การวิเคราะห์และแนวทางจัดการความเสี่ยงด้านไอทีของหน่วยงานภาครัฐ

ICT risk management and analysis in the government organizations

วรัญญากรณ์ สิริพิพัฒนพร และ สมชาย นำประเสริฐชัย
สาขาเทคโนโลยีสารสนเทศ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์
E-mail:g5414550611@ku.ac.th, snp@ku.ac.th

บทคัดย่อ

หน่วยงานของรัฐลงทุนด้านเทคโนโลยีสารสนเทศและการสื่อสารเพื่อเป็นเครื่องมือสนับสนุนในการปฏิบัติภารกิจต่างๆ ให้บรรลุเป้าหมาย อย่างไรก็ตามหน่วยงานของรัฐยังมีความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการสื่อสารหลายประเด็น การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาประเด็นและสาเหตุของความเสี่ยงด้าน ICT ของหน่วยงานรัฐ และนำเสนอแนวทางเพื่อลดความเสี่ยง และให้สามารถบรรลุเป้าหมายของหน่วยงานได้ การวิจัยนี้เป็นการวิจัยเชิงคุณภาพในรูปแบบของกรณีศึกษาโดยใช้หน่วยงานภาครัฐระดับกรม จำนวน 7 แห่ง

ผลการศึกษาพบว่าประเด็นความเสี่ยงด้าน ICT ของหน่วยงานของรัฐมีลักษณะที่คล้ายกัน และมีสาเหตุหลักมาจากงบประมาณที่ได้รับน้อยกว่างบประมาณที่กำหนด การขาดแคลนบุคลากรด้าน ICT และการบริหารจัดการและขั้นตอนการดำเนินการที่ไม่เอื้อต่อการตอบสนองด้าน ICT

คำสำคัญ :

การจัดการความเสี่ยง เทคโนโลยีสารสนเทศและการสื่อสาร หน่วยงานภาครัฐ

Abstract

The government organizations have invested in information and communication technology as strategic tools for achieving goal. However, they have several risks related to information and communication technology. The research objectives focus on studying the issue and cases of the risk related to ICT and provide the suggestions to reduce the risk level. This research used the qualitative research based on seven cases of government organizations in department level.

The research results showed that the cause of ICT risks of government organizations came from 1) received budgets less than expected budgets 2) lacks of qualified ICT personal and 3) ICT management and procedure not suitable to ICT responses.

Keyword :

ICT risk management, information technology, government organization

1. คำนำ

ICT มีบทบาทสำคัญยิ่งต่อการเติบโตทางเศรษฐกิจของประเทศ การลงทุนด้าน ICT สามารถสร้างการเติบโตให้กับระบบเศรษฐกิจ และช่วยยกระดับผลิตภัณฑ์มวลรวมภายในประเทศ (GDP) ได้ หน่วยงานภาครัฐมีการลงทุนด้าน ICT และนำ ICT ไปใช้เป็นเครื่องมือเพื่อเพิ่มประสิทธิภาพของการบริหารจัดการการปฏิบัติงาน และการให้บริการ เมื่อมีการลงทุนด้าน ICT และ ICT กลายเป็นเครื่องมือสำคัญขององค์กร ทำให้ ICT กับธุรกิจมีความสัมพันธ์กันอย่างใกล้ชิด ดังนั้น การควบคุมและการประเมินความมั่นคงปลอดภัย ด้าน ICT ของหน่วยงานจึงจำเป็นสำหรับทุกองค์กร [1] หน่วยงานของรัฐส่วนใหญ่ลงทุนทางด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อเป็นเครื่องมือสนับสนุนกิจกรรมและกระบวนการต่างๆ ในระดับปฏิบัติการ และสนับสนุนการวางแผน และตัดสินใจในระดับบริหารการลงทุนด้าน ICT ประกอบด้วย การลงทุนด้านโครงสร้างระบบเครือข่าย ด้านอุปกรณ์คอมพิวเตอร์ ตลอดจนด้านระบบสารสนเทศ ทำให้การลงทุนด้าน ICT ของหน่วยงานภาครัฐใช้งบประมาณจำนวนมาก เช่นในปีงบประมาณ พ.ศ.2556 หน่วยงานภาครัฐทั้งประเทศมีการลงทุนด้าน ICT ถึง 1.4 หมื่นล้านบาท [2]

แม้ว่าหน่วยงานของรัฐจะมีการลงทุนทางด้าน ICT อย่างต่อเนื่องมานานหลายปี แต่หน่วยงานของรัฐยังคงประสบกับปัญหา เช่นปัญหาจากเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงอย่างรวดเร็ว ปัญหาด้านงบประมาณ และปัญหาการถูกรุกรานความปลอดภัยด้าน ICT เป็นต้น ทำให้การลงทุนการบริหารจัดการและการใช้ประโยชน์จากเทคโนโลยีสารสนเทศนั้นไม่เต็มประสิทธิภาพ ส่งผลกระทบต่อการบรรลุเป้าหมายของหน่วยงาน ดังนั้นการเข้าใจและสามารถบริหารจัดการความเสี่ยงด้าน ICT จะช่วยให้หน่วยงานภาครัฐสามารถตระหนักถึงปัญหา และสามารถบริหารจัดการความเสี่ยงต่างๆ ที่จะส่งผลกระทบต่อการบรรลุเป้าหมายของหน่วยงานได้ดียิ่งขึ้น

