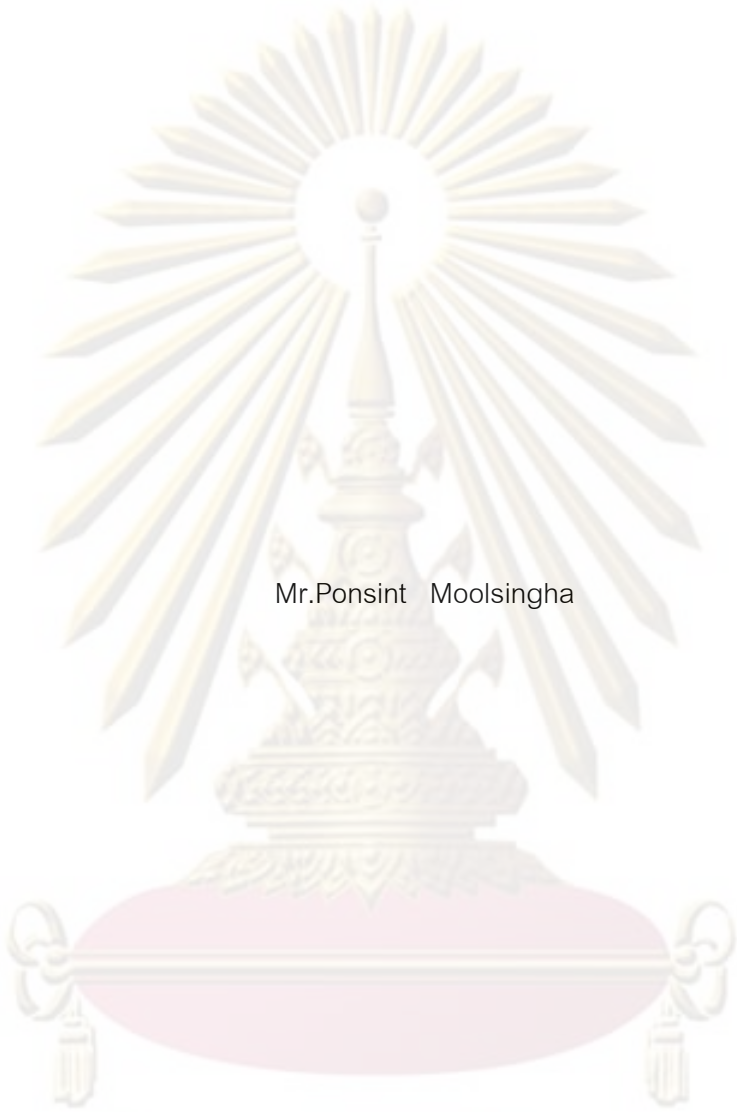
แนวทางของรูปแบบความมั่นคงปลอดภัยสำหรับจัดจ้างการบริการภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง

นายพลสินธ์ มูลสิงห์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2552

SECURITY GUIDELINE FOR OFF-PREMISE SERVICE OUTSOURCING

Mr.Ponsint Moolsingha



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 2009

หัวข้อวิทยานิพนธ์	แนวทางของรูปแบบความมั่นคงปลอดภัยสำหรับจัดจ้างการบริการภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง
โดย	นายพลสินธ์ มูลสิงห์
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	อาจารย์ ดร.ยรรยง เต็งอำนวย

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์ จารุมาตร ปิ่นทอง)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... กรรมการ
(อาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์)

..... กรรมการภายนอกมหาวิทยาลัย
(อาจารย์ ดร.โกเมน พิบูลย์โรจน์)

พลสินธ์ มูลสิงห์ : แนวทางของรูปแบบความมั่นคงปลอดภัยสำหรับจัดจ้างการบริการภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง. (SECURITY GUIDELINE FOR OFF-PREMISE SERVICE OUTSOURCING) อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก : อ.ดร. ยรรยง เต็งอำนวย, 84 หน้า.

ในปัจจุบันบริษัทหรือองค์กร ซึ่งเป็นผู้ว่าจ้างขนาดใหญ่ไม่อาจปฏิเสธได้ว่า การจัดจ้างภายนอกเพื่อบริการด้านระบบงานสารสนเทศแก่ลูกค้าของผู้ว่าจ้างนั้น เป็นหนึ่งในปัจจัยที่ขับเคลื่อนและขยายการเจริญเติบโตของผู้ว่าจ้าง ดังนั้นการป้องกันข้อมูลของผู้ว่าจ้างเป็นเรื่องที่ต้องให้ความสำคัญเป็นระดับต้น ๆ

แต่เนื่องจากการจัดจ้างภายนอกเพื่อทำระบบเทคโนโลยีสารสนเทศนั้น การทำงานเกี่ยวกับข้อมูลของผู้ว่าจ้างเป็นเรื่องที่ต้องให้ความสำคัญ จึงต้องให้ผู้รับจ้างจากภายนอกเข้ามาติดตั้งอุปกรณ์ โปรแกรมปฏิบัติงาน และมีบุคลากรมาประจำอยู่ภายในเครือข่ายหรือที่ทำการของผู้ว่าจ้าง ซึ่งเป็นผลให้เกิดความเสี่ยงในด้านความมั่นคงปลอดภัยต่อผู้ว่าจ้างได้โดยเฉพาะอย่างยิ่งผู้ว่าจ้างที่มีระบบความมั่นคงปลอดภัยของข้อมูลสูง เช่น ธนาคาร สถาบันการเงิน อีกทั้งยังเป็นค่าใช้จ่ายที่สูงสำหรับผู้ว่าจ้าง และในส่วนของบริษัทที่ให้บริการจัดจ้างภายนอก โดยเฉพาะหากบริษัทมีจำนวนผู้ว่าจ้างในการให้บริการหลายราย ทำให้ต้องใช้ทรัพยากรซ้ำซ้อนกันเป็นจำนวนมาก ทั้งระบบเครื่อง กำลังคน และค่าใช้จ่ายในการเดินทาง เพื่อให้ตอบสนองความต้องการของผู้ว่าจ้างได้

ดังนั้นจึงควรมีรูปแบบในการบริการจัดจ้างภายนอกเพื่อทำระบบเทคโนโลยีสารสนเทศให้บริการแก่บุคคลากรของผู้ว่าจ้าง และลูกค้าของผู้ว่าจ้างโดยที่มีการติดตั้งเครื่องระบบงานและข้อมูลอยู่ภายนอกเครือข่ายหรือที่ทำการของผู้ว่าจ้าง มีระบบความมั่นคงปลอดภัยของข้อมูลของผู้ว่าจ้าง และผู้ว่าจ้างต้องสามารถควบคุมติดตามได้

เนื้องานของการวิจัยนี้จะทำให้ทราบแนวทางและรูปแบบในการให้บริการจัดจ้างภายนอกที่มีความน่าเชื่อถือและความมั่นคงปลอดภัยของรูปแบบการจัดจ้างภายนอกให้กับผู้ว่าจ้าง

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

ปีการศึกษา 2009

4971450321 : MAJOR COMPUTER SCIENCE

KEY WORD: OUTSOURCING / OFF-PREMISE / SECURITY MODEL / IT SECURITY GOVERNANCE FRAMEWORK / TRUST

PONSINT MOOLSINGHA : SECURITY GUIDELINE FOR OFF-PREMISE SERVICE OUTSOURCING. THESIS ADVISOR : YUNYONG TENGAMNUAY, Ph.D., 84 pp.

Presently, companies cannot deny that IT outsourcing for their customers is the key growth driver. Hence, data security will become the main issue to focus on.

In fact, Information technology management is a must. Therefore, IT outsourcing have to install hardware and software and maintain server in customers premise. This increases risk especially in data confidential firms such as banks or financial firms. Moreover, outsourcing usually has high cost and will cost more if there are many outsources due to redundant and duplicate resource.

As a result, any IT outsourcing firm should have a proper framework for employees of customers and their customers by setting up server and operating system external to customer premise which is safe, efficient, and controllable.

The purposes of this research is to provide about a security guideline for off-premise service outsourcing of IT service.

Department : Computer Engineering Student's signature .....
Field of study : Computer Science Advisor's signature .....
Academic year : 2009

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ ด้วยดี เนื่องมาจาก ความช่วยเหลืออย่างดียิ่งของท่าน อ.ดร.ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ได้สละเวลาให้คำปรึกษาแนะนำแนวทางเกี่ยวกับงานวิจัยอย่างดีตลอดมาจน เสร็จสมบูรณ์ และผู้วิจัยขอกราบขอบพระคุณคณะกรรมการสอบวิทยานิพนธ์ทุกท่านที่ได้ให้คำแนะนำ ข้อคิดเห็น ข้อเสนอแนะ และแนวทางในการพัฒนางานวิจัยนี้

ขอขอบคุณ ผู้ร่วมวิจัยทุกท่านที่ให้คำแนะนำประเด็นเกี่ยวกับความปลอดภัยในการจัดจ้างภายนอก และผู้ร่วมงานในบริษัททุกคนที่ให้คำแนะนำจึงทำให้สำเร็จลุล่วงเป็นอย่างดี

ขอขอบคุณ พี่ธุรการภาคฯ ทุกๆ คนที่ช่วยอำนวยความสะดวกในการทำงาน และช่วยตักเตือนแนะนำสิ่งดีๆ เสมอมา

สุดท้ายนี้ ขอกราบขอบพระคุณคุณพ่อคุณแม่ที่ให้โอกาสเราได้เกิด ได้เติบโต ได้เลี้ยงดูเป็นอย่างดี และคอยสนับสนุนในด้านการศึกษาเป็นอย่างดี และภรรยาที่ช่วยเหลือและให้กำลังใจเสมอมา

สารบัญ

บทที่ หน้า

สารบัญตาราง

สารบัญภาพ

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันบริษัทหรือองค์กร ซึ่งเป็นผู้ว่าจ้างขนาดใหญ่ไม่อาจปฏิเสธได้ว่า การจัดจ้างภายนอกเพื่อบริการด้านระบบงานสารสนเทศแก่ลูกค้าของผู้ว่าจ้างนั้น เป็นหนึ่งในปัจ จัยที่ขับเคลื่อนและขยายการเจริญเติบโตของผู้ว่าจ้าง ดังนั้นการป้องกันข้อมูลของผู้ว่าจ้างเป็นเรื่องที่ต้องให้ความสำคัญเป็นระดับต้น ๆ

แต่เนื่องจากการจัดจ้างภายนอกเพื่อทำระบบเทคโนโลยีสารสนเทศนั้น การทำงานเกี่ยวกับข้อมูลของผู้ว่าจ้างเป็นเรื่องที่ต้องให้ความสำคั ญ จึงต้องให้ผู้รับจ้างจากภายนอกเข้ามาติดตั้งอุปกรณ์ โปรแกรมปฏิบัติงาน และมีบุคลากรมาประจำอยู่ภายในเครือข่ายหรือที่ทำการของผู้ว่าจ้าง ซึ่งเป็นผลให้เกิดความเสี่ยงในด้าน ความมั่นคงปลอดภัย ต่อผู้ว่าจ้างได้โดยเฉพาะอย่างยิ่งผู้ว่าจ้างที่มีระบบ ความมั่นคงปลอดภัย ของข้อมูลสูง เช่น ธนาคาร สถาบันการเงิน อีกทั้งยังเป็นค่าใช้จ่ายที่สูงสำหรับผู้ว่าจ้าง และในส่วนของบริษัทที่ให้บริการจัดจ้างภายนอก โดยเฉพาะหากบริษัทมีจำนวนผู้ว่าจ้างในการให้บริการหลายราย ทำให้ต้องใช้ทรัพยากรซ้ำซ้อนกันเป็นจำนวนมาก ทั้งระบบเครื่อง กำลังคน และค่า ใช้จ่ายในการเดินทาง เพื่อให้ตอบสนองความต้องการของผู้ว่าจ้างได้

ดังนั้นจึงควรมีรูปแบบในการบริการจัดจ้างภายนอกเพื่อทำระบบเทคโนโลยีสารสนเทศให้บริการแก่บุคคลากรของผู้ว่าจ้าง และลูกค้าของผู้ว่าจ้างโดยที่มีการติดตั้งเครื่องระบบงานและข้อมูลอยู่ภายนอกเครือข่ายหรือที่ทำการของผู้ว่าจ้าง มีระบบความมั่นคงปลอดภัย ของข้อมูลของผู้ว่าจ้าง และผู้ว่าจ้างต้องสามารถควบคุมติดตามได้

เนื้องานของการวิจัยนี้จะทำให้ทราบแนวทางและรูปแบบในการให้บริการจัดจ้างภายนอกที่มีความน่าเชื่อถือและความมั่นคงปลอดภัยของรูปแบบการจัดจ้างภายนอกให้กับผู้ว่าจ้าง

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อนำเสนอ แนวทางการจัดการโครงสร้างระบบ ความมั่นคงปลอดภัยของการบริการจัดจ้างภายนอกให้บริการ ดูแลระบบสารสนเทศ ซึ่งติดตั้งอยู่ภายนอกที่ทำการของผู้ว่าจ้างโดยให้มีความมั่นคงปลอดภัยและมั่นคงน่าเชื่อถือในมุมมองของผู้ว่าจ้าง

