บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ในโลกปัจจุบัน เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานขององค์กร ทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลระบบงานสำคัญต่าง ๆ ซึ่งหากุเป็นธุรกิจรับประกันวินาศภัยจะมีการนำเทคโนโลยีสารสนเทศมาใช้สำหรับการประมวลผลระบบงานที่เกี่ยวกับการรับประกันภัย การรับชำระหนี้ การจ่ายค่าสินไหมทดแทน การบริหารจัดการ ตลอดจนระบบงานบัญชี เทคโนโลยีสารสนเทศเป็นโครงสร้างพื้นฐานที่สำคัญในการสนับสนุนการทำธุรกรรม และในการดำเนินงานตั้งแต่การใช้บันทึกรายการธุรกิจที่เกิดขึ้นประจำวัน การให้บริการลูกค้าและให้ข้อมูลสำหรับผู้บริหารในการตัดสินใจ และให้ระบบสารสนเทศที่จะเป็นเครื่องมือที่ช่วยให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพลดต้นทุน เพิ่มขีดความสามารถในการแข่งขัน

ในขณะเดียวกันการนำเทคโนโลยีสารสนเทศมาใช้ก็มีความเสี่ยงหลายประการที่ควรคำนึงถึง ซึ่งหากองค์กรไม่มีการบริหารจัดการและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ ก็อาจส่งผลกระทบต่อการดำเนินงานหรือสร้างความเสียหายต่อองค์กรและลูกค้าได้ ทั้งนี้ ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการประกอบธุรกิจขององค์กร สามารถแบ่งออกเป็น 4 ประเภทหลัก คือ Access Risk, Integrity Risk, Availabily Risk และ Infrastructure Risk

นอกจากความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น ยังมีความเสี่ยงเกี่ยวกับการที่ผู้บริหารขององค์กรมิได้รับข้อมูลที่เกี่ยวข้องอย่างถูกต้องและทันเวลาเพื่อใช้ประกอบการตัดสินใจทางธุรกิจ ดังนั้น องค์กรก็ควรพิจารณาว่าข้อมูลใดบ้างที่จำเป็นแก่การตัดสินใจ รวมทั้งจัดให้มีระบบการตรวจสอบความถูกต้องของข้อมูล และจัดเตรียมข้อมูลดังกล่าวให้พร้อม เพื่อประโยชน์การดำเนินธุรกิจขององค์กร

นอกจากความเสี่ยงต่าง ๆ ข้างต้นแล้ว หากจะพิจารณาในด้านการพัฒนาระบบงาน ก็มีผลการวิจัยเกี่ยวกับสาเหตุที่หน่วยงานล้มเหลวในการพัฒนาระบบงานคอมพิวเตอร์ (Charles R. Neco: 1989) ได้แก่ ผู้บริหารระดับสูงไม่สนับสนุนหรือไม่มีส่วนร่วมในการพัฒนา หรือไม่มีคณะกรรมการระดับสูง (Steering Committee) ในการพัฒนาระบบงาน การเปลี่ยนความต้องการ

หรือวัตถุประสงค์ของระบบงานบ่อย การเลือกเทคโนโลยีที่ก้าวหน้า ล้ำสมัยเกินกว่าที่พนักงานจะทำความเข้าใจ การขาดคู่มือหรือวิธีการพัฒนาระบบงานให้เป็นขั้นตอนอย่างเป็นมาตรฐาน และบุคลากรที่เกี่ยวข้องกับการพัฒนาระบบมีไม่เพียงพอและได้รับการฝึกอบรมที่ไม่เพียงพอ

ดังนั้น ทุกวันนี้หลายองค์กรในประเทศไทยและทั่วโลก ได้พิจารณาถึง "Best Practices" หรือมาตรฐานที่ควรนำมาเป็นแนวทางในการเตรียมระบบสารสนเทศขององค์กรให้พร้อมเข้าสู่ยุค IT Governance โดยที่ "Best Practices" ที่นิยมใช้กันได้แก่ มาตรฐาน ISO/IEC17799, COBIT และ ITIL เป็นต้น