การบริหารจัดการความเสี่ยงด้าน ICT (ICT Risk Management) มีเป้าหมายเพื่อลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้นได้ซึ่งส่งผลต่อการบรรลุเป้าหมายขององค์กร ความเสี่ยงด้าน ICT เป็นความเสี่ยงขององค์กร เนื่องจากองค์กรได้นำเทคโนโลยีสารสนเทศและการสื่อสารเข้ามาเป็นเครื่องมือเพื่อใช้สนับสนุนการดำเนินการขององค์กรทั้งในระดับของการวางแผน การตัดสินใจ การปฏิบัติการและการให้บริการองค์กรหลายแห่งพยายามสร้างระบบ และแนวทางช่วยบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการสื่อสารระบบ หรือแนวทางการจัดการความปลอดภัย (Information Security Management System: ISMS) ที่มีการนำไปใช้อย่างแพร่หลายเช่น BS7799, ISO/IEC17799, ISO/IEC 27001 และ COBIT [3, 4, 5]

Information Security Risk Management (ISO/IEC 27005:2011) [6] ที่เป็นมาตรฐานเกี่ยวกับ “การบริหารจัดการความเสี่ยงด้าน ISMS (Information Security Risk Management)” ซึ่งพัฒนามาจาก ISO/IEC 17799 แทนที่มาตรฐานเดิม คือ BS 7799 Part 3 ที่มุ่งเน้นทางด้านการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศกล่าวถึงความเสี่ยงที่เป็นผล กระทบในด้านลบ ซึ่งอาจเกิดจากช่องโหวในด้านต่างๆ ได้ เช่น ด้านบุคคลขาดความตระหนักเรื่องความปลอดภัย อาจส่งผลให้เกิดข้อผิดพลาดในการใช้งาน หรือขาดกลไก ในการตรวจสอบอาจส่งผลให้เกิดการประมวลผลข้อมูลที่ผิดกฎหมาย ด้านอุปกรณ์ฮาร์ดแวร์ขาดการดูแลหรือจัดเก็บข้อมูลโดยไม่มีการป้องกัน อาจส่งผลให้เกิดการขโมยสื่อหรือเอกสารได้ เป็นต้น โดยการบริหารจัดการความเสี่ยงเป็นกระบวนการในการระบุความ

เสี่ยงที่เกิดขึ้น การประเมินความเสี่ยง และขั้นตอนในการลดความเสี่ยงคือการทำให้ความเสี่ยงที่เหลืออยู่ในระดับที่สามารถยอมรับได้ ในกรอบแนวทาง Control Objectives for Information and Related Technology (COBIT) เป็นเครื่องมือในการบริหารจัดการ ICT โดยอ้างถึงประเด็นที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้าน ICT พร้อมทั้งแนวทางการปฏิบัติเพื่อการควบคุมภายในด้านเทคโนโลยีสำหรับองค์กรต่างๆ กรอบแนวทาง COBIT เป็นที่ยอมรับอย่างกว้างขวางสำหรับใช้ในการบริหารจัดการโครงการและการกำกับดูแลด้าน ICT [7] โครงสร้างของกรอบ COBIT ได้ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ (Business Process) ซึ่งแบ่งได้เป็น 4 ส่วนหลัก (domain) ได้แก่ การวางแผนและการจัดการองค์กร (Planning and Organization: PO) การจัดหาและการนำไปใช้ (Acquisition and Implementation: AI) การส่งมอบและการสนับสนุน (Delivery and Support: DS) และการตรวจสอบและการประเมินผล (Monitoring and Evaluation : ME) อย่างไรก็ตามรายละเอียดส่วนใหญ่ในกระบวนการต่างๆ ที่กำหนดใน COBIT นั้นกล่าวว่า“ต้องทำอะไร” มากกว่า “ทำอย่างไร” [8] ซึ่งอาจทำให้การดำเนินการต้องอาศัย แนวทางหรือมาตรฐานอื่นมาช่วยดำเนินการ

ส่วนกรอบแนวคิดของ ISO/IEC27001:2005 มีประเด็นหลักหลายประเด็นที่เกี่ยวข้องกับ COBIT สามารถเชื่อมโยง เปรียบเทียบกันได้ เช่น นโยบายความมั่นคงปลอดภัยของ ISO/IEC 27001:2005 เทียบได้กับ PO1: กำหนด แผนกลยุทธ์ด้านไอที PO3: กำหนดทิศทางเทคโนโลยี PO6: สื่อสารทิศทางและจุดมุ่งหมายของการจัดการ และ M1: การติดตามกระบวนการของ COBIT ได้ อย่างไรก็ตาม ทั้งสองกรอบนี้มีข้อเด่นที่แตกต่างกัน [9]

การประเมินความเสี่ยงด้าน ICT ของหน่วยงานของรัฐส่วนใหญ่ไม่ได้มีการเลือกแนวทางบริหารจัดการความเสี่ยงมาใช้ในการดำเนินการอย่างเป็นทางการ ทำให้ไม่มีการจัดเก็บข้อมูลที่เพียงพอต่อการประเมิน ดังนั้นจึงเป็นเรื่องยากที่จะนำเกณฑ์หรือแนวทางในการประเมินความเสี่ยงมาใช้โดยตรง การศึกษาประเมินความเสี่ยงด้าน ICT นี้จึงได้ประยุกต์แนวทางของ COBIT มาใช้เป็นเครื่องมือในการวิเคราะห์ความเสี่ยง เนื่องจากมีความสอดคล้องและสามารถปรับกระบวนการที่องค์กรดำเนินการให้เข้ากับประเด็นต่างๆ ได้อย่างเหมาะสม นอกจากนี้ยังสามารถนำแนวคิดในเรื่องของการควบคุมภายในของ COBIT มาช่วยในการปรับปรุงแนวทาง การลดความเสี่ยงของหลายหน่วยงานของรัฐที่ประสบอยู่ได้อีกด้วย

