

บทที่ 5

สรุปผลการวิจัย



5.1 สรุปผลการวิจัย

การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT เกี่ยวข้องกับการศึกษารวบรวมข้อมูลเกี่ยวกับเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ และการตรวจสอบระบบเทคโนโลยีสารสนเทศ และ COBIT FRAMEWORK เพื่อนำกรอบมาตรฐานของ COBIT มาใช้เป็นแนวทางในการจัดทำแนวการตรวจสอบระบบเทคโนโลยีสารสนเทศ โดยได้พิจารณาจัดทำแนวการตรวจสอบโดยแบ่งการตรวจสอบตามโครงสร้างของมาตรฐาน COBIT บนพื้นฐานของกระบวนการทางธุรกิจ 4 กระบวนการหลัก (Domain) ได้แก่ การวางแผนและการจัดการองค์กร (PO : Planning and Organization) การจัดหาและติดตั้ง (AI : Acquisition and Implementation) การส่งมอบและบำรุงรักษา (DS : Delivery and Support) การติดตามผล (M : Monitoring) ทั้งนี้แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Audit Program) จะประกอบด้วย หัวข้อการตรวจสอบ วัตถุประสงค์การตรวจสอบ ความเสี่ยง การควบคุมที่ควรมี และวิธีการทดสอบ/ตรวจสอบ ซึ่งสามารถใช้เป็นเครื่องมือช่วยผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศในการปฏิบัติงานตรวจสอบ และทำให้หัวหน้าหน่วยงานตรวจสอบระบบเทคโนโลยีสารสนเทศสามารถใช้เป็นเครื่องมือในการสอบทานและควบคุมงานตรวจสอบให้สามารถดำเนินการได้บรรลุวัตถุประสงค์ของการตรวจสอบ

มาตรฐาน COBIT นั้นมีจุดประสงค์ในการสร้างความมั่นใจว่า การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศสอดคล้องกับวัตถุประสงค์เชิงธุรกิจขององค์กร (Business Objectives) เพื่อให้เกิดการใช้ทรัพยากรอย่างมีประสิทธิภาพอันจะส่งประโยชน์สูงสุดแก่องค์กร ช่วยให้เกิดความสมดุลระหว่างความเสี่ยงด้านเทคโนโลยีสารสนเทศและผลตอบแทนของการลงทุนในระบบสารสนเทศ โดยมาตรฐาน COBIT มีพื้นฐานมาจาก FRAMEWORK ชั้นนำต่างๆ มากมาย ได้แก่ The Software Engineering Institute's Capability Maturity Model (CMM), ISO 9000, The Information Technology Infrastructure Library (ITIL) ของประเทศอังกฤษ อย่างไรก็ตาม COBIT ยังขาดในส่วนของ Guideline เพื่อใช้ในทางปฏิบัติ เนื่องจาก COBIT เป็น FRAMEWORK ที่เน้นในเรื่องของการควบคุม (Control) เป็นหลัก COBIT จะมุ่งประเด็นในการบอกว่าองค์กรต้องการอะไรบ้าง (What) แต่ไม่มีรายละเอียดในแง่ของวิธีการที่จะนำไปสู่จุดนั้น (How) ซึ่งเหมาะสมกับผู้

ตรวจสอบระบบเทคโนโลยีสารสนเทศที่จะนำมามาตรฐาน COBIT มาใช้เพื่อทำเป็น Audit Program แต่ในกรณีผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศมีประเด็นที่พบจากการตรวจสอบ และพิจารณาข้อเสนอแนะเพื่อการปรับปรุง จะต้องนำ FRAMEWORK อื่น ๆ เข้าร่วมเพื่อเพิ่มเติมรายละเอียดของการนำไปปฏิบัติ เช่น รายละเอียดในกระบวนการของ ITIL สามารถนำไปใช้เป็นรายละเอียดในข้อเสนอแนะเพื่อการปรับปรุงหากมีประเด็นที่พบจากการตรวจสอบในกระบวนการการส่งมอบและบำรุงรักษา (DS : Delivery and Support)

5.2 อภิปรายผลการศึกษา

ผลการศึกษาพบว่า แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT ‘ ผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถนำมาใช้เป็นเครื่องมือในการปฏิบัติงานตรวจสอบ และหัวหน้าหน่วยงานตรวจสอบสามารถใช้เป็นเครื่องมือในการสอบทานและควบคุมงาน ซึ่งทำให้การตรวจสอบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างครอบคลุมตามระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร และบรรลุวัตถุประสงค์ของการตรวจสอบอย่างใดก็ตาม รายละเอียดของการนำไปปฏิบัติในกระบวนการต่าง ๆ ในมาตรฐาน COBIT ผู้ตรวจสอบจะต้องพิจารณาข้อมูลเพิ่มเติมจาก FRAMEWORK อื่น ๆ เช่น มาตรฐาน ISO/IEC27001 ,ISO/IEC17799 ที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร, ISO/IEC 13335 ซึ่งเป็นมาตรฐานว่าด้วยแนวทางปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัย, ISO/IEC 15408 ซึ่งเป็นมาตรฐานว่าด้วยเรื่องเทคนิควิธีด้านความมั่นคงปลอดภัยซึ่งจะถูกใช้เป็นเงื่อนไขกลางหรือเกณฑ์กลาง (Common Criteria) ในการประเมินระบบในเรื่องของความมั่นคงปลอดภัย, ITIL (IT Infrastructure Library) ซึ่งเป็นแนวทางปฏิบัติว่าด้วยเรื่องเกี่ยวกับโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ซึ่ง ITIL นี้เป็นแนวทางปฏิบัติที่ดีเยี่ยม (best practice) ในการบริหารจัดการด้าน IT Service ตลอดจนเครื่องมือต่าง ๆ ที่ใช้สำหรับบริหารจัดการระบบเทคโนโลยีสารสนเทศ เช่น PRINCE2, PMBOX, TickIT, TOGAF8.1

5.3 ข้อเสนอแนะ

ผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถใช้แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศเป็นเครื่องมือในการปฏิบัติงานตรวจสอบ อย่างไรก็ตาม หากสามารถรวบรวมข้อมูลเกี่ยวกับรายละเอียดการนำไปปฏิบัติสำหรับกระบวนการทางธุรกิจทั้ง 4 กระบวนการหลัก (Domain) ไม่ว่าจะเป็นกระบวนการ การวางแผนและการจัดการองค์กร (PO : Planning and Organization) การจัดหาและติดตั้ง (AI : Acquisition and Implementation) การส่งมอบและบำรุงรักษา (DS : Delivery and Support) การติดตามผล (M : Monitoring) จะช่วยให้การปฏิบัติงานตรวจสอบระบบเทคโนโลยีสารสนเทศใช้ระยะเวลาสั้นลง