มาตรฐาน "COBIT" ย่อมาจาก "Control OBjectives for Information and Related Technology" COBIT นั้นมีจุดประสงค์ในการสร้างความมั่นใจว่าการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศนั้นสอดคล้องกับวัตถุประสงค์เชิงธุรกิจขององค์กร (Business Objectives) เพื่อให้เกิดการใช้ทรัพยากรอย่างมีประสิทธิผลอันจะส่งประโยชน์สูงสุดแก่องค์กร ช่วยให้เกิดความสมดุลย์ระหว่างความเสี่ยงด้านเทคโนโลยีสารสนเทศ และผลตอบแทนของการลงทุนในระบบสารสนเทศ โดย COBIT นั้นมีพื้นฐานมาจาก Framework ชั้นนำต่าง ๆ มากมาย ได้แก่ The Software Engineering Institute's Capability Maturity Model (CMM), ISO 9000 และ The Information Technology Infrastructure Library (ITIL) ของประเทศอังกฤษ อย่างไรก็ตาม COBIT นั้นก็ยังขาดในส่วนของ Guideline เพื่อใช้ในทางปฏิบัติเนื่องจาก COBIT เป็น Framework ที่เน้นในเรื่องของการควบคุม (Control) เป็นหลัก

นอกจากนี้ เพื่อป้องกันความเสี่ยงอันเกิดจากเทคโนโลยีสารสนเทศดังกล่าว มาตรการในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ซึ่งมีมาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่าง ๆ จะต้องนำมาประยุกต์ใช้ในการบริหารจัดการเทคโนโลยีสารสนเทศ โดยมีการควบคุมและตรวจสอบระบบสารสนเทศเป็นสิ่งที่จะช่วยในการติดตามและควบคุมการปฏิบัติตามมาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่าง ๆ ข้างต้น ดังนั้น การตรวจสอบระบบสารสนเทศจึงมีความสำคัญ และเป็นที่มาของการศึกษาวิจัยนี้

1.2 วัตถุประสงค์ของการวิจัย

วัตถุประสงค์ของการวิจัย มีดังต่อไปนี้

1. เพื่อศึกษาเกี่ยวกับการตรวจสอบระบบสารสนเทศ ซึ่งจะช่วยในการป้องกันความเสี่ยงต่าง ๆ ดังกล่าวข้างต้น

2. การนำมาตรฐานของ COBIT Framework มาประยุกต์ในการจัดทำแนวการตรวจสอบระบบสารสนเทศ (Audit Program)

1.3 ขอบเขตของการวิจัย

ขอบเขตของการวิจัย มีดังต่อไปนี้

1. จัดทำแนวการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Audit Program) ซึ่งประกอบด้วย หัวข้อการตรวจสอบ วัตถุประสงค์การตรวจสอบ ความเสี่ยง การควบคุมที่ควรมี และวิธีการทดสอบ/ตรวจสอบ

2. จัดทำข้อมูลกรณีศึกษาในการนำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Audit Program) มาใช้ในการตรวจสอบ

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับ มีดังต่อไปนี้

1. มีแนวทางการตรวจสอบระบบสารสนเทศ ซึ่งครอบคลุมถึงมาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่าง ๆ

2. องค์กรสามารถสร้างระบบการควบคุมทางด้านระบบสารสนเทศที่ยังขาดอยู่ เพื่อลดความเสี่ยงของระบบสารสนเทศ

3. การบริหารจัดการภายในองค์กร สามารถบรรลุวัตถุประสงค์ในการดำเนินธุรกิจ กล่าวคือ องค์กรมีประสิทธิภาพลดต้นทุน เพิ่มกำไร และเพิ่มขีดความสามารถในการแข่งขัน