2. วิธีการ

การศึกษานี้เลือกหน่วยงานระดับกรมของภาครัฐ เนื่องจากหน่วยงานดังกล่าวเป็นหน่วยงานที่ต้องมีการจัดทำแผนแม่บทด้านเทคโนโลยีสารสนเทศและการสื่อสารตามข้อกำหนดของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย [10]

การเก็บข้อมูลใช้วิธีการสำรวจและสัมภาษณ์ผู้บริหารระดับสูง ผู้ใช้งานทั่วไป และเจ้าหน้าที่ที่ทำหน้าที่ดูแล ระบบเทคโนโลยีสารสนเทศและการสื่อสารของแต่ละหน่วยงาน โดยใช้ประเด็นคำถามตาม 4 กระบวนการหลักของ COBIT 3.0 [11] ดังนี้ (1) เรื่องการวางแผนและการจัดการองค์กร (PO : Planning and Organization) เช่น มีการจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศหรือไม่ มีการกำหนดโครงสร้างด้านสารสนเทศหรือไม่ มีการกำหนดทิศทางด้านเทคโนโลยีหรือไม่ มีการจัดโครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศและความสัมพันธ์กับหน่วยงานอื่น

หรือไม่ เป็นต้น (2)เรื่องการจัดหาและการนำระบบออกใช้งานจริง (AI : Acquisition and Implementation) เช่น ในเรื่องของการเลือก เทคโนโลยีมาใช้ในการปฏิบัติงาน (Identify Automated Solutions) เพื่อให้มั่นใจว่าจะตอบสนองความต้องการข้อมูลของผู้ใช้ได้อย่างมีประสิทธิผล และประสิทธิภาพนั้นมีการกำหนดความต้องการสารสนเทศหรือไม่ มีการศึกษาความเป็นไปได้ของเทคโนโลยีหรือไม่ เป็นต้น (3) เรื่องการส่งมอบและการสนับสนุน (DS : Delivery and Support) เช่น การกำหนดและการจัดการระดับการให้บริการ (Define and Manage Service Levels) เพื่อให้เกิดความเข้าใจที่ถูกต้องของระดับบริการที่เป็นที่ต้องการนั้นมีการกำหนดกรอบข้อตกลงเกี่ยวกับการให้บริการหรือไม่ มีแผนการปรับปรุงการให้บริการ เป็นต้น (4) เรื่องการติดตามผล (M : Monitoring) เช่น การติดตามกระบวนการทำงาน (Monitor the Processes) เพื่อให้มั่นใจว่ากิจกรรมด้าน IT สามารถบรรลุเป้าหมายการปฏิบัติงานตามที่กำหนด มีการรวบรวมข้อมูลหรือไม่ มีการประเมินประสิทธิภาพการปฏิบัติงานหรือไม่ มีการประเมินความพึงพอใจของผู้รับบริการหรือไม่ เป็นต้น ซึ่งคำถามที่ใช้ในการสัมภาษณ์ได้ประยุกต์แนวทางของ COBIT 3.0 มาใช้ แม้ว่าจะเป็นรุ่นเก่าแต่มีความเหมาะสมในการประเมินความเสี่ยงด้าน ICT ของหน่วยงานภาครัฐ เนื่องจากได้ตรวจสอบกับผู้เชี่ยวชาญและ ทดสอบกับหน่วยงานตัวอย่าง และผู้วิจัยยังได้ประยุกต์ให้มีความเหมาะสมกับบริบทของหน่วยงานของรัฐของประเทศไทยยิ่งขึ้น

นอกจากนี้คณะผู้วิจัยยังได้รวบรวมข้อมูลต่างๆ ที่เกี่ยวข้องของแต่ละหน่วยงานมาประกอบการศึกษาวิเคราะห์เพิ่มเติม เช่นแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร แผนปฏิบัติการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปี รายงานผลการประเมินการดำเนินการด้าน ICT ของแต่ละหน่วยงานเป็นต้น

ผลลัพธ์ที่ได้ผ่านการวิเคราะห์ร่วมกับผู้เชี่ยวชาญด้าน ICT จำนวน 3 คน โดยผู้เชี่ยวชาญ 2 คนเป็นที่ปรึกษาด้านการวางแผนด้าน ICT ให้กับหน่วยงานรัฐมานานกว่า 10 ปี และผู้เชี่ยวชาญอีกคนเป็นนักวิชาการที่มีประสบการณ์ด้านเทคโนโลยีสารสนเทศมากกว่า 30 ปี

3. ผลการทดลอง

หน่วยงานกรณีศึกษาทั้ง 7 แห่งมีการจัดทำแผนแม่บทด้าน ICT ตามกรอบที่ทางกระทรวงเทคโนโลยีสารสนเทศ และการสื่อสารกำหนด[12] โดยมีรองอธิบดีกรมดำรงตำแหน่งผู้บริหารสารสนเทศระดับสูง (Chief Information Officer: CIO) ทำหน้าที่กำหนดแนวนโยบายด้าน ICT พิจารณากลั่นกรองข้อเสนอและรายละเอียดโครงการ และแผนการปฏิบัติงานด้าน ICT และแผนงบประมาณ ตลอดจนความเหมาะสมของโครงการด้าน ICT ของหน่วยงาน และมีศูนย์เทคโนโลยีสารสนเทศเป็นหน่วยงานหลักในการบริหารจัดการ และให้บริการด้าน ICT