1.3 ขอบเขตของการวิจัย

1. งานวิจัยนี้จะนำเสนอแนวทางการให้บริการจัดจ้างภายนอกในมุมมองในระดับผู้บริการระดับสูงเท่านั้น
2. งานวิจัยนี้จะนำเสนอแนวทางการให้บริการจัดจ้างภายนอกโดยเป็นระบบที่ติดตั้งอยู่นอกที่ทำการของผู้ว่าจ้าง
3. งานวิจัยนี้จะนำเสนอแนวทางการให้บริการจัดจ้างภายนอกในประเภทให้บริการดูแลระบบเทคโนโลยีสารสาเทศเท่านั้น
4. รูปแบบของผู้ว่าจ้างจำกัดเฉพาะสถาบันการเงินประเภทธนาคารแต่ไม่เปิดเผยชื่อหน่วยงาน
5. แนวทางรูปแบบการจัดจ้างภายนอกที่นำเสนอมีการเพิ่มประเด็นในส่วนที่เกี่ยวกับกฎหมายทางสื่ออิเล็คทรอนิกส์
6. รูปแบบการให้บริการจัดจ้างภายนอกจะอ้างอิงจาก โครงสร้างความมั่นคงปลอดภัยธรรมมาภิบาล (Information Security Governance Framework) สำหรับหน่วยงานบริการด้านสารสนเทศ

1.4 ขั้นตอนการวิจัย

1. รวบรวมและ ศึกษา ข้อมูล ของ การ จัดจ้างภายนอกเพื่อ ดูแล ระบบเทคโนโลยีสารสนเทศที่อยู่นอกที่ทำการของผู้ว่าจ้าง
2. ศึกษาทฤษฎีพื้นฐานของโครงสร้างความมั่นคงปลอดภัยธรรมมาภิบาล
3. รวบรวมข้อมูลกรณีศึกษาของธุรกิจธนาคารที่เกี่ยวข้องกับการจัดจ้างภายนอกที่มีประเด็นที่เกี่ยวข้อง และวิเคราะห์เปรียบเทียบข้อดีข้อเสียของการจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้าง
4. วิเคราะห์ประเด็นที่เกี่ยวข้องและสังเคราะห์รูปแบบการจัดจ้างภายนอกที่เหมาะสม
5. วิเคราะห์และวิจารณ์รูปแบบการจัดจ้างภายนอกที่สังเคราะห์ขึ้นรวมถึงสรุปผล
6. เรียบเรียงวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับจากงานวิจัย

1. ผู้ให้บริการจัดจ้างภายน อกสามา รถนำแนวทางไปใช้กับองค์กรเพื่อสร้างความน่าเชื่อถือให้กับผู้ว่าจ้างที่ต้องการความมั่นคงปลอดภัยของข้อมูลสูง

2. สร้างความน่าเชื่อถือใน การบริการจัดจ้างภายนอกที่มีการให้บริการอยู่ภายนอกที่ทำการของผู้ว่าจ้าง
3. ผู้ให้บริการจัดจ้างภายนอกสามารถนำแนวทางไปใช้เพื่อลดทรัพยาก ร และค่าใช้จ่ายในการให้บริการจัดจ้างภายนอกได้
4. ผู้ว่าจ้างสามารถทราบแนวทางในการเลือกผู้ให้บริการจัดจ้างภายนอกได้อย่างมีประสิทธิภาพ

1.6 โครงสร้างของวิทยานิพนธ์

เนื้อหาของวิทยานิพนธ์ฉบับนี้ถูกแบ่งออกเป็น 6 บท ดังนี้คือ บทที่ 1 เป็นบทนำ บทที่ 2 กล่าวถึงทฤษฎีแล ะงานวิจัยที่เกี่ยวข้อง บทที่ 3 กล่าวถึงการดำเนินงานวิจัย โดยอธิบายเป็นขั้นตอนต่างๆ ส่วนในบทที่ 4 เป็นการสังเคราะห์การจัดจ้างภายนอก บทที่ 5 ผลจากการประเมินและท้ายสุดคือบทที่ 6 เป็นการสรุปผลและข้อเสนอแนะของงานวิจัย ซึ่งอาจจะเป็นประโยชน์ต่องานวิจัยอื่นๆ ต่อไปในอนาคต

1.7 คำจำกัดความที่ใช้ในการวิจัย

NISCC (National Infrastructure Security Co-ordination Centre) ซึ่งปัจจุบันได้มีการเปลี่ยนชื่อเป็น CPNI (Centre for the Protection of National Infrastructure) เป็นหน่วยที่ได้รับอนุญาตจากประเทศอังกฤษ ในการให้คำแนะนำที่ เกี่ยวกับการป้องกัน ความมั่นคงปลอดภัยให้กับหน่วยงานของรัฐ และองค์กรทางธุรกิจ และเกี่ยวกับโครงสร้างการเชื่อมโยงข้ามประเทศอีกด้วย โดยวัตถุประสงค์ขององค์กรเพื่อลดช่องโหว่ให้กับโครงสร้างที่อาจถูกโจมตีจากผู้ไม่ประสงค์ดี และการโจมตีจากภายนอกประเทศ เป็นองค์กรที่ มีบุค ลากรที่มีความรู้ มีประส บการณ์ด้านความปลอดภัย ซึ่งบุค ลากรขององค์กรนั้นมาจากหลากหลายหน่วยงาน ทั้งหน่วยงานภาครัฐ และจากหน่วยงานภาคเอกชน เพื่อให้บริการเกี่ยวกับให้ความรู้ด้านความมั่นคงปลอดภัย

โครงสร้างความมั่นคงปลอดภัยธรรมมาภิบาล หมายถึง โครงสร้างความมั่นค งปลอดภัยธรรมมาภิบาล ซึ่งเป็นโ ครงสร้างแนวทางในการรักษาความมั่นคงปลอดภัย ที่ดี โดยการจัดการระบบความมั่นคงปลอดภัยที่ดี ซึ่งกรอบงานที่จำนำธรรมาภิบาลเข้าไปเกี่ยวข้องกับเรื่องต่าง ๆ ที่สำคัญมีอยู่ 6 ด้านดังนี้ 1) หน้าที่ความรับผิดชอบ 2) การริเริ่มในทางที่ถูกต้อง 3) โปร่งใส 4) มีผู้รับผิดชอบชัดเจน 5) มีความยั่งยืน และ 6) การประเมินตัวเอง การมี โครงสร้างความมั่นคง

ปลอดภัยธรรมมาภิบาล นั้นเป็นตัวพลักดันให้วัตถุประสงค์ในการดำเนินงานด้านความมั่นคงปลอดภัยบรรลุวัตถุประสงค์ และวิสัยทัศน์ได้อย่างแน่นอน

เทคโนโลยีสารสนเทศ (Information Techonogy) หมายถึง เทคโนโลยี สำหรับ การประมวลผลสารสนเทศ ซึ่งครอบคลุมถึงการรับ-ส่ง การแปลง การจัดเก็บ การประมวลผล และการค้นคืนสารสนเทศ ในการประยุกต์ การบริการ และพื้นฐานทางเทคโนโลยี สามารถแบ่งกลุ่มย่อยเป็น 3 กลุ่ม ได้แก่ คอมพิวเตอร์ , การสื่อสาร แล ะข้อมูลแบบมัลติมีเดีย ซึ่งในแต่ละกลุ่มนี้ยังแบ่งเป็นกลุ่มย่อยๆ ได้อีกมากมาย องค์ประกอบทั้ง 3 ส่วนนี้ ยังต้องอาศัยการทำงานร่วมกัน ยกตัวอย่างเช่น เครื่องเซิร์ฟเวอร์คอมพิวเตอร์ (คอมพิวเตอร์) เป็นองค์ประกอบสำคัญของ ระบบเครือข่าย (การสื่อสาร) โดยมีการส่งข้อมูลต่างๆ ไปยังเครื่องลูก (ข้อมูลแบบมัลติมีเดีย)

การบริการจัดจ้างภายนอก (Outsourcing) คือกระบวนการที่องค์กรใดองค์กรหนึ่งที่จะมอบหมายการบริหาร ดำเนินการ โครงการหรือการบริการที่องค์กรนั้น ๆ จะต้องทำให้กับบุคคลภายนอกที่มีความชำนาญในด้านนั้น ๆ มาดำเนินการแท นโดยองค์กรนั้น ๆ จะเป็นผู้กำหนดนโยบายบริหารและการกำหนดคุณภาพของการให้บริการของผู้ให้บริการ จัดจ้างภายนอก ปัจจุบันในประเทศไทยได้มีการให้บริการจัดจ้างภายนอก ด้านระบบสารสนเทศ หลายรูปแบบ ได้แก่

— การบริการเครื่องคอมพิวเตอร์ (Desktop Service) เป็นการดูแลเครื่องคอมพิ วเตอร์ Desktop เครื่อง Server และระบบเครือข่ายท้องถิ่น (LAN) ซึ่งเป็นส่วนที่ผู้ใช้บริการด้านสารสนเทศของหน่วยงานนั้นๆจะต้องได้รับบริการจากส่วนงานที่ให้บริการขององค์กรนั้นๆ ขอบเขตของการบริการนี้ยังแบ่งเป็นหลายระดับ โดยเริ่มตั้งแต่การวางแผนการวางระบบของผู้ว่ าจ้าง การดำเนินการติดตั้งทดสอบระบบงานต่างๆ การตอบปัญหาการใช้งานของเครื่อง PC ในลักษณะการบริการ ณ. จุดเดียว (SPOC-Single Point Of Contact) การดูแลบำรุงรักษาซ่อมแซมเมื่อเครื่องชำรุด ไปจนถึงการซึ่งอาจจะรวมถึงการจัดซื้อ ติดตั้ง และการเปลี่ยนเครื่องให้ทันสมัยแ ละพร้อมที่จะใช้งานกับระบบงานใหม่ๆอยู่ตลอดเวลาเป็นต้น ซึ่งผู้ว่าจ้างสามารถเลือกระดับการให้บริการจากผู้ให้บริการตามความจำเป็นได้

— การบริการเชื่อมต่อและจัดการเครือข่ายสื่อสาร (Network Management / Networking & Connectivity Service) เป็นการบริหาร จัดการให้องค์กรสามารถใช้งานเครือข่ายสื่อสารคอมพิวเตอร์เพื่อเชื่อมโยงการทำงานระหว่างส่วนงานต่าง ๆ ขององค์กร หรือระหว่างองค์กรได้อย่างมีประสิทธิภาพสูงสุด โดยที่ผู้รับจ้างจะทำหน้าที่บริหารระบบเครือข่ายการสื่อสารของผู้

ว่าจ้างซึ่งอาจจะรวมถึงการจัดหา ติดตั้งอุปกรณ์สื่อสารต่า งๆตามที่ผู้ว่าจ้างต้องการให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา

— การบริการศูนย์คอมพิวเตอร์ เป็นการบริการที่ครอบคลุมการบริหารจัดการศูนย์คอมพิวเตอร์ให้สามารถดำเนินการได้อย่างมีประสิทธิภาพสูงสุด การบริการอาจครอบคลุมถึงการออกแบบ จัดหาอุปกรณ์คอมพิวเตอร์ ติดตั้ง รวมถึงการจัดหาบุคลากรที่มีความรู้ความชำนาญด้านการดำเนินการในศูนย์คอมพิวเตอร์มาดำเนินการบริหารศูนย์คอมพิวเตอร์แทนผู้ว่าจ้าง การดูแลระบบคอมพิวเตอร์ โดยที่ ระดับของคุณภาพของการให้บริการ จะถูกกำหนดโดยข้อตกลงระหว่างผู้ว่าจ้างและผู้ให้บริการและจะถูกควบคุมโดยผู้ว่าจ้าง

— การให้บริการด้านความต่อเนื่องการให้บริการเป็นการบริการเพื่อเพิ่มความมั่นใจให้กับผู้ว่าจ้างในความต่อเนื่องของการให้บริการขององค์กรนั้นๆว่าจะสามารถให้บริการได้อย่างต่อเนื่องมากที่สุด การบริการนี้อาจจะรวมถึงการออกแบบ ติดตั้ง บริหาร ศูนย์คอมพิวเตอร์สำรองขององค์กรนั้นเพื่อเป็นการเพิ่มความมั่นใจในการให้บริการในกรณีที่เกิดเหตุการณ์ฉุกเฉินหรือเกิดการเสียหายอย่างรุนแรงของศูนย์คอมพิวเตอร์หลัก การปรับปรุงเครื่องให้มีขนาดและความทันสมัยอยู่เสมอสามารถรองรับงานที่เพิ่มเติมได้

