรณ์	16 ก.ย. – 8 ต.ค. 49
	6.2 เสนอรายงานวิจัยฉบับสมบูรณ์ให้อาจารย์ที่ปรึกษาพิจารณา	9 – 31 ต.ค. 49
	6.3 สอบ Defense งานวิจัย	1 – 30 พ.ย. 49
	6.4 ปรับปรุง / แก้ไขรายงานวิจัยฉบับสมบูรณ์ตามคำแนะนำของคณะกรรมการสอบงานวิจัย	1 ธ.ค. 49 – 13 ม.ค. 50
	6.5 ส่งรายงานวิจัยฉบับสมบูรณ์ให้กับวิทยาลัยฯ	14 ม.ค. 50

1.5.2 <u>ระยะเวลาในการทำงานวิจัย</u>

แผนงานวิจัยมีระยะเวลาทั้งสิ้น 11 เดือน 2 ภาคเรียนปกติ คือ ภาคเรียนที่ 2/2548 และภาคเรียนที่ 1/2549 โดยเริ่มตั้งแต่วันที่ 7 พฤศจิกายน 2548 ถึงวันที่ 30 กันยายน 2549 ซึ่งระยะเวลาของแต่ละขั้นตอนการดำเนินงานวิจัยแสดง ดังตารางที่ 1.2

ตารางที่ 1.2

แผนการดำเนินงานวิจัย

ขั้นตอน	กิจกรรม	พ.ย. 48				ธ.ค. 48				ม.ค. 49				ก.พ. 49				มี.ค. 49				เม.ย. 49				พ.ค. 49				มิ.ย. 49				ก.ค. 49				ส.ค. 49				ก.ย. 49			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	เตรียมหัวข้องานค้นคว้าอิสระ																																											
2	วางแผนงานวิจัย																																											
3	เสนอรายงานวิจัยส่วนแรก																																											
4	ดำเนินงานวิจัย																																											
5	สรุปผลการวิจัย																																											
6	เสนอรายงานวิจัยฉบับสมบูรณ์																																											

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ผู้ศึกษาหรือผู้วิจัยสามารถนำผลการศึกษาที่ได้มาเป็นแนวทางในการขจัดปัญหาและอุปสรรคของกระบวนการตรวจสอบระบบสารสนเทศ เฉพาะการตรวจรับระบบงานในส่วนของการบริหารโครงการเทคโนโลยีสารสนเทศ (IT Project Management) ขององค์กรที่นำมาเป็นกรณีศึกษาประสบอยู่ในปัจจุบันให้เหมาะสม

2. ผู้สนใจหรือผู้เริ่มทำงานตรวจสอบระบบสารสนเทศสามารถทราบถึงแนวคิดของการตรวจสอบระบบสารสนเทศตามมาตรฐาน COBIT และสามารถนำมาตรฐาน COBIT มาประยุกต์ใช้กับการปฏิบัติงานจริง

3. ผู้บริหารสามารถใช้ประโยชน์จากการค้นคว้านี้ ไปใช้ในการประเมินประสิทธิภาพการตรวจสอบระบบสารสนเทศขององค์กร

1.7 นิยามศัพท์ (เฉพาะที่ใช้ในงานวิจัย)

1. การบริหารโครงการ (Project Management) หมายถึง กระบวนการในการกำหนด วางแผน ชี้แนะ ติดตาม และควบคุมโครงการพัฒนาระบบให้สามารถดำเนินการได้ตามระยะเวลาและงบประมาณที่กำหนดไว้ได้

2. เจ้าของโครงการ (Project Owner) คือ หน่วยงานที่จัดตั้งโครงการ และให้การสนับสนุนด้านการเงินในการดำเนินการพัฒนาระบบ

3. ผู้บริหารโครงการ (Project Manager) คือ บุคคลที่คอยดูแล ให้คำแนะนำ ควบคุม และติดตามผลการดำเนินงานของโครงการให้เป็นไปตามแผนงานที่กำหนดขึ้น

4. เจ้าของระบบงานและข้อมูล (Application / Data Owner) คือ หน่วยงานที่มีหน้าที่รับผิดชอบ และมีอำนาจตัดสินใจเกี่ยวกับการใช้ระบบงาน หรือข้อมูล

5. Test Scenario คือ เงื่อนไขการทดสอบโปรแกรมระบบงานที่แต่ละหน่วยงานผู้ใช้ระบบต้องร่วมทดสอบ

5. User Acceptance Test Script คือ เอกสารที่จัดทำขึ้นเพื่อแสดงรายละเอียดของการทดสอบระบบงาน ผลการทดสอบที่คาดหวัง และผลการทดสอบที่ได้รับ

6. UAT Summary คือ เอกสารที่จัดทำขึ้นเพื่อสรุปเงื่อนไขการทดสอบระบบงาน ผลการทดสอบที่คาดหวัง และผลการทดสอบที่ได้รับ

7. UAT Sign-off คือ เอกสารที่จัดทำขึ้นเพื่อแสดงว่าโปรแกรมระบบงานบนระบบทดสอบได้ผ่านการตรวจรับจากแต่ละหน่วยงานผู้ใช้ระบบที่ร่วมทดสอบ

8. System Live Request คือ เอกสารที่จัดทำขึ้นเพื่อขออนุมัตินำโปรแกรมระบบงานไปใช้จริง