การดำเนินการด้าน ICT ของหน่วยงานกรณีศึกษาทั้ง 7 แห่งมีการจัดจ้างที่ปรึกษาภายนอกมาช่วยในการดำเนินการจัดทำแผนแม่บทด้าน ICT อย่างไรก็ตามหน่วยงานทั้ง 7 แห่งมีการกำหนดงบประมาณด้าน ICT เฉลี่ยอยู่ระหว่าง 50-120 ล้านบาทต่อปี แต่หน่วยงานส่วนใหญ่ไม่สามารถดำเนินการด้าน ICT ได้ตามแผนที่กำหนดลงบเนื่องมาจากงบประมาณที่ได้รับจัดสรรนั้นไม่เพียงพอ ทำให้หน่วยงานเกิดความเสี่ยงด้าน ICT ในประเด็นต่างๆ ที่กำหนดตามกรอบของ COBIT โดยความเสี่ยงด้าน ICT สูงสุด10 ประเด็นของหน่วยงานทั้ง 7 แห่งดังแสดงในตารางที่ 1

ตารางที่ 1 แสดงความเสี่ยงด้าน ICT สูงสุด 10 ประเด็นของหน่วยงานทั้ง 7 แห่ง

ลำดับ	ความเสี่ยง	หน่วยงานกรณีศึกษา						
		A	B	C	D	E	F	G
1	การกำหนดสถาปัตยกรรมด้านสารสนเทศ	✓	✓	✓	✓	✓	✓	✓
2	การกำหนดและการจัดการระดับการให้บริการ	✓	✓	✓	✓	✓	✓	✓
3	การจัดการการเปลี่ยนแปลง	✓	✓	✓	✓	✓	✓	-
4	การต่อเนื่องในการให้บริการ	✓	✓	✓	✓	✓	✓	✓
5	การช่วยเหลือและให้คำปรึกษาแก่ผู้ใช้งาน	✓	✓	✓	✓	✓	✓	✓
6	การจัดการคุณภาพ	✓		✓	✓	✓	✓	-
7	การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ	✓	✓	-	✓	✓	-	✓
8	การจัดการด้านสมรรถนะและความสามารถของระบบ	✓	✓	-	✓	✓	-	-
9	การจัดการปัญหาและเหตุการณ์ที่เกิดขึ้น	-	✓	-	✓	✓	✓	-
10	การรักษาความปลอดภัยระบบสารสนเทศ	✓	-	✓	✓	✓	✓	-

หมายเหตุ : A, B, C, D, E, F และ G แทนชื่อหน่วยงานที่เป็นกรณีศึกษาทั้ง 7 แห่ง

✓หมายถึงประเด็นความเสี่ยงด้าน ICT ที่ปรากฏในองค์กรทั้ง 7 แห่ง

1) การกำหนดสถาปัตยกรรมด้านสารสนเทศ (Enterprise Architecture) เป็นโครงสร้างที่รวมทุกสิ่งทุกอย่างในองค์กรเข้าไว้ด้วยกัน เริ่มตั้งแต่กลยุทธ์ทางธุรกิจ โครงสร้างองค์กร กระบวนการทำงาน ความเสี่ยงในองค์กร ข้อมูลสนับสนุนการทำงาน ระบบซอฟต์แวร์ต่างๆ โครงสร้างพื้นฐานทางด้าน IT และระบบความปลอดภัยภายในองค์กร สถาปัตยกรรมองค์กรช่วยให้หน่วยงานสามารถวิเคราะห์และทำความเข้าใจองค์กรได้ดีขึ้นสำหรับการพัฒนาโครงสร้างองค์กรในอนาคต ตามแนวทางกลยุทธ์ขององค์กรที่กำหนดไว้

2) การกำหนดและการจัดการระดับการให้บริการ หน่วยงานต่างๆ ได้ให้ความสำคัญกับระดับการให้บริการ (Service Level Agreement) มากขึ้น เนื่องจากเป็นเสมือนข้อตกลงในการให้บริการระหว่างผู้ให้บริการกับผู้รับบริการ การกำหนดและการจัดการระดับการให้บริการด้าน ICT เป็นความเสี่ยงอีกประเด็นหนึ่งที่เกิดขึ้นกับหน่วยงานของรัฐ จากกรณีศึกษาพบว่าประเด็นดังกล่าวนี้ยังเป็นความเสี่ยง ที่เกิดขึ้นในทุกหน่วยงานกรณีศึกษา ไม่มีหน่วยงานใดที่มีการกำหนดข้อตกลงกับผู้รับบริการ เนื่องจากหน่วยงานของรัฐเห็นว่าเป็นการให้บริการที่ไม่มีค่าใช้จ่าย จึงไม่จำเป็นต้องมีสัญญาหรือเงื่อนไขที่อาจสร้างปัญหาให้กับหน่วยงาน

3) การจัดการการเปลี่ยนแปลง เป็นการบริหารจัดการสำหรับรองรับการเปลี่ยนแปลงเพื่อให้เกิดความพร้อมและลดการต่อต้าน เนื่องจากการพัฒนาระบบสารสนเทศมาใช้สนับสนุนการบริหารจัดการ การปฏิบัติการนั้นก่อให้เกิดการเปลี่ยนแปลงในการดำเนินการ หน่วยงานส่วนใหญ่ไม่มีการจัดการการเปลี่ยนแปลงจึง