— การให้บริการด้านศูนย์คอมพิวเตอร์ของการบริ การนี้เป็นการให้บริการที่สามารถครอบคลุมเริ่มตั้งแต่การออกแบบ ติดตั้ง ดูแล ศูนย์คอมพิวเตอร์ที่ให้บริการ Web ซึ่งอาจจะรวมถึงการนำ Web Server ของผู้ว่าจ้างมาติดตั้งและดูแลการให้บริการด้าน อินเตอร์เน็ตขององค์กรนั้นๆ ผู้ให้บริการจัดจ้างภายนอกของบริการนี้ส่วนใหญ่เป็นผู้ให้บริการด้านอินเตอร์เน็ตเดิมอยู่แล้ว

— การให้บริการด้านการบริหารระบบงานการบริการนี้เป็นการให้บริการด้านการบริหารโปรแกรมระบบงานต่างๆขององค์กรนั้นๆซึ่งอาจจะเริ่มตั้งแต่ออกแบบ พัฒนา ติดตั้ง ดูแลโปรแกรมระบบงานนอกจากนี้อาจจะรวมถึงการตอบปัญหาด้านโปรแกรม การจัดการบริหาร ของโปรแกรมระบบงานต่างๆ

ความเสี่ยง (Risk) หมายถึงสถานการณ์ที่เกิดขึ้นโดยอาจ มีผลกระทบเป็นอุปสรรคต่อการบรรลุเป้าหมายขององค์กร ความเสี่ยงนี้วัดได้จากความบ่อยครั้งที่เกิด และความน่าจะเป็น รวมถึงเหตุการณ์ไม่แน่นอนที่อาจเกิดขึ้น ซึ่งหากเกิดขึ้นจะมีผลกระทบในเชิงลบต่อการบรรลุวัตถุประสงค์หรือภารกิจขององค์กร หรือโอกาสที่จะเกิดความสูญเสีย หรือสิ่งที่ไม่คาดหวัง ไม่พึงประสงค์จากการดำเนินงาน ตัวอย่างของความเสี่ยงเช่น ภัยธรรมชาติ การก่อการร้าย ความเสียหายของระบบเทคโนโลยีสารส นเทศ บุคลากรไม่มีความรู้และประสบ การณ์ที่เหมาะสมอย่างเพียงพอต่อองค์กร

ดังนั้นควรมีกิจกรรมควบคุม มีทั้งเชิงป้องกันแก้ไข การอำนวยการหรือกำหนดในระดับนโยบา ย
รวมถึงการลดหรือถ่ายโอนความเสี่ยง

BSC (Balanced Scorecard) หมายถึง เครื่องมือการจัดการที่ช่วยในกา รนำกลยุทธ์สู้การปฏิบั ติ โดยการวัดหรือประ เมิณที่ทำให้องค์กรเกิดความสอดคล้องเป็นอันหนึ่งอันเดียวกัน และมุ่งเน้นในสิ่งที่สำคัญต่อความสำเร็จขององค์กร โดยกำหนดมุมมอง 4 ด้านที่จะแสดงให้เห็นความสำคัญด้านต่าง ๆ ขององค์กรดังนี้ 1) มุมมองด้านการเงิน 2) มุมมองด้านลูกค้าภายนอก 3) มุมมองด้านกระบวนการภายใน และ 4) มุมมองด้านนวัตกรรมและการเรียนรู้

SLA (Service Lavel Agreement) คือ พันธะสัญญาในการให้บริการของหน่วยงานบริการในแต่ละองค์กร โดยมีการกำหนดระดับของการให้บริการไว้อย่างชัดเจนและรับรู้โดยทั่วกัน ซึ่งคำว่า ระดับของการให้บริการนั้น ครอบคลุมถึงลักษณะของการให้ บริการ ลำดับความสำคัญ อำนาจหน้าที่รับผิดชอบ และการรับประกัน อาจกล่าวได้อีกนัยหนึ่งว่า SLA คือข้อตกลงในรูปแบบของเวลาหรือประสิทธิภาพการส่งมอบงานบริการให้กับลูกค้า โดยในปัจจุบัน SLA มีผลกระทบต่อการเลือกใช้บริการเพราะถือเป็นตัวชี้วัดศักยภาพของผู้ให้บริการ ซึ่งในแต่ละบริการอาจจะมี SLA มากกว่า 1 แบบ หรือไม่มีเลยก็ได้

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

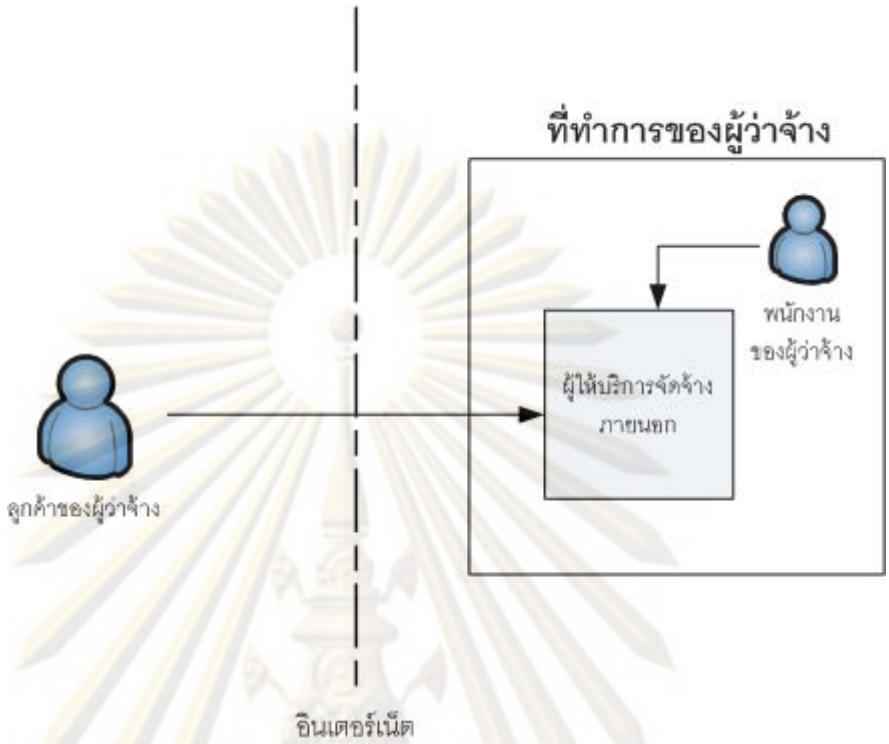
2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 การจัดจ้างภายนอกเพื่อทำระบบเทคโนโลยีสารสนเทศ

ในปัจจุบันพบว่า ทุกผู้ว่าจ้างเริ่มให้ความสำคัญกับงานทางด้านไอที และมีการลงทุนทั้งด้านเครื่องมืออุปกรณ์ ฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่าย รวมถึงการพัฒนาบุคลากรเป็นจำนวน มาก [6] ขณะเดียวกันแรงผลักดันของระบบเศรษฐกิจใหม่ที่พึ่งพาข้อมูลข่าวสารมากขึ้น ทำให้ผู้ว่าจ้างส่วนใหญ่ไม่ได้มีสายการผลิตหรือเป้าหมายหลักที่เกี่ยวกับเทคโนโลยีสารส นเทศเป็นผลให้เกิดขาดแคลนบุคลากรที่มีความรู้ความสามารถดังจะเห็นได้จากการตั้งแผนกไอทีใน องค์กรของผู้ว่าจ้าง ซึ่งหาบุคลากรได้ยากเพราะผู้มีความรู้ความสามารถไม่อยาก ทำงาน ในหน่วยงานไอทีเหล่านั้นทำให้งานทางไอทีไม่ประสบผลสำเร็จถ้าองค์กรทำการพัฒนาและดำเนินงานเหล่านี้เอง

ดังนั้นองค์กรต่าง ๆ จึงเริ่ม ให้ความสนใจ หน่วยงานให้บริการจากภายนอก ซึ่งอาจเป็นบริษัท หรือธุรกิจที่ให้บริ การพัฒนาเทคโนโลยีสารสนเทศ เป็นบริษัทที่มีความรู้ความชำนาญสามารถพัฒนาระบบงานให้เสร็จได้เร็ว มีคุณภาพ และควบคุมค่าใช้จ่ายได้ การว่าจ้างหน่วยงานหรือบริษั ทภายนอกในการพัฒนาระบบงานทางด้านไอทีแทนการพัฒนาหน่วยงาน ด้านนี้ ของตนเอง เช่นนี้เรียกว่า การจัดจ้างภายนอก การเรียกใช้บริการในลักษณะนี้เริ่มเป็นที่รู้จักกันมากขึ้นและมีบริษัทเข้ามาดำเนินธุรกิจจำพวกนี้มากขึ้น [6]

ปัจจุบัน ความต้องการในการใช้งานทางด้านระบบเทคโนโลยี สารสนเทศมีความหลากหลาย มากขึ้น เช่นการตั้งเว็บไซต์ให้กับผู้ว่าจ้าง การบริหารเซิร์ฟเวอร์ การทำระบบบริการลูกค้า เช่น ระบบออนไลน์ในรูปแบบ eservice ต่าง ๆ ดังนั้นจึงมีการดำเนินการโดยบริษัทที่ให้บริการจัดจ้างภายนอกมีการดูแลฮาร์ดแวร์ ซอฟต์แวร์ เซิร์ฟเวอร์ เครือข่าย และสถานีบริการต่าง ๆ ให้ทั้งหมด โดยให้ผู้ว่าจ้างเป็น ผู้ใช้งาน โครงสร้าง ในระบบธุรกิจของ การบริการจึงมีรูปแบบเป็นการเชื่อมโยงผ่านทางเครือข่ายดังรูปที่ 2.1



รูปที่ 2.1 การให้บริการผ่านการจัดจ้างภายนอก

2.1.2 มาตรฐานสากลต่าง ๆ ที่ว่าด้วยการบริหารความเสี่ยง

มาตรฐานสากลต่าง ๆ ที่ว่าด้วยการบริหารความเสี่ยง มีอยู่หลายมาตรฐานด้วยกัน ซึ่งมีลักษณะที่แตกต่างกันไปโดยมีลักษณะดังนี้

— มาตรฐาน NIST 800-30 [10] นั้น จะเน้นเรื่อง การกำหน ด ภัยที่จะเกิดขึ้น และ ช่องโหว่ ของระบบให้ไ ด้เสียก่อน จากนั้นจึงดูโอกาสของความเสี่ยงที่ อาจจะเกิดขึ้ น ประกอบกับ ผลกระทบจากความเสี่ยงดังกล่าว ตลอดจนถึงวิธีการแก้ไขปัญหา ของความเสี่ยง ในรูปแบบต่าง ๆ

— มาตรฐาน OCTAVE [11] ของ SEI นั้นจะเน้นไปที่ “คน และ กระบ วนการ” โดยมีการทำเวิร์คช็อปเป็นทีม ประกอบด้วย ทั้งผู้บริหาร และฝ่ายปฏิบัติการจากส่วนของกา รรักษา ความมั่นคงปลอดภัย ข้อมูลคอมพิวเตอ ร์ และจากส่วนของการบริหารธุรกิจซึ่ง OCTAVE จะมีการใช้แบบสอบถามในการสอบถามทีมที่เข้า ร่วมเวิร์คช็อบ เพื่อที่จะให้ทุกคนได้เข้าใจ เรื่องของความเสี่ยง และรู้จักวิเคราะห์ ผลกระทบของความเสี่ยงที่อาจเกิดขึ้น ซึ่ง OCTAVE จะลง รายละเอียดได้ดีกว่า NIST 800-30 เพราะผู้ร่วมทีมแต่ละคนจะมีความเข้าใจ กระบวนการ ที่ตัวเอง รับผิดชอบอยู่ได้เป็นอย่างดี

– มาตรฐาน AS / NZC 4630:2004 [12] นั้นจะครอบคลุมเนื้อหาด้านการบริหารความเสี่ยงที่กว้างกว่า NIST 800-30 และ AS/NZS 4360:2004 จะเน้นเรื่องของสถานะการณ์ด้านการเงิน ความมั่นคงปลอดภัย ของพนักงาน และความเสี่ยง ในการตัดสินใจทางธุรกิจของผู้บริหารด้วย องค์กรที่มีความจำเป็นต้อง “การยอมทำตาม” กฎหมาย SOX HIPAA และ GLBA นั้นมักจะเริ่มที่มาตรฐาน NIST 800-30 ก่อน จากนั้นก็ค่อ ยปรับลงรายละเอียดเข้าสู่มาตรฐาน OCTAVE ซึ่งใช้เวลามากกว่า แต่จะได้ผลดีตรงการทำเวิร์คช็อบ ที่ความต้องการด้านความมั่นคงปลอดภัยและความต้องการด้านการดำเนินธุรกิจได้มาปรับให้เข้ากัน และเหมาะสมกับการดำเนินงานขององค์กร

– ISO/IEC 17799 และ ISO/IEC 27001 [13] ถือได้ว่าเป็นมาตรฐานสากล (International Standard) ด้านการบริหารจัดการเรื่องความมั่นคงปลอดภัย ข้อมูล ซึ่งจะครอบคลุมเรื่องสำคัญต่าง ๆ อาทิเช่น การควบคุมด้าน ความมั่นคงปลอดภัย และ การบริหารจัดการสิ่งที่จะเกิดขึ้นด้านความมั่นคงปลอดภัยซึ่งวัตถุประสงค์ของการบริหารความเสี่ยงระบบสารสนเทศซึ่งก็คือการลดความเสี่ยงให้อยู่ในจุดที่ยอมรับได้