มักประสบปัญหาในขั้นเริ่มต้นใช้งานระบบใหม่หรือเริ่มใช้ระบบงานทดแทน

4) ความต่อเนื่องในการให้บริการ องค์กรธุรกิจมักมีการตั้งเป้าหมายความต่อเนื่องในการให้บริการอยู่ที่ร้อยละ 99.999 ที่หมายความว่าธุรกิจไม่ยอมให้เกิดการหยุดชะงักหรือระบบขัดข้องเกิดขึ้น จากการศึกษาสำรวจและสัมภาษณ์พบว่าหน่วยงานของรัฐกรณีศึกษานั้นทุกหน่วยงานเห็นความสำคัญของความต่อเนื่องของการให้บริการ อย่างไรก็ตามด้วยข้อจำกัดของงบประมาณที่มีอยู่นั้นทำให้การดำเนินการต้องมีกระบวนการดำเนินการเป็นลำดับขั้นตั้งแต่การสำรองข้อมูล การสำรองระบบและการสร้างระบบที่สามารถทำงานทดแทนได้อย่างทันทีทันใด ซึ่งในส่วนของการดำเนินการสร้างระบบที่สามารถทำงานทดแทนได้อย่างทันทีทันใดนั้นมักจะเป็นโครงการที่อยู่ในปีสุดท้ายของแผนแม่บทด้าน ICT เนื่องจากต้องรอความพร้อมในส่วนของโครงสร้างพื้นฐานซึ่งมีการลงทุนที่สูงมาก หน่วยงานที่เป็นกรณีศึกษาทั้งหมดได้มีการวางแผนตั้งแต่จัดทำแผนแม่บทด้าน ICT แต่ยังไม่มีหน่วยงานใดที่สามารถปฏิบัติได้จริง

5) การช่วยเหลือและให้คำปรึกษาแก่ผู้ใช้งาน เมื่อหน่วยงานมีการนำคอมพิวเตอร์และระบบสารสนเทศมาเป็นเครื่องมือสนับสนุนในการปฏิบัติงาน ปัญหาหนึ่งที่มักเกิดขึ้นกับทุกหน่วยงานคือปัญหาการใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศต่างๆ ในการปฏิบัติหน้าที่และการบรรลุเป้าหมายขององค์กร หน่วยงานของรัฐขนาดใหญ่มักมีบุคลากรด้าน ICT ของศูนย์เทคโนโลยีสารสนเทศเป็นผู้ให้บริการช่วยเหลือ และให้คำปรึกษาแก่ผู้ใช้งาน ในขณะที่หน่วยงานของรัฐ ส่วนหนึ่งได้มีการจัดจ้างหน่วยงานภายนอกในการให้บริการแก้ไขปัญหาและให้คำปรึกษาด้าน ICT โดยเฉพาะ อย่างยิ่งปัญหาที่เกิดขึ้นกับระบบสารสนเทศเฉพาะเจาะจง เหตุผลหลักของการจัดหาหน่วยงานภายนอกในการให้บริการคือบุคลากรภายในนั้นมีจำนวนจำกัด และยังขาดความเข้าใจเชิงลึกในเรื่องระบบสารสนเทศแบบเฉพาะเจาะจง อย่างไรก็ตามไม่ว่าจะเป็นการดำเนินการให้ความช่วยเหลือและคำปรึกษาแก่ผู้ใช้งานก็ตามส่วนใหญ่ยังไม่สามารถตอบสนองต่อความต้องการและความเร่งด่วนของผู้ใช้งานโดยบุคลากรภายในหรือหน่วยงานภายนอกได้ ทำให้เกิดการหยุดชะงักของงาน

ปัจจัยความสำเร็จในการให้ความช่วยเหลือและให้คำปรึกษาด้าน ICT นั้นขึ้นอยู่กับความสามารถของบุคลากรและความสัมพันธ์ที่ดีระหว่างบุคลากรที่ให้บริการกับผู้รับบริการ ความเสี่ยงในประเด็นนี้จึงเป็นประเด็นสำคัญต่อการบรรลุเป้าหมายของหน่วยงาน

6) การจัดการคุณภาพ เป็นประเด็นความเสี่ยงที่สะท้อนถึงคุณภาพของระบบ ICT ที่องค์กรนำมาใช้ว่ามีความเหมาะสมกับความต้องการทางด้านธุรกิจหรือสามารถตอบสนองต่อความต้องการของหน่วยงานหรือกลุ่มเป้าหมายได้หรือไม่ การจัดการคุณภาพด้าน ICT ของหน่วยงานรัฐมักเน้นการดำเนินการในระดับปฏิบัติการแบบแยกตามฟังก์ชั่นไม่ได้มีการบูรณาการให้เกิดการเชื่อมโยงระหว่างระบบงาน ทำให้การดำเนินการในบางส่วนเกิดความซ้ำซ้อนกัน ระบบสารสนเทศที่พัฒนา ขาดการวางแผนในภาพรวม และขาดการมีส่วนร่วมของผู้ที่เกี่ยวข้อง ดังนั้นระบบสารสนเทศบางส่วน จึงมีคุณภาพที่ไม่สามารถตอบสนองต่อความพึงพอใจ ของผู้ใช้งานได้ และไม่สามารถบูรณาการข้อมูลเพื่อนำไปใช้ในการวางแผนและตัดสินใจของผู้บริหารได้ อย่างไรก็ตามหน่วยงานรัฐได้เริ่มตระหนักถึงความสำคัญนี้ และได้มีการเตรียมการเพื่อพัฒนาปรับปรุงให้ระบบสารสนเทศมีคุณภาพที่สามารถนำข้อมูลต่างๆ มาใช้เพื่อให้เกิดประโยชน์กับหน่วยงานมากยิ่งขึ้น