– ITIL [14] จัดว่าเป็นการรวบรวมเอาความรู้ที่มีอยู่แล้วในการบริหารจัดการศูนย์ฯ ซึ่งได้ถูกนำไปใช้แล้วในวงการอุตสาหกรรมต่างๆที่จำเป็นต้องใช้ไอที ในช่วงเวลาหลายสิบปีที่ผ่านมา ITIL จึงถูกเรียกว่าเป็น Best Practice ของการบริหารจัดการ ไอที ซึ่งในเวลาต่อมาได้มีการกล่าวถึง ITIL ในแง่ที่เป็นโครงสร้างการบริหารการบริการด้านไอที กันอย่างแพร่หลาย และได้กลายเป็น de facto standard ไปในปัจจุบัน ประโยชน์จากการนำความรู้ ITIL มาใช้ นั้น คือประโยชน์ที่เกิดขึ้นจากการที่สามารถปรับปรุงกระบวนการให้ดีขึ้น มีประสิทธิภาพมากขึ้นนั่นเอง

2.1.3 กรอบโครงสร้างระบบภิบาลด้านความมั่นคงปลอดภัยสารสนเทศ [9]

ปัจจุบันความสำคัญของข้อมูลสารสนเทศนั้นเป็นที่ยอมรับกันอย่างกว้างขวาง และระบบสารสนเทศนั้นปัจจุบันได้นำมาใช้กันอย่างแพร่หลายกับทุกบริ ษัทหรือองค์กรทั่วไป ในการเติบ โตขององค์กรนั้น ๆ ต้องอาศัยระบบสารสนเทศอีกด้วย แต่ก็มีโอกาสให้เกิดความเสี่ยงตามมากับประโยชน์ที่ได้รับอีกด้วย ดังนั้นจึงต้องมีระบบการจัดการที่ครอบคลุมภัยที่จะเกิดขึ้นกับระบบสารสนเทศในทุก ๆ ด้านของบริษัทหรือองค์กร คณะกรรมการและผู้บริหารต้องการความมั่นใจว่าได้มีการจัดการกับความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศรวมอยู่ในนโยบายและแผนขององค์กรแล้ว อีกทั้งต้องมีความเหมาะสมและเป็นประโยชน์สูงสุดกับบริษัทหรือองค์กร

ผู้บริหารมีหน้าที่ในการทำให้แน่ใจว่าองค์กรนั้นสามารถให้ ความมั่นคงปลอดภัย ระบบสารสนเทศแก่ผู้ใช้ได้ (ผู้ใช้ภายในองค์กรและผู้ใช้ภายนอกองค์กร) อย่างเท่าเทียมกัน นอกจากนั้นองค์กรเองมีความต้องการที่จะป้องกันจากความเสี่ยงที่จะเกิดขึ้นจากการใช้ระบบสารสนเทศ ถึงแม้ว่าจะเกิดขึ้นพร้อมกับประโยชน์ที่จะได้รับ

ดังนั้นการเพิ่มของการใช้ระบบสารสนเทศมากขึ้นทำให้เกิดโอกาสที่เป็ นอันตรายกับระบบความมั่นคงปลอดภัย สารสนเทศได้ จึงนำไปสู่ความจำเป็นต้องมีระบบภิบาลด้าน ความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพ

เพื่อให้ระบบภิบาลด้านความมั่นคงปลอดภัยมีประสิทธิภาพนั้นต้องมีการนำการจัดการด้านความมั่นคงปลอดภัย สารสนเทศ (ISM-Information Security Management System) ที่เป็นมาตรฐานสากล เพื่อ ในการรักษาความมั่นคงปลอดภัยของผู้ให้บริการ เช่น

- การควบคุมระยะไกล และการแบ่งปันระบบ
- ระบบการจัดเก็บ และการสำรองข้อมูล
- กระบวนการและมาตรการ การเรียกคือข้อมูล
- การเข้าถึงระบบและการจัดการกำหนดสิทธิ

สิ่งที่จะได้รับจา กการที่มีระบบภิบาลด้าน ความมั่นคงปลอดภัย สารสนเทศ ระบบภิบาลด้านควมปลอดภัยสารสนเทศ ถ้ามีการจัดการอย่างเหมาะสมจะได้ประโยชน์ 4 ข้อพื้นฐานดังต่อไปนี้

1. แนวทางของนโยบายและแผน
   - จะได้ความต้องการด้านระบบ ความมั่นคงปลอดภัย สารสนเทศที่ได้ มาจากความต้องการขององค์กร
   - แนวทางการแก้ปัญหาระบบ ความมั่นคงปลอดภัย สารสนเทศที่เหมาะสมกับกระบวนการขององค์กร
   - การลงทุนในระบบ ความมั่นคงปลอดภัย สารสนเทศให้อยู่ในแนวเดียวกับนโยบายและแผนขององค์กรที่ได้ยอมรับไว้บนรูปแบบความเสี่ยงที่เกิดขึ้น
2. ประโยชน์ที่ได้รับ
   - มีมาตรฐานของวิธีปฏิบัติด้านระบบความมั่นคงปลอดภัย
   - มีการจัดลำดับอย่างเหมาะสม กระจายการทำงานในส่วนที่มีผลกระทบมากที่สุดเพื่อประโยชน์สูงสุด
   - แนวทางทั้งหมด ครอบคลุมกระบวนการทั้งองค์กรเช่นเดียวกับเทคโนโลยี

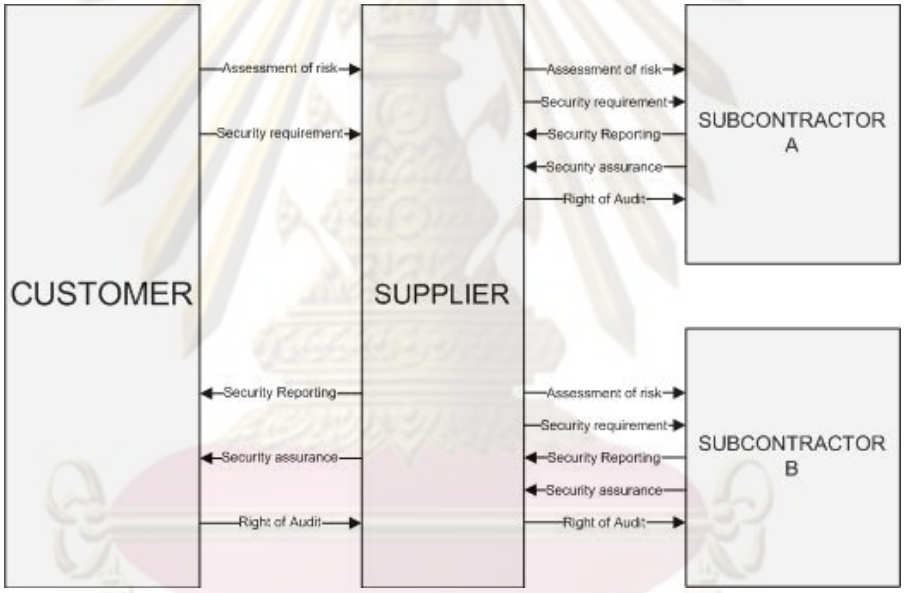
- มีการพัฒนาปรับปรุงแก้ไขอย่างต่อเนื่อง

3. การจัดการความเสี่ยง

- มีการยอมรับในรูปแบบของความเสี่ยงที่อาจเกิดขึ้น
- เข้าใจในความเสี่ยงที่อาจเกิดขึ้น
- รับรู้ความสามารถในการจัดการด้านความเสี่ยงที่อาจเกิดขึ้นล่วงหน้า

4. การวัดความสำเร็จ

- กำหนดมาตรในการวัด
- กระบวนการตวจสอบกับผลตอบรับจากกระบวนการที่สร้างขึ้น



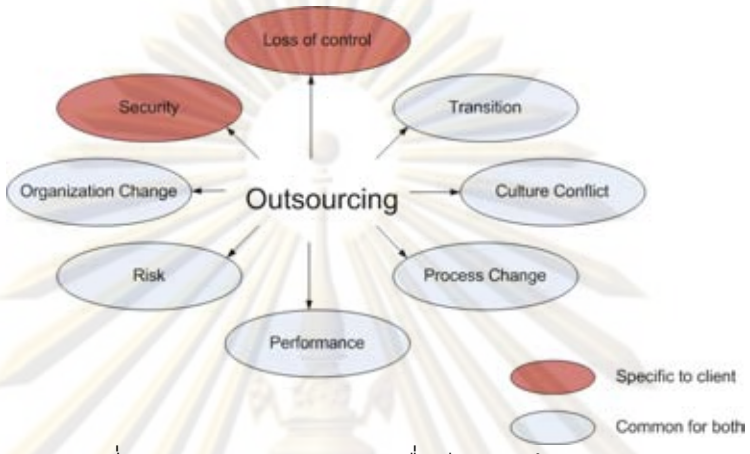
รูปที่ 2.2 รูปแบบของกระบวนการการจัดการด้านระบบความมั่นคงปลอดภัยสารสนเทศ [8]

2.2 งานวิจัยที่เกี่ยวข้อง

ซอมเมอร์ [1] ได้นำเสนอรูปแบบการให้บริการที่มีความยืดหยุ่นที่จะสามารถเชื่อมต่อกั บระบบอีอาพี(ERP – Enterprise Resource Plan) ได้ง่ายและมีความมั่นคงปลอดภัย ซึ่งสามารถนำไปใช้กับการทำการจัดจ้างภายนอกโดยผู้ให้บริการจัดจ้างภายนอกอยู่นอกที่ทำการของผู้ว่าจ้าง

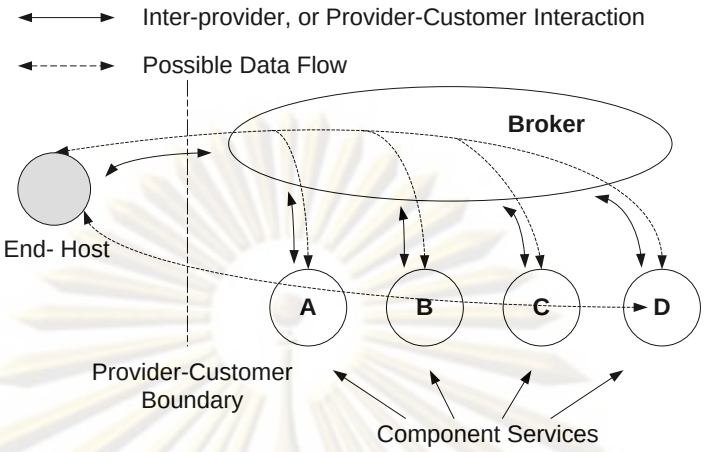
ฟานจิงเมียง และคณะ [5] ได้นำเสนอผลกระทบกับองค์ กร เมื่อมีการจัดจ้างภายนอก และแนวทางการจัดการของการจัดจ้างภายนอกโดยการใช้ โครงสร้างความมั่นคงปลอดภัยธรรม

มาภิบาลในการบริหารการจัดจ้างภายนอกเพื่อลดความ เสี่ยงที่จะเกิดขึ้นกับองค์กรเนื่องจากมีการจัดจ้างภายนอกดังรูปที่ 2.3



รูปที่ 2.3 ผลกระทบกับธุรกิจเมื่อมีการจัดจ้างภายนอก

รามาน และคณะ [4] ได้นำเสนอโครงสร้างของการผนวกการให้บริการของ Application Service Provider (ASPs) โดยมีการให้บริการร่วมกันแก่ลูกค้าโดยใช้ Broker Model คือรูปแบบการร่วมกันให้บริการของผู้ให้บริการ หลายรายโดยมีผู้ให้บริการ รายหนึ่งทำหน้าที่เป็นตัวแทนและทำหน้าที่ให้บริการเพื่อประโยชน์ของผู้ว่าจ้าง ดังแสดงในรูปที่ 4 โดยผู้ให้บริการที่แท้จริงอยู่ภายใต้ของผู้ให้บริการที่ทำหน้าที่เป็นตัวแทน ซึ่งเรียกว่า broker ทำงานแบบ end to end Service นายหน้ารับหน้าที่เป็นผู้รวบรวมการบริการ ซึ่ง broker จะให้บริการตามลักษณะงานของแต่ละผู้ให้บริการที่อยู่ภายใต้ นายหน้า เพราะลักษณะการให้บริการ ของแต่ละผู้ให้บริการ ที่อยู่ภายใต้นายหน้า เดียวกันอาจไม่เชื่อถือซึ่งกันและกัน ซึ่งเป็นข้อ จำกัดของการแลกเปลี่ยนข้อมูลภายในระบบนายหน้า