7) การจัดหาและบำรุงรักษาโครงสร้างพื้นฐาน ด้านเทคโนโลยีสารสนเทศ หน่วยงานของรัฐที่มีปัญหาเกี่ยวกับโครงสร้างพื้นฐานด้าน ICT ยังไม่สามารถตอบสนองต่อความต้องการของผู้ใช้งานและรองรับบริการต่างๆ

ที่มีได้อย่างมีประสิทธิภาพ ทั้งนี้มาจากงบประมาณที่จำกัดทำให้ไม่สามารถปรับเปลี่ยนโครงสร้างพื้นฐานด้าน ICT ได้ตามการเปลี่ยนแปลงของเทคโนโลยีและความคาดหวังของผู้ใช้งานและผู้รับบริการที่มีสูงขึ้นได้ จากการสำรวจพบว่าหน่วยงานของรัฐตั้งงบประมาณสำหรับการบำรุงรักษาโครงสร้างพื้นฐานด้าน ICT น้อยมาก ทำให้ประสิทธิภาพของโครงสร้างพื้นฐานด้าน ICT ไม่สามารถปรับเปลี่ยนและรองรับต่อความต้องการได้

8) การจัดการด้านสมรรถนะและความสามารถของระบบ เป็นการบริหารจัดการระบบให้มีสมรรถนะและความสามารถที่เหมาะสมกับปริมาณภาระงาน โดยไม่จำเป็นต้องลงทุนระบบให้สูงเกินไป และไม่ก่อให้เกิดประโยชน์ หรือความได้เปรียบในการแข่งขัน ดังนั้นหน่วยงานต้องศึกษา วิเคราะห์ปริมาณงาน ขนาดของข้อมูล จำนวนผู้ใช้และข้อมูลอื่นๆ ที่เกี่ยวข้องกับการออกแบบระบบ เพื่อให้ระบบมีสมรรถนะและความสามารถที่เหมาะสม จากการศึกษา พบว่าการวิเคราะห์และออกแบบสมรรถนะของระบบส่วนใหญ่นั้นเป็นการประเมินอย่างคร่าวๆ ของบุคลากรด้าน ICT เท่านั้น ไม่ได้มีการศึกษาวิเคราะห์ในรายละเอียดต่างๆ ซึ่งอาจทำให้สมรรถนะและความสามารถของระบบไม่ สอดคล้องกับภาระที่ต้องรองรับ นอกจากนี้งบประมาณ ที่ได้รับมักน้อยกว่างบประมาณที่กำหนดในแผนจึงทำให้สมรรถนะและความสามารถของระบบต่ำกว่าที่ต้องการ ดังนั้นความเสี่ยงในประเด็นนี้ผู้บริหารระดับสูงต้องมีความรู้ความเข้าใจเกี่ยวกับการลงทุนด้าน ICT เพื่อให้มีการจัดสรรงบประมาณสำหรับดำเนินการอย่างเหมาะสม

9) การจัดการปัญหาและเหตุการณ์ที่เกิดขึ้น ความสามารถในการจัดการปัญหาและเหตุการณ์ที่เกิดขึ้นนั้นจะช่วยให้ระดับความรุนแรงของผลกระทบจากปัญหาต่างๆ ลดลง หน่วยงานของรัฐเริ่มให้ความสำคัญกับการจัดการปัญหาและเหตุการณ์ต่างๆ มากยิ่งขึ้น โดย 3 ใน7 หน่วยงานได้มีการจัดทำแผนดำเนินการฉุกเฉินสำหรับเป็นแนวทางปฏิบัติหากเกิดเหตุการณ์ที่ไม่คาดคิดเกิดขึ้น หน่วยงานของรัฐมีการกำหนดระดับของปัญหาว่าปัญหาใดใครเป็นผู้ตัดสินใจ และจะดำเนินการอย่างไร การดำเนินการในส่วนนี้มักจะผนวกเข้ากับแผนการจัดการความเสี่ยงของหน่วยงาน

10) การรักษาความปลอดภัยระบบสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกำหนดให้หน่วยงานของรัฐทุกแห่งต้องดำเนินการโครงการที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศ อย่างไรก็ตามจากการสำรวจพบว่ามีเพียง 2 หน่วยงานเท่านั้นที่กำหนดการดำเนินการด้านการรักษาความปลอดภัยระบบสารสนเทศทั้งในระดับนโยบายและแนวทางปฏิบัติที่จริงจัง ตั้งแต่การออกแบบระบบสารสนเทศและการป้องกันตรวจสอบการเข้าใช้งานระบบ ในขณะที่หน่วยงานที่ไม่ได้ดำเนินการอย่างจริงจังเห็นว่าข้อมูลต่างๆ ที่หน่วยงานมีอยู่นั้นไม่มีอะไรที่เป็นความลับจึงทำให้เกิดความหละหลวมในการรักษาความปลอดภัยของระบบสารสนเทศ