รูปที่ 2.4 ระบบนายหน้า

รูปที่ 2.4 แสดงการทำงาน ระบบนายหน้า ซึ่งแสดง กระแสข้อมูล ของ การให้บริหาร ผู้ให้บริการแต่ละรายที่วิ่งสู่นายหน้าแสดงดังเส้นประที่อยู่ด้านบน และ นายหน้าสามารถกำหนด การแลกเปลี่ยนข้อมูลให้เป็นไปตาม ส่วนข้อมูลที่แสดงดังเส้นประที่อยู่ด้านล่าง

แทนจา และสเตฟาน [17] ได้นำเสนอ aplication service provider ในการให้บริการที่มีประสิทธิภาพ เพื่อตอบสนองการทำ supply chain management และมีการนำเสนอแนวทางการทำ SLA ที่อ้างอิงจากสถาบัน ITAA

สถาบัน NICC นำเสนอ รูปแบบแนวทางการจัดการความมั่นคงปลอดภัยของการจัดจ้างภายนอก [8] โดยนำเสนอแนวทางด้านความปลอดภัยสำหรับการจัดจ้างภายนอกหน่วยงานด้านเทคโนโลยีสารสนเทศ

2.3 โครงสร้างของกรณีศึกษา

หน่วยงานที่ใช้เป็นกรณีศึกษามีหลายส่วนซึ่งมีรายละเอียดดังนี้

1. กรณีศึกษาส่วนของผู้ว่าจ้าง เป็น ธนาคารที่ให้บริการในประเทศไทยไทย เริ่มก่อตั้งเมื่อวันที่ 8 มิถุนายน พ.ศ.2488 ด้วยทุนจดทะเบียน 5 ล้านบาท ด้วยพนักงานชุดแรกเริ่มเพียง 21 คน มีการเติบโตอย่างมั่นคง มีสาขาในประเทศจำนวน 721 สาขา โดยเป็นสาขากรุงเทพมหาน คร 245 สาขา สาขาในส่วนภูมิภาคจำนวน 476 สาขา และมีสาขาหรือสำนักงานตัวแทนต่างประเทศ 7 แห่ง ได้แก่ สาขา ลอสแองเจลิส สาขาฮ่องกง สาขาหมู่เกาะเคย์แมน สาขาเซินเจิ้น สำนักงานผู้แทนกรุงปักกิ่ง สำนักงานผู้แทนนครเซี่ยงไฮ้ และสำนักงานผู้แทนเมืองคุนหมิง สาขาและสำนักงาน ผู้แทนในต่างประเทศเหล่านี้ให้บริการและส่งเสริมความสะดวกต่างๆ ด้านการค้า

การเงินระหว่างประเทศไทยและประเทศคู่ค้าทั่วโลก โดยมีความมุ่งมั่นในการเป็นสถาบันการเงินไทยที่แข็งแกร่ง สามารถตอบสนองความต้องการของลูกค้าด้วยบริการด้านการเงินที่หลากหลายครบถ้วน ในคุณภาพมาตรฐานสากล โดยผสมผสานการใช้เทคโนโลยีและทรัพยากรมนุษย์ ทั้งนี้เพื่อให้บรรลุผลที่ดีและเป็นธรรม ต่อลูกค้า ผู้ถือหุ้น พนักงาน และประเทศไทย

2. กรณีศึกษาส่วนของผู้ให้บริการจัดจ้าง ภายนอก เป็นบริษัทที่อยู่ในกลุ่มสนับสนุนงานให้แก่ธนาคารที่ให้บริการในประเทศไทย และกลุ่มบริษัทในเครือ โดยเริ่มต้นจาก ทุนจดทะเบียน 10 ล้านบาท ก่อตั้งขึ้นในวันที่ 16 มีนาคม พ.ศ. 2536 ซึ่งเป้าหมายของ คือ การให้บริการพัฒนาซอฟต์แวร์ การให้คำปรึกษา และการสนับสนุนงานด้านสารสนเทศให้แก่ธุรกิจการธนาคาร เงินทุนหลักทรัพย์และธรุกิจการประกัน เป็นต้ น และในปี พ.ศ. 2547 บริษัท ได้รับการรับรองมาตรฐานการพัฒนาซอฟต์แวร์คุณภาพ CAPABILITY MATURITY MODEL (SW-CMM) LEVEL 3 จากสถาบัน Software Engineering Institute (SEI) ของมหาวิทยาลัย Carnegie Mellon เมือง Pittsburgh, รัฐ Pennsylvania ประเทศสหรัฐอเมริกา ซึ่งเป็นสถาบันที่มีชื่อเสียงในด้าน Software Engineering เป็นที่ยอมรับจากทั่วโลก ได้ให้การรับรองว่าบริษัท มีกระบวนการพัฒนาซอฟต์แวร์ที่มีคุณภาพตามหลักสากล ซึ่งบริษัทประกาศใช้เป็นมาตรฐานองค์กรรวมทั้งนำไปสู่การปรับปรุงคุณภาพอย่างต่อเนื่อง และมีวิสัยทัศน์ว่าจะ เป็นบริษั ทที่มั่นคง ริเริ่มในสิ่งใหม่ และกระทำทุกวิถีทางเพื่อให้เป็นบริษัทชั้นนำในการให้บริการครบวงจรทางด้านเทคโนโลยีสารสนเทศ อย่างดีที่สุดแก่ลูกค้า โดยบริษัทมุ่งมั่นที่จะให้บริการด้วยบุคลากรที่มีคุณภาพและมีกระบวนการทำงานที่เป็นมาตรฐานสากล

3. กรณีศึกษาส่วนของผู้ให้ บริการรับช่วงต่อ ที่ให้บริการเครือข่ายเพื่อเชื่อมต่อระหว่างผู้ว่าจ้างและผู้ให้บริการจัดจ้าง เป็นบริษัทที่ให้บริการการ สื่อสารครบวงจร บริษัท หนึ่งของประเทศไทย และใน ระหว่างปี พ.ศ. 2548 – 2550 กลุ่มบริษัทได้รับอนุญาตจากคณะกรรมการกิจการโทรคมนาคมแห่งชาติ สำหรับการ ให้บริการอินเทอร์เน็ต รวมทั้งบริการอินเทอร์เน็ตผ่านโทรศัพท์ (VoIP) บริการโทรศัพท์สาธารณะ บริการโทรศัพท์พื้นฐาน บริการโทรศัพท์ทางไกลระหว่างประเทศ และบริการโครงข่ายอินเทอร์เน็ตระหว่างประเทศ นอกจากนี้ยังได้รับใบอนุญาตสำหรับทดสอบให้บริการเชื่อมโยงโครงข่ายอินเต อร์เน็ตระหว่างประเทศผ่านเทคโนโลยี Leased Line (International Private Leased Circuit – IPLC) และบริการเชื่อมโยงอินเทอร์เน็ตระหว่างประเทศผ่านเทคโนโลยี MPLS (International Internet Protocol Virtual Private Network – IP VPN) เป็นเวลา 1 ปี

บทที่ 3

ขั้นตอนการดำเนินงานวิจัย

การศึกษาเกี่ยวกับโครงสร้างการ จัดการความมั่นคงปลอดภัยเพื่อเป็นแนวทางการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้างโดยใช้กรอบแนวคิดของ โครงสร้างความมั่นคงปลอดภัยธรรมมาภิบาล [8] กรณีศึกษาของบริษัท ที่ให้การสนับ สนุนระบบเทคโนโลยีสารสนเทศให้กับสถาบันการเงินแห่งหนึ่งในประเทศไทย ซึ่งในบทนี้เป็น การศึกษาถึงระเบียบวิธีการวิจัย โดยผู้วิจัยได้ค้นคว้าจากตำรา เอกสารและงานวิจัยที่เกี่ยวกับแนวทางความมั่นคงปลอดภัยของการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้างในทุกด้าน โดยการศึกษารูปแบบ การจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง และความมั่นคงปลอดภัยเมื่อมีการจัดจ้างภายนอก [1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 16, 17, 18] ดังนั้นผู้วิจัยจึงเลือกศึกษาการวิจัยเชิง คุณภาพ [15] (qualitative research) แล้วนำข้อมูลที่ได้นำมาเปรียบเทียบและนำมาสรุปวางแนวทางความมั่นคงปลอดภัยการจัดจ้างภายนอก อันจะช่วยสร้างประสิทธิภาพของผู้ให้บริการจัดจ้าง และสร้างความน่าเชื่อถือให้กับผู้ว่าจ้าง

3.1 แนวทางในการวิจัย

ในการวิจัยนี้ ผู้วิจัยได้นำเอา แนวคิดโครงสร้างความมั่นคงปลอดภัยธรรมมาภิบาล [8] เพื่อเป็นการกำหนดแนวทางโครงสร้างความมั่นคงป ลอดภัยการจัดจ้างภายนอกที่อยู่นอกที่ทำการ และนำเอารูปแบบการบริการจัดจ้างภายนอกที่มีอยู่ในปัจจุบันมาเป็นแนวทางใน รูปแบบการจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้างเพื่อสร้างความน่าเชื่อถือด้านความปลอดภัยให้กับผู้ว่าจ้าง โดยมุ่งประเด็นด้านความปลอดภัยที่ครอบคลุมเพื่อให้เกิดความน่าเชื่อถือ ดังนั้นผู้วิจัยเลือกศึกษาการวิจัยเชิงคุณภาพ โดยการศึกษาในสิ่งที่ไม่สามารถวัดได้ คือ เป้าหมายที่สามารถลดทอนเป็นตัวเลขได้ เช่นความรู้สึก ความคิด ประสบการณ์ เป็นต้น ซึ่งมโนทัศน์ทั้งหลายดังกล่าวเกี่ยวข้องกับการศึกษาความรู้แบบนัย นิยม เพื่อที่จะสามาร ถบรรยาย ให้เข้าใจมโนทัศน์เหล่านั้น เพราะฉะนั้น ผู้วิจัยจึงเลือกศึกษาแนวทางนี้

3.2 ระเบียบวิธีวิจัย

1. รวบรวมและ ศึกษา ข้อมูล ของ ความน่าเชื่อถือ การ จัดจ้างภายนอกเพื่อ ดูแล ระบบเทคโนโลยีสารสนเทศ ที่อยู่นอกที่ทำการของผู้ว่าจ้าง โดยอ้างอิงจากข้อมูลบริ ษัทให้บริการสนับสนุนสถาบันการเงินที่นำมาเป็นกรณีศึกษา

2. ศึกษาทฤษฎีพื้นฐานของโครงสร้างความมั่นคงปลอดภัยธรรมมาภิบาล
3. รวบรวมข้อมูลกรณีศึกษาของ การลดทรัพยากร และค่ าใช้จ่ายของ การจัดจ้างภายนอก และประเด็นที่เกี่ยวข้อง และวิเคราะห์เปรียบเทียบการจัดจ้างภายนอกที่อยู่นอกที่ ทำการของผู้ว่าจ้าง โดยอ้างอิงจากข้อมูลบริษัทให้บริการสนับสนุนสถาบันการเงินที่นำมาเป็นกรณีศึกษา
4. วิเคราะห์ประเด็นที่เกี่ยวข้องและสังเคราะห์รูปแบบการจัดจ้างภายนอกที่เหมาะสม
5. ประเมินรูปแบบการจัดจ้างภายนอกที่สังเคราะห์ขึ้นรวมถึงสรุปผล

3.3 ประชากรการประเมิน

ผู้วิจัยได้ประเมินผลของรูปแบบโดยอาศัยการวิจารณ์ จากบุคคลที่เกี่ยวข้องกับการดูแลรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศทั้งสองฝ่ายในการจัดจ้างภายนอก ของบริษัทให้บริการสนับสนุนสถาบันการเงินที่เป็นกรณีศึกษา โดยแบ่งเป็น 2 กลุ่มดังนี้

1. กลุ่มของผู้ว่าจ้างจะประกอบด้วย

— ผู้อำนวยการ ฝ่าย ดูแลโครงสร้างด้านความปลอดภัยของ สถาบันการเงินที่เป็นกรณีศึกษา เป็นผู้ที่กำ หนดรูปแบบความมั่นคงปลอดภัยภายในสถาบันการเงินของกรณีศึกษา และรูปแบบการดำเนินงานด้านสารสนเทศภายในสถาบันการเงินของกรณีศึกษา

— เจ้าหน้าที่ดูแลด้านความมั่นคงปลอดภั ยในการดำเนินงานของการจัดจ้างภายนอก และกำกับดูแล และเฝ้าติดตามเพื่อการรายงานผล

2. กลุ่มของผู้ให้บริการจัดจ้างภายนอก

— หัวหน้าฝ่ายดูแลความมั่นคงปลอดภัยที่เกี่ยวข้องกับการให้บริการจัดจ้างภายนอก และเป็นผู้กำหนดแนวทางด้านความมั่นคงความปลอดภัย ภายใน บริษัทให้การสนั บสนุนระบบเทคโนโลยีสารสนเทศให้กับสถาบันการเงินของกรณีศึกษา

— เจ้าหน้าที่ดูแลด้านความมั่นคงปลอดภัยในการดำเนินงานของ บริษัทให้การสนับสนุนระบบเทคโนโลยีสารสนเทศให้กับสถาบันการเงินของกรณีศึกษา