ผลการทดลองและวิจารณ์

ปัญหาความเสี่ยงด้าน ICT ของหน่วยงานภาครัฐมาจากหลายสาเหตุ โดยเฉพาะอย่างยิ่งงบประมาณที่ไม่เพียงพอกับความต้องการด้าน ICT ในการสนับสนุนภารกิจที่ต้องการ จากข้อมูลการสำรวจหน่วยงานทั้ง 7 แห่งได้รับงบประมาณสำหรับการดำเนินการจริงไม่ถึงร้อยละ 60 เมื่อเทียบกับงบประมาณที่กำหนดในแผน นอกจากนี้หน่วยงานของรัฐยังขาดบุคลากรด้าน ICT ที่มีความรู้ ความสามารถเชิงลึก ทำให้ต้องพึ่งพาหน่วยงานภายนอกในรูปแบบต่างๆ เช่นการจัดจ้างที่ปรึกษา การจัดหาผู้พัฒนาระบบภายนอก เป็นต้น นอกจากนี้หน่วยงานรัฐยังจำกัดจำนวนนักวิชาการคอมพิวเตอร์ทั้งอัตราเงินเดือนของเจ้าหน้าที่ยังต่ำเมื่อเปรียบเทียบกับหน่วยงานภาคเอกชน ทำให้ปริมาณการเข้าออกงานของบุคลากรด้านนี้สูง

อย่างไรก็ตามความเสี่ยงด้าน ICT ของหน่วยงานภาครัฐยังเป็นประเด็นทั้งในส่วนของการบริหารจัดการและการพัฒนาระบบสารสนเทศ ดังนั้นหากมีการวางแผนและออกแบบแนวทางการดำเนินการที่เหมาะสมก็สามารถช่วยการบริหารจัดการความเสี่ยงด้าน ICT ให้อยู่ในระดับที่ยอมรับได้ หากคณะกรรมการด้าน ICT ของหน่วยงานมีการดำเนินการที่จริงจังมีการประยุกต์หลักการจัดการต่างๆ เช่น การจัดการคุณภาพ การบริหารการเปลี่ยนแปลง และการติดตามประเมินผล เป็นต้น นอกจากนี้หน่วยงานยังสามารถพัฒนาระบบเทคโนโลยีสารสนเทศ เพื่อช่วยให้การดำเนินการเกี่ยวกับความเสี่ยงด้าน ICT ให้เป็นไปอย่างมีประสิทธิภาพ ยิ่งขึ้นดังแสดงในตารางที่ 2

ตารางที่2 แสดงแนวทางการจัดการความเสี่ยงด้าน ICT

ความเสี่ยง	แนวทางการดำเนินการ เพื่อการจัดการความเสี่ยงด้าน ICT
การกำหนดสถาปัตยกรรมด้านสารสนเทศ	กำหนดสถาปัตยกรรมด้านสารสนเทศในขั้นตอนการออกแบบและจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ซึ่งสอดคล้องกับแนวโน้มของการเปลี่ยนแปลงเทคโนโลยีในอนาคต
การกำหนดและการจัดการระดับการให้บริการ	กำหนดนโยบายด้านเทคโนโลยีสารสนเทศที่ชัดเจน รวมทั้งระดับการให้บริการด้านเทคโนโลยีสารสนเทศ (SLA)
การจัดการการเปลี่ยนแปลง	การบริหารจัดการการเปลี่ยนแปลง เพื่อเตรียมความพร้อมในส่วนของผู้ที่เกี่ยวข้อง และลดการต่อต้านในช่วงเริ่มต้นของการดำเนินการ
ความต่อเนื่องในการให้บริการ	แนวทางการดำเนินการสถานการณ์ฉุกเฉิน มีการจัดทำแผนเตรียมรับสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยทั้งในส่วนของแผน BCP (Business Continuity Plan) และแผน DRP (Disaster Recovery Plan) เพื่อให้หน่วยงานมีความสามารถในการให้บริการอย่างต่อเนื่องได้
การช่วยเหลือและให้คำปรึกษาแก่ผู้ใช้งาน	การสร้างความสัมพันธ์ที่ดีระหว่างบุคลากรด้าน ICT กับบุคลากรในหน่วยงานอื่นๆ การพัฒนากระบวนให้คำปรึกษาและช่วยเหลือด้านไอที
การจัดการคุณภาพ	การกำหนดนโยบายด้านเทคโนโลยีสารสนเทศที่ชัดเจน
การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี	โครงการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ/ระบบเครือข่าย ระบบฐานข้อมูลและโครงสร้างพื้นฐานอื่นๆ
การจัดการด้านสมรรถนะและความสามารถของระบบ	การบริหารจัดการและการประเมินความคุ้มค่าของทรัพยากรด้านเทคโนโลยีสารสนเทศ

ความเสี่ยง	แนวทางการดำเนินการ เพื่อการจัดการความเสี่ยงด้าน ICT
การจัดการปัญหาและเหตุการณ์ที่เกิดขึ้น	การจัดทำคู่มือและแนวทางปฏิบัติด้าน ICT/ ระบบ FAQs การจัดทำแผนเตรียมรับสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยทั้งในส่วนของแผน BCP (Business Continuity Plan) และแผน DRP (Disaster Recovery Plan) เพื่อให้หน่วยงานมีความพร้อมในการรับเหตุการณ์ฉุกเฉิน
การรักษาความปลอดภัยระบบสารสนเทศ	การพัฒนาศูนย์เทคโนโลยีสารสนเทศ/ระบบป้องกันความปลอดภัยระบบสารสนเทศโดยการนำมาตรฐานที่เกี่ยวข้องกับการรักษาความปลอดภัยที่เป็นสากลมาประยุกต์ใช้ เช่น ISO/IEC17799 หรือ COBIT