3.4 การวิเคราะห์ข้อมูล

ในการวิเคราห์ข้อมูลผู้วิจัยได้ดำเนินการวิเคราะ ห์ดังนี้ ใช้เทคนิคการวิเคราะห์เนื้อหา โดยมีการจัดกลุ่มตามประเด็นต่าง ๆ แล้ววิเคราะห์และสังเคราะห์รูปแบบการจัดจ้างภายนอก โดยใช้วัตถุประสงค์ และแนวคิดในการวิจัยเป็นกรอบในการวิเคราะห์แนวทางรูปแบบการจัดจ้างภายนอก

โดยอยู่นอกที่ทำการของผู้ว่าจ้างตามกรอบ ของโครงสร้างความมั่นคงปลอดภัยธรรมมาภิบาล ที่มุ่งเน้นการบริหารจัดการระดับบนคือ กลุ่มระดับบริหาร

บทที่ 4

การสังเคราะห์รูปแบบการจัดจ้างภายนอก

4.1 นิยาม

1. ผู้ว่าจ้าง คือผู้ซึ่งตกลงว่าจ้าง การจัดจ้างภายนอกเพื่อ ให้ดำเนินงาน การบริการโปรแกรมประยุกต์ และรวมถึงการดูแลบำรุงรักษา ทั้งหมดหรือแต่บางส่วน เพื่อประโยชน์แก่ ผู้ว่าจ้าง รวมถึงเป็นผู้กำหนดการรักษาความมั่นคงความปลอดภัย มีหน้าที่ในการประเมินความเสี่ยงภายในองค์กรที่เกี่ยวข้องเมื่อมีการจัดจ้างภายนอกอยู่นอกที่ทำการ และเป็นคนให้ความต้องการเกี่ยวกับความมั่นคงปลอดภัย รวมถึงการเฝ้าติดตามระบบความปลอดภัยของในส่วนที่ผู้ให้บริการจัดจ้างดูแลรักษาอยู่

2. ผู้ให้บริการจัดจ้าง ภายนอก คือผู้ที่ให้บริการจัดจ้าง ภายนอกให้ บริการโปรแกรมประยุกต์ และรวมถึงการดูแลรักษาทั้งหมด เพื่อให้ประโยชน์แก่ผู้ว่าจ้าง เป็นผู้ร่วมทำข้อตก ลงเกี่ยวกับระบบความมั่นคงปลอดภัยกับผู้ว่าจ้าง และเป็นผู้กำหนดการรักษาความมั่นคงปลอดภัยกับผู้รับช่วงต่อในการให้บริการจัดจ้างภายนอก มีหน้าที่ในการรายงานความปลอดภัยให้กับผู้ว่าจ้างตลอดช่วงเวลาในสัญญา และรับประกันด้านความมั่นคงความปลอดภัยให้กับผู้ว่าจ้าง รวมถึ งมีหน้าที่ในการประเมินความเสี่ยงที่เกี่ยวข้องผู้ว่าจ้างเมื่อมีการจัดจ้างภายนอกอยู่นอกที่ทำการ และเป็นคนให้ความต้องการเกี่ยวกับความมั่นคงปลอดภัยของผู้ว่าจ้างแก่ผู้รับช่วงต่อผู้ให้บริการจัดจ้างภายนอก รวมถึงการเฝ้าติดตามระบบความปลอดภัยของในส่วนที่ผู้รับช่วงต่ อให้บริการจัดจ้างดูแลรักษาอยู่

3. ผู้รับช่วงต่อผู้ให้บริการจัดจ้างภายนอก ควรจะหมายรวมไปถึง ผู้ที่รับสัญญาต่อจาก ผู้ให้บริการจัดจ้างภายนอก ทั้งทางตรงและทางอ้อม รวมทั้งผู้ผลิตฮาร์แวร์ซอฟ์แวร์บริการ และการบำรุงรักษา ผู้ให้บริการด้านการสื่อสาร ผู้ให้บริการด้าน พลังงาน น้ำมัน น้ำ และสิ่งใช้สอยต่างๆ ผู้ให้บริการด้านการขนส่ง เหล่านี้ต่าง มีหน้าที่ในการรายงานความปลอดภัยให้กับผู้ว่าจ้างตลอดช่วงเวลาในสัญญา และรับประกันด้านความมั่นคงความปลอดภัยให้กับผู้ว่าจ้าง

4.2 สังเคราะห์ แนวทางของ รูปแบบความมั่นคงปลอดภัยสำหรับจัดจ้าง การบริการภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง

การจัดจ้างภายนอก ที่สามารถสร้างความน่าเชื่อและความมั่นคงให้กับผู้ว่าจ้าง ผู้ให้บริการจัดจ้างภายนอกต้องมีความสามารถในการจัดระบบรักษาความมั่นคงปลอดภัย ให้กับผู้ว่าจ้าง และผู้ให้บริการจัดจ้างภายนอก เพื่อให้ความเชื่อมั่นในการจัดการระบบรักษาความมั่นคงปลอดภัย และ

ลดความเสี่ยง การจัดการระบบรักษา ความมั่นคงปลอดภัย ให้มีความต่อเนื่องตลอดการทำจัดจ้างภายนอก ถือเป็นสิ่งสำคัญในการจัดการความเสี่ยง แ ละการปฏิบัติตามสัญญา ซึ่งรวมไปถึงการจัดการเกี่ยวกับระบบรักษาความมั่นคงปลอดภัย จากการสังเคราะห์แนวทางโครงสร้างระบบความมั่นคงปลอดภัยการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้างนั้น มีองค์ประกอบที่สำคัญดังนี้

1. แนวทางความมั่นคงปลอดภัยการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง
2. โครงสร้างการจัดจ้างภายนอกที่อยู่นอกที่ทำการผู้ว่าจ้าง
3. การทำข้อตกลงร่วมกันของคู่สัญญาระหว่างผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก
4. Balance ScoreCard ด้านความปลอดภัยของผู้ให้บริการจัดจ้างภายนอก
5. การบริหารจัดการระบบสารสนเทศตามพระราชบัญญัติคอมพิวเตอร์ 2550

4.2.1 แนวทางความมั่นคงปลอดภัย การจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง

การรักษาความมั่นคงปลอดภัย เป็นสิ่งที่ผู้ให้บริการจัดจ้างภายนอก พึงปฏิบัติไปพร้อมกับการสร้างผลประโยชน์ทางการค้าให้กับองค์กรของผู้ให้บริการจัดจ้างภายนอกเอง ซึ่งมีขั้นตอนการดำเนินงานแสดงดังรูปที่ 4.1

รูปที่ 4.1 ความสัมพันธ์ระหว่างการดำเนินการจัดการระบบรักษาความมั่นคงปลอดภัย

การแบ่งปันข้อมูลและหลักการขั้นพื้นฐานที่จำเป็นต่อองค์กรต้องมีประสิทธิภาพเพียงพอที่จะจัดการด้านความเสี่ยงที่จะเกิดขึ้นกับระบบและข้อมูลที่มีความอ่อนไหว ผู้ว่าจ้างต้องแน่ใจว่ามีการทำสัญญา ควบคุมและครอบคลุมในทุกส่วน และสามารถประเมินความเสี่ยง ได้ ซึ่งองค์ประกอบในการจัดการรักษา ความมั่นคงปลอดภัย เมื่อมีการให้บริการจัดจ้างภายนอก ดังรูปที่ 4.2

รูปที่ 4.2 องค์ประกอบในการจัดการระบบความมั่นคงปลอดภัยเมื่อมีการให้บริการจัดจ้างภายนอก

1. หน้าที่และความรับผิดชอบ

การทำจัดจ้างภายนอก จะต้องมีผู้ที่ทำหน้าที่ในความรับผิดชอบหลักที่เป็นที่ยอมรับ โดยเริ่มจากที่องค์ของกรผู้ว่าจ้าง ตามด้วยในส่วนองค์กรของผู้ให้บริการจัดจ้างภายนอก ซึ่งในการทำสัญญาว่าจ้างนั้นต้องมีการยอมรับในส่วนของ ความมั่นคงปลอดภั ย และผู้ที่รับผิดชอบ ทั้งในองค์กรของผู้ว่าจ้างและในองค์กรผู้ให้บริการจัดจ้างภายนอก ซึ่งแสดงดังตารางที่ 4.2 และตารางที่ 4.3

ตารางที่ 4.1 ตำแหน่งหน้าที่หลักในส่วนของผู้ว่าจ้าง

ตำแหน่ง	หน้าที่/ความรับผิดชอบ
ผู้จัดการทั่วไป (general manager)	ผู้จัดการทั่วไ ป (general manager) ต้องชี้แจง และมีหน้าที่รับผิดชอบในการให้การสนับสนุนการจัดจ้างภายนอกรวมถึงสามารถชี้แจงและให้ความเชื่อมั่นว่า — เรื่องความเสี่ยงของระบบรักษา ความมั่นคงปลอดภัย และข้อตกลงต่างๆ ทุกฝ่ายเข้าใจตรงกัน — ระดับความเสี่ยงในการรักษาความมั่นคงปลอดภัยอยู่ในระดับ — ข้อเรียกร้องด้านระบบรักษา ความมั่นคงปลอดภัย มีให้เห็นเด่นชัด — มีการปฏิบัติตามโครงร่างของระบบรักษา ความมั่นคงปลอดภัยที่เหมาะสม — มีการจัดระบบดูแลความเสี่ยงในการรักษา ความมั่นคงปลอดภัยตลอดช่วงการดำเนินการ จัดจ้างภายนอก ให้ความเชื่อมั่นว่าความเสี่ยงต่ อระบบรักษา ความมั่นคงปลอดภัย นั้นได้รับการควบคุมดูแลอย่างทั่วถึงและพร้อมที่จะปฏิบัติทุกเมื่อ
ผู้จัดการด้านการรักษาความมั่นคงปลอดภัยในการจัดจ้างภายนอก (security manager)	ผู้จัดการด้าน ความมั่นคงปลอดภัย ต้องเป็นผู้ที่น่าเชื่อถือและต้องให้ความมั่นใจแก่ ผู้ให้ผู้จัดการ ทั่วไปในระหว่างขั้นตอนการดำเนินการจัดจ้างภายนอกดังนี้ — มีความเข้าใจตรงกันในเรื่องความเสี่ยงของระบบรักษา ความมั่นคงปลอดภัยและข้อตกลง — ระดับความเสี่ยงในเรื่องการรักษาความมั่นคงปลอดภัย อยู่ในระดับที่น่าพอใจต่อองค์กร — ข้อเรียกร้องด้านการรักษาความมั่นคงปลอดภัยมีให้เห็นเด่นชัด — มีการจัดระบบดูแลควบคุมความเสี่ยงในการรักษา ความมั่นคงปลอดภัยตลอดช่วงการดำเนินการจัดจ้างภายนอก

ตารางที่ 4.1 (ต่อ) ตำแหน่งหน้าที่หลักในส่วนของผู้ว่าจ้าง

ตำแหน่ง	หน้าที่/ความรับผิดชอบ
	— ให้ความเชื่อมั่นว่าความเสี่ยงต่อการรักษาระบบ ความมั่นคงปลอดภัย นั้นได้รับการควบคุมดูแลอย่างทั่วถึง พร้อมที่จะปฏิบัติ มีการรายงานสถานการณ์ สอบสวนและแก้ไขข้อผิดพลาด ผู้จัดการด้านการรักษาความมั่นคงปลอดภัยในกา รจัดจ้างภายนอก ควรเป็นผู้ที่เชี่ยวชาญและมีประสบการณ์ในการจัดระบบรักษาความมั่นคงปลอดภัยเป็นอย่างดี
บุคคลที่ 3 หรือที่ปรึกษา	บุคคลที่ 3 ที่ผ่านการพิจารณาจาก ผู้ว่าจ้าง และมีหน้าที่ในการให้ความเชื่อมั่นดังต่อไปนี้ — เครื่องมือและอุปกรณ์ ที่ช่วยในการควบคุมดูแลระบบรักษาความมั่นคงปลอดภัย ของผู้ให้บริการจัดจ้างภายนอก ทำงานอย่างสอดคล้องกับข้อเรียกร้องที่ได้ทำไว้ในสัญญา — ให้ความเชื่อมั่นว่าความเสี่ยงที่มีต่อการรักษา ความมั่นคงปลอดภัย นั้นได้รับการดูแลอย่างทั่วถึง พร้อมที่จะปฏิบัติและมีการรายงานสถานการณ์สอบสวนและแก้ไขข้อผิดพลาด

ตารางที่ 4.2 ตำแหน่งหน้าที่หลักในส่วนของผู้ให้บริการจัดจ้างภายนอก

ตำแหน่ง	หน้าที่/ความรับผิดชอบ
ผู้อำนวยการ (senior commercial director)	ผู้อำนวยการมีหน้าที่ในการประมูลสั ญญาว่าจ้างและติดตามผลงานในการจัดจ้างภายนอก และต้องแน่ใจว่า — ความเสี่ยงของระบบรักษา ความมั่นคงปลอดภัย และข้อตกลงต่างๆ ทุกฝ่ายมีความเข้าใจตรงกัน — ระดับความเสี่ยงในการรักษาความมั่นคงปลอดภัยอยู่ในระดับที่น่าพอใจต่อองค์กร — มีการจัดระบบดูแลความเสี่ยงในการรักษา ความมั่นคงปลอดภัยตลอดช่วงการดำเนินการจัดจ้างภายนอก

ตารางที่ 4.2 (ต่อ) ตำแหน่งหน้าที่หลักในส่วนของผู้ให้บริการจัดจ้างภายนอก

ตำแหน่ง	หน้าที่/ความรับผิดชอบ
	— ให้ความเชื่อมั่นว่า ความเสี่ยงที่มีต่อการรักษาความมั่งคงปลอดภัย นั้นได้รับการดูแลอย่างทั่วถึง พร้อมที่จะปฏิบัติและมีการรายงานสถานการณ์สอบสวนและแก้ไขข้อผิดพลาด — สิ่งที่นำเสนอให้กับผู้ว่าจ้างครบถ้วนและถูกต้อง
ผู้จัดการด้านความมั่นคงปลอดภัย (security manager)	ผู้จัดการด้าน ความมั่นคงปลอดภัย (security manager) จะต้องสามารถชี้แจงให้ ผู้อำนวยการมีความเชื่อมั่นว่า — เรื่องความเสี่ยงของระบบรักษา ความมั่นคงปลอดภัย และข้อตกลงต่าง ๆ ทุกฝ่ายเข้าใจตรงกัน — ระดับความเสี่ยงในการรักษาความมั่นคงปลอดภัย อยู่ในระดับที่น่าพอใจต่อองค์กร — มีการจัดระบบดูแลค วามเสี่ยงในการรักษา ความมั่นคงปลอดภัยตลอดช่วงการดำเนินการ จัดจ้างภายนอก — ให้ความเชื่อมั่นว่าความเสี่ยงที่มีต่อการรักษา ความมั่นคงปลอดภัย นั้นได้รับการดูแลอย่า งทั่วถึง พร้อมที่จะปฏิบัติและมีการรายงานสถานการณ์สอบสวนและแก้ไขข้อผิดพลาด การทำจัดจ้างภายนอกผู้ให้บริการจัดจ้างภายนอกผู้จัดการด้านความมั่นคงปลอดภัย ควรเป็นผู้ ที่มีความเชี่ยวชาญและมีประสบการณ์ในการจัดการระบบรักษาความมั่นคงปลอดภัยเป็นอย่างดี
หน้าที่รับผิดชอบอื่นๆ	หน้าที่รับผิดชอบอื่น ๆ ที่เกี่ยวข้องกับระบบรั กษาความปลอด ภัยจะถูกให้คำ นิยามโดยดูจากคุณสมบัติของกิ จกรรมที่ทำการจัดจ้างภายนอก

2. การประเมินความเสี่ยง

— ผู้ว่าจ้างทำการประเมินความเสี่ยงก่อนที่ตัดสินใจเริ่มต้นกระบวนการจัดจ้างภายนอก การประเมินความเสี่ยงนั้นเป็นสิ่งที่จำเป็นอย่างยิ่งที่จะให้ความเชื่อมั่นว่าองค์กรเข้าใจในความต้องการเกี่ยวกับระบบรักษา ความมั่ นคงปลอดภัย และให้ความเชื่อมั่นว่า ผู้ให้บริการจัดจ้างภายนอกเข้าใจถึงความเสี่ยงที่อาจเกิดขึ้นและทำข้อตกลงที่จะจัดการควบคุมดูแล

— ผู้ว่าจ้างประเมินความเสี่ยงควรพิจารณาให้อยู่ภายใต้กฎและข้อตกลงมาตรฐานขององค์กร อาจทำได้โดยการทำรายการที่แสดงถึงข้อบังคับ และมาตรฐานที่เหมาะสม และพิจารณาผลกระทบต่างๆ ที่จะเกิดขึ้นนั้นเพื่อควบคุมและจัดการความเสี่ยงที่เกิดขึ้น ซึ่งมีหลักการประเมินความเสี่ยงให้เกิดประโยชน์ได้ดังนี้

- การประเมินความเสี่ยงจะทำได้ง่ายขึ้นโดยอาศัยผู้เชี่ยวชาญและผู้มีประสบการณ์ในการรักษาความมั่นคงปลอดภัยของข้อมูล จากภาคธุรกิจ
- สำหรับแต่ละขั้นตอนการดำเนินธุรกิจ และระบบมีการ ชี้ให้การดำเนินธุรกิจและหน้าที่ที่อยู่ภายใต้ระบบข้อมูลข่าวสาร ของการจัดจ้างภายนอกขึ้นอยู่กับขอบเขตในการที่จะทำจัดจ้างภายนอก
- สำหรับแต่ละขั้นตอนของการดำเนินธุรกิจและระบบ คำนึงถึงการประเมินผลกระ ทบทางธุรกิจ เพื่อจะได้เข้าใจถึงผลกระทบด้านการสูญเสียความลับ ความมั่นคงหรือความเพียงพอในการนำไปใช้ของระบบ โดยใช้ระบบการวัดผลกระทบ ต่อความมั่นคง
- การประเมินความเสี่ยงต้อง เข้าถึงการคุกคามด้าน ความมั่นคงปลอดภัย ของธุรกิจและระบบต่างๆ ในเรื่องของบุคค ล และองค์กรที่กระทำการก่อให้เกิดความเสียหายหรือแรงจูงใจ และความสามารถในการที่จะให้เกิดความเสียหาย องค์กร CNI มีข้อมูลการคุกคามนี้น่าเชื่อถือได้จาก NISCC [3] โดยสมมุติฐานที่ว่า การคุกคามของข้อมูลข่าวสารมักจะมีอิทธิพลมากที่สุดในการทำการประเมินความเสี่ยง และผลที่จะตามมาในก ารรักษา ความมั่นคงปลอดภัย และการตัดสินใจในการ จัดจ้างภายนอกเป็นเรื่องที่ ไวต่อสิ่งที่มากระตุ้นเป็นที่สุด
- พิจารณาถึงความไม่มั่นคงที่เกิดขึ้นในปัจจุบันและสถานะ ข้อตกลงของแต่ละระบบนิยามระดับความเสี่ยงที่แสดงซึ่งอาจจะสามารถยอมรับได้ควบคู่ไปกับความเสี่ยงขององค์กร
- ชี้ให้เห็นถึงช่องว่างระหว่างระดับความเสี่ยงปัจจุบันที่ค้างอ ยู่ และระดับความยินยอม และระดับ เป้าหมายของ ความเสี่ยงที่คงอยู่เมื่อมีการ จัดจ้างภายนอก โดยสมมุติฐานว่าถ้าการปรับปรุงด้านการรักษา ความมั่นคงปลอดภัย มีความจำเป็นในการกำจัดช่องว่าง เพราะฉะนั้นจะมีค่าใช้ จ่ายในการเปลี่ยนแปลงและดำเนินการรักษาความมั่นคงปลอดภัย

— กระบวนการการประเมินความเสี่ยงนั้น ควรคาดว่าอาจมีความไม่มั่นคงและเกิดการคุกคามในด้านต่างๆ จากการทำ จัดจ้างภายนอก ได้

— ผู้จัดการด้านการรักษาความมั่นคงปลอดภัยในการ จัดจ้างภายนอก มีการจัดทำผลการประเมินความ เสี่ยงเป็นลายลักษณ์อักษร เพื่อให้ ผู้ให้การสนับสนุนการทำจัดจ้างภายนอกได้ตรวจสอบและพิจารณา

— เมื่อมีการเตรียมข้อมูลให้กับผู้ให้บริการจัดจ้างภายนอกในช่วงกระบวนการการจัดหาจัดจ้างภายนอก และระหว่างการดำเนินการตามสัญญา ผู้จัดการฝ่ายการจั ดหาต้องแน่ใจว่าได้ชี้แจงให้กับผู้ให้บริการจัดจ้างภายนอกได้เข้าใจว่าการประเมินความเสี่ยง ข้อบังคับ ข้อกำหนดต่าง ๆ เป็นส่วนประกอบสำคัญในสัญญาที่ ผู้ให้บริการจัดจ้างภายนอกพึงปฏิบั ติ อย่างไรก็ตามควรมีการระบุว่าเรื่องเกี่ยวกับความเสี่ยงของระบบรักษา ความมั่นคงปลอดภัย นี้เป็นเรื่องระเอียดอ่อน ต่อองค์กรของ ผู้ว่าจ้าง เพราะฉะนั้นจะต้องหาระดับที่เหมาะสมในก ารแบ่งปันข้อมูลเหล่านี้กับ ผู้ให้บริการจัดจ้างภายนอก

— มีการยืนยันว่าผู้ให้บริการจัดจ้างภายนอกมีความเข้าใจในเรื่องของการประเมินความเสี่ยง และความต้องการที่มีการตกลงกันระหว่างผู้ว่าจ้าง และผู้ให้บริการจัดจ้างภายนอก

3. การให้ความเชื่อมั่น (การประกันภัย) ว่าการดำเนินการให้เป็นไปตามข้อตกลง

— เพื่อให้แน่ใจว่ามีการจัดการระบบควบคุมความเสี่ยงอย่างต่อเนื่องในระหว่างช่วงการดำเนินงานของผู้ให้บริการจัดจ้าง ผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก ควรมีการวางแผนการจัดการระบบรักษาความมั่นคงปลอดภัยร่วมกัน ส่วนแรกเลยคือส่วนที่ดำเนินการเปลี่ยนแปลงถ่ายการรักษา ความมั่นคงปลอดภัย ควบคู่ไปกับการให้บริการ ที่เปลี่ยน แปลง คือ ผู้ให้บริการจัดจ้างภายนอกมีหน้าที่รับผิดชอบในการปฏิบัติเปลี่ยนถ่าย ระบบการจัดการ ความมั่นคงปลอดภัย ไปสู่ผู้ให้บริการจัดจ้างซึ่งสอดคล้องกับการประเมินความเสี่ยง

— การพัฒนาร่วมกันในสิ่งแรกของแผน ควรเป็นข้อตกลงตามพันธะสัญญาของ ผู้ให้บริการจัดจ้างภายนอก (ควบคู่ไปกับแผน) การบริการเปลี่ยนถ่าย ในการที่จะทำให้การเปลี่ยนถ่ายระบบการจัดการความมั่นคงปลอดภัย เข้าสู่ขั้นตอนสุดท้ ายอย่างสมบูรณ์แบบ ผู้ให้บริการจัดจ้างภายนอกควรกำหนดวันที่ แน่นอนในแผน และวันที่จัดการให้เป็นจริงอย่างสมบูรณ์แบบ อย่างชัดเจน และสุดท้ายควรมีการตรวจทานรูปแบบ การประกันภัยหลังจากการ จัดการให้เป็นจริงโดยผู้ว่าจ้าง ซึ่งสามารถใช้ควบคู่กับการจัดการด้านระบบรักษาความมั่นคงปลอดภัย

— ขบวนการที่ควรระบุไว้ในสัญญาสำหรับการจัดการระบบรักษา ความมั่นคงปลอดภัย ของ ผู้ให้บริการจัดจ้างภายนอก มีดังนี้

- การเปลี่ยนแปลงในเรื่องของความเสี่ยง รวมถึงกระบวนการทางธุรกิจ และผลกระทบทางธุรกิจ การคุมคามและความไม่มั่นคง
- การเปลี่ยนแปลงของข้อบังคับ หรือข้อตกลงร่วมกัน
- การเปลี่ยนแปลงของข้อเรียกร้องด้าน ความมั่นคงปลอดภัย รวมถึงรายละเอียดด้านการควบคุม
- ผลที่ได้รับ และการแก้ไขเปลี่ยนแปลงจากการรักษา ความมั่นคงปลอดภัย และการรายงานความเชื่อมั่น
- การเปลี่ยนแปลงขอบเขตปัจจัยสำคัญที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย

— ขั้นตอนการดำเนินการ ควรเห็น ชอบตรงกันระหว่างผู้ว่าจ้างแล ะผู้ให้บริการจัดจ้างภายนอก ในการที่จะใช้ระบบใหม่ หรือการเปลี่ยนแปลงที่เป็นปัจจัยสำคัญ ที่จะกระทบระบบรักษาความมั่นคงปลอดภัย

— ขั้นตอนการดำเนินการควรให้ความกระจ่างถึงข้อเรียกร้องในระดับการรักษา ความมั่นคงปลอดภัยแบบวันต่อวันของผู้ว่าจ้าง (เช่น การเพิ่มเติมหรือเปลี่ยนแปลงของผู้ว่าจ้างว่าได้ รับการอนุญาตและถูกดำเนินการโดยผู้ให้บริการจัดจ้างภายนอก)