หากหน่วยงานของรัฐมีการดำเนินการดังกล่าวอย่างจริงจังแล้ว ก็สามารถลดระดับความเสี่ยงด้าน ICT ได้ โดยเฉพาะอย่างยิ่งการดำเนินการในส่วนของโครงการ ICT เช่นการพัฒนาโครงสร้างพื้นฐานด้าน ICT การพิจารณาในการออกแบบระบบสารสนเทศให้คำนึงถึงความปลอดภัยมากขึ้น การพัฒนาระบบ Helpdesk และ FAQs ในการให้บริการคำปรึกษาปัญหาด้าน ICT รวมทั้งกำหนดให้มีการประเมินความสำเร็จของโครงการทั้งในส่วนของการบรรลุเป้าหมายและความคุ้มค่า เพื่อนำมาเป็นบทเรียนในการลงทุนและออกแบบพัฒนาปรับปรุงระบบสารสนเทศขององค์กรในอนาคตให้มีความเหมาะสมยิ่งขึ้น

4. บทวิจารณ์

หน่วยงานของรัฐ ที่มีความเสี่ยงด้าน ICT ส่วนใหญ่นั้นมาจากสาเหตุ ได้แก่งบประมาณด้าน ICT ที่ได้รับนั้นน้อยกว่างบประมาณที่กำหนดในแผนค่อนข้างมาก ทำให้ไม่สามารถดำเนินการได้ตามแผนที่กำหนด บุคลากรด้าน ICT มีจำนวนน้อยเมื่อเปรียบเทียบกับปริมาณงานที่ต้องรับผิดชอบ บุคลากรส่วนใหญ่ไม่ได้สำเร็จการศึกษาในสาขาที่เกี่ยวข้องกับด้าน ICT อีกทั้ง หน่วยงานรัฐยังขาดสิ่งจูงใจในการดึงดูดบุคลากรด้าน ICT ที่มีศักยภาพให้มาร่วมงานหรืออยู่กับองค์กรตลอดไป

การบริหารจัดการความเสี่ยงด้าน ICT ของหน่วยงานของรัฐนั้นจำเป็นต้องมีการบริหารจัดการงบประมาณด้าน ICT ที่เหมาะสม เข้าใจ และลงทุนโครงการ ICT อย่างรอบคอบ มีการกำหนดนโยบาย การพัฒนา/ปรับปรุงกระบวน การดำเนินการด้าน ICT ที่มีประสิทธิภาพและสามารถนำไปปฏิบัติได้จริง มีการติดตามประเมินผลอย่างต่อเนื่อง มีการส่งเสริมการพัฒนาบุคลากรทุกระดับให้มีความพร้อม มีความรู้ ความเข้าใจ และความสามารถในการใช้ ICT ให้เกิดประโยชน์อย่างเหมาะสม มีกลไกในการสร้าง นโยบายและแนวทางการใช้ประโยชน์จากการลงทุนด้าน ICT ที่ชัดเจน และส่งเสริมการมีส่วนร่วมของผู้ที่มีส่วนเกี่ยวข้องให้มากยิ่งขึ้น

5. กิตติกรรมประกาศ

คณะผู้วิจัยขอขอบคุณผู้บริหารระดับสูง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร บุคลากรด้าน ICT และบุคลากรทั่วไปที่เกี่ยวข้องของหน่วยงานที่เป็นกรณีศึกษาทั้ง 7 แห่ง ที่สละเวลาในการให้ข้อมูลและเอกสารต่างๆ ที่เกี่ยวข้อง ขอขอบคุณผู้เชี่ยวชาญด้าน ICT ที่ให้ความคิดเห็นเกี่ยวกับประเด็นคำถามที่ประยุกต์ใช้เป็นเครื่องมือ และให้ข้อเสนอแนะที่เป็นประโยชน์เพิ่มเติม

เอกสารอ้างอิง

[1] Biene-Hershey, M.V., (2007) IT security and IT audit between 1960 and 2000, The history of Information Security: A comprehensive Handbook, Elsevier, 655-680

[2] สำนักงบประมาณร่วมกับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารและสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). (2555). เอกสารการประชุมสัมมนาเรื่อง “นโยบายการบูรณาการด้านICT และการจัดสรร งบประมาณของหน่วยงานภาครัฐ”. ห้องประชุมแซฟไฟร์๑๑๗-๑๒๐ชั้น๑ศูนย์การประชุมอิมแพคฟอรั่มเมืองทอง ธานีแจ้งวัฒนะกรุงเทพมหานคร

[3]Broderick, J.S., (2006) ISMS, security standards and security regulations, Information Security Technical Report, 26-31

[4] ISO/IEC-27001:2005. Information technology-Security techniques- Information security management systems- requirements. Switzerland :International Organization for Standardization (ISO).

[5] ISO/IEC-17799:2005. Information technology-Security techniques-Code of practice for information security management. Switzerland :International Organization for Standardization (ISO).

[6] ISO/IEC-27005:2011. Information technology-Security techniques- Information security risk. Switzerland :International Organization for Standardization (ISO); 2011

[7] Boritz,J.E.,(2005) Is practitioners’ views on core concepts of information integrity, International Journal of Accounting Information Systems, 6 (4), pp. 260–279

[8] Solms, B.V. (2005) “Information Security governance: COBIT or ISO 17799 or both?”. Computer & Security, 24, 99-104

[9] Broderick J.S., (2006). “ISMS, security standards and security regulations”. Science Direct., 26-31

[10] Yin, R.K., (1994). Case study research: design and methods. 2nd edition. Thousand Oaks, CA:Sage

[11] COBIT.3rd ed. Framework July 2000. ISACA. Information Security Management Systems Informational User Group,

[12] สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2552). แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 2) ของประเทศไทย ปีพ.ศ. 2552-2556, พิมพ์ครั้งที่ 1: สิงหาคม 2556