4. การจัดการระบบรักษาความมั่นคงปลอดภัยระหว่างการดำเนินการจัดจ้างภายนอก

— เมื่อมีการประเมินความเสี่ยงแล้วก็เป็นไป ได้ที่จะแสดงให้เห็นอย่างเด่นชัดถึงข้อเรียกร้องเกี่ยวกับระบบรักษา ความมั่นคงปลอดภัย เพื่อจะนำไปสื่อสารต่อ ผู้ให้บริการจัดจ้างภายนอก ผู้ที่จะเข้ามาจัดจ้างภายนอก

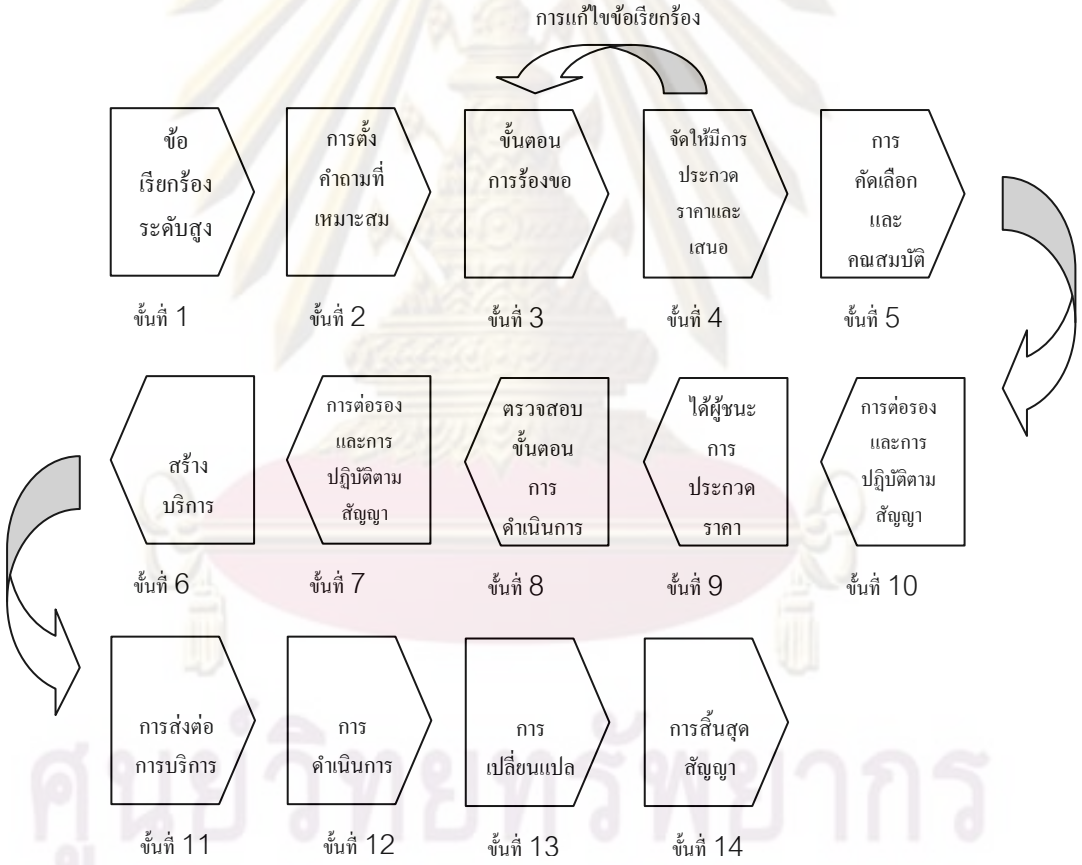
— มีหลายวิธีที่สื่อสาร ของข้อเรียกร้องต่าง ๆ และเพื่อให้การสื่อสารเกี่ยวกับระบบรักษาความมั่นคงปลอดภัย เป็นไปอย่างมีประสิทธิภาพ ทั้ง 2 ฝ่ายต้องมีการประสานงานกันเพื่อเข้าถึงระบบควบคุมดูแล ความมั่นคงปลอดภัย และเพิ่มความเชื่อมั่นว่า ผู้ให้บริการจัดจ้างภายนอกได้ปฏิบัติตามข้อเรียกร้อง

— เมื่อผู้ให้บริการจัดจ้างภายนอก ได้รับทราบรายละเอียดเพิ่มเติ มเกี่ยวกับระบบและความต้องการของ ผู้ว่าจ้าง วิธีการในการดำเนินการจัดระบบรักษา ความมั่นคงปลอดภัย ก็ถือเป็นตัวเชื่อมโยงการสื่อสารระหว่าง ผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก และความต้องการเฉพาะด้านที่เกี่ยวกับระบบรักษาความมั่นคงปลอดภัย

– ผู้ว่าจ้างและ ผู้ให้บริการจัดจ้างภายนอก มีความเ ห็นร่วมกันที่จะใช้มาตรฐาน ISO/IEC 27001 ในการจัดการความมั่นคงปลอดภัย ในการประเมินความเสี่ยง และปฏิบัติตามข้อเรียกร้องและการควบคุมให้เป็นไปตามวัตถุประสงค์ ของ ISO/IEC 27001 ตั้งแต่แรกเริ่มและต่อเนื่องตลอดช่วงอายุสัญญา

5. ระบบรักษาความมั่นคงปลอดภัยในช่วงอายุสัญญา

ภาพรวมของการเข้าถึงระบบรักษา ความมั่นคงปลอดภัย ในช่วงอายุสัญญา ตามรูปที่ 4.3 และรายละเอียดตามตารางที่ 4.4



รูปที่ 4.3 ขั้นตอนการจัดการระบบรักษาความมั่นคงปลอดภัยตลอดช่วงอายุสัญญา

ตารางที่ 4.3 รายละเอียดเกี่ยวกับขั้นตอนการจัดการระบบรักษาความมั่นคงปลอดภัย ในตลอดช่วงอายุสัญญา

ลำดับขั้นที่	กิจกรรม	กิจกรรมแบบชี้เฉพาะ
1. ข้อเรียกร้องระดับสูง	ผู้ว่าจ้างระบุถึงข้อเรียกร้องระดับสูงในการบริการภายใต้สัญญาการจัดจ้างภายนอก	- ผู้ให้บริการจัดจ้างที่มีคุณสมบัติครบ มีประสบการณ์ และเป็นผู้เชี่ยวชาญด้านระบบรักษาความมั่นคงปลอดภัย - จัดการประเมินความเสี่ยง - กำหนดขั้นตอนการเรียกร้องของการออกแบบคำร้อง และนโยบาย
2. การตั้งคำถามที่เหมาะสมเบื้องต้น	- ผู้ว่าจ้างเสนอข้อเรียกร้องระดับสูงกับผู้ให้บริการ จัดจ้างภายนอกและตั้งคำถามที่เหมาะสม และขอคำตอบ - ผู้ให้บริการจัดจ้างภายนอก ตอบคำถาม	- ผู้ว่าจ้าง ออกแบบประเมิน ความเสี่ยง และความต้องการด้าน ความมั่นคงปลอดภัย ให้แก่ผู้ให้บริการ จัดจ้างภายนอก รวมถึงขอคำตอบและข้อแนะนำวิธีการจัดการ ระบบความมั่นคงปลอดภัย เช่นเดียวกับการหาความสามารถของการจัดการระบบความมั่นคงปลอดภัย - ผู้ว่าจ้าง มีข้อผูกมัดกับ ผู้ให้บริการจัดจ้างภายนอก ว่าจะรักษาข้อมูลทั้งที่ได้รับและที่ส่งต่อ
3. หลักฐานแสดงข้อเรียกร้อง	- ผู้ว่าจ้าง จัดการเรื่องรายละเอียดขั้นตอนของข้อเรียกร้องความต้องการ	- ผู้ว่าจ้างเลือกวิธีที่จะจัดการรักษาความมั่นคงปลอดภัย สร้างและออกแบบการควบคุมตามวัตถุประสงค์ระดับสูง ซึ่งมีความเกี่ยวเนื่องกับระบบให้อยู่ในขั้นตอนของข้อเรียกร้อง - ผู้ว่าจ้างสั่งให้มีการบังคับใช้ระบบ

ตารางที่ 4.3 (ต่อ) รายละเอียดเกี่ยวกับขั้นตอนการจัดการระบบรักษา ความมั่นคงปลอดภัย ในตลอดช่วงอายุสัญญา

ลำดับขั้นที่	กิจกรรม	กิจกรรมแบบชี้เฉพาะ
		ความมั่นคงปลอดภัยกับผู้ที่มีหน้าที่รับผิดชอบภายในองค์กรของตน
4. จัดให้มีการนำเสนอโครงการ	- ผู้ว่าจ้างจัดการเรื่องรายละเอียดของขั้นตอนของข้อเรียกร้อง และออกแบบเงื่อนไขโดยรวมให้แก่ผู้ให้บริการจัดจ้างภายนอก และจัดให้มีการประกวดราคา - ผู้ว่าจ้างจัดให้มีการประกวดราคาโดยมุ่งให้ความสำคัญไปที่ระบบรักษาความมั่นคงปลอดภัยและอ้างถึงการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย รายละเอียด การควบคุมการเข้าถึง การจัดการระบบรักษาความมั่นคงปลอดภัยและความเชื่อมั่น (การประกันภัย)	- ผู้ว่าจ้างออกแบบขั้นตอนด้านการรักษาความมั่นคงปลอดภัย การประเมินความเสี่ยง ขั้นตอนความต้องการเพื่อให้ปฏิบัติตาม (compliance requirement) รวมถึงสำเนาเอกสารอ้างอิงทั้งหมด และวัตถุประสงค์การควบคุมชั้นสูงแก่ผู้ให้บริการจัดจ้างภายนอก - ผู้ว่าจ้างชี้เฉพาะถึงการจัดการรักษาความปลอดภัยและความเชื่อมั่นให้มีการนำมาใช้ โดยใช้ร่วมกับโครงร่างรายละเอียดด้านการควบคุมถ้าเป็นไปได้ - ผู้ว่าจ้างเปลี่ยนเกณฑ์ของการรักษาความมั่นคงปลอดภัยให้เป็นรายละเอียดหรือเงื่อนไขในสัญญา
5. การคัดเลือกและคุณสมบัติ	- ผู้ว่าจ้างสร้างทีมประเมินผล การประกวดราคา และชี้ให้เห็นถึงวิธีการให้คะแนนในการประเมินผลจากผู้ให้บริการจัดจ้างภายนอก - พื้นที่หลักในการรักษาความมั่นคงปลอดภัยควรจะถูกเชื่อมโยงกับระดับความเสี่ยงในการรักษาความ	- ผู้ว่าจ้างชี้ให้เห็นถึงการคัดเลือกที่เกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัย - ผู้ที่มีคุณสมบัติ ประสบการณ์และความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยของ ผู้ว่าจ้างถือเป็นส่วนหนึ่งของคณะกรรมการ

ตารางที่ 4.3 (ต่อ) รายละเอียดเกี่ยวกับขั้นตอนการจัดการระบบรักษา ความมั่นคงปลอดภัย ในตลอดช่วงอายุสัญญา

ลำดับขั้นที่	กิจกรรม	กิจกรรมแบบชี้เฉพาะ
	มั่นคงปลอดภัยจากการประเมินความเสี่ยง	ประเมินผลระบบรักษาความมั่นคงปลอดภัย ของผู้ให้บริการจัดจ้างภายนอก
6. ข้อเสนอสุดท้ายและข้อเสนอที่ดีที่สุด	ผู้ว่าจ้างต่อรองข้อเสนอสุดท้ายจากผู้ประกวดราคา และขอบเขตของราคา	ผู้ที่มีคุณสมบัติ มีประสบการณ์ และเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยของ ผู้ว่าจ้างตรวจสอบข้อเสนอสุดท้ายของการประมูลให้เป็นไปอย่างเหมาะสมและเป็นไปในทิศทางเดียวกัน
7. ผู้ชนะการประกวดราคา	- คณะกรรมการประเมินผลการประกวดราคาของผู้ว่าจ้างระบุผู้ประเมินที่เหมาะสม - ผู้ว่าจ้างตรวจสอบความสามารถของผู้ให้บริการจัดจ้างภายนอก	- ผู้ที่มีคุณสมบัติ มีประสบการณ์และเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยของผู้ว่าจ้างตรวจสอบว่าผู้ประมูลที่เหมาะสม มีความสามารถในการจัดระบบรักษาความมั่นคงปลอดภัยตามที่ผู้ว่าจ้างต้องการหรือไม่ และแนวทางในการรักษาความมั่นคงปลอดภัยได้รวมอยู่ในค่าใช้จ่ายที่ได้ทำการเสนอเข้าประกวดราคา - ผู้ที่มีคุณสมบัติ มีประสบการณ์และเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยของผู้ว่าจ้างตรวจสอบความสามารถในการรักษาความมั่นคงปลอดภัยของผู้ให้บริการจัดจ้างภายนอก
8.ตรวจสอบการ	ฝ่ายดำเนินการของผู้ให้บริการจัด	ผู้ที่มีคุณสมบัติ มีประสบการณ์ และ

ตารางที่ 4.3 (ต่อ) รายละเอียดเกี่ยวกับขั้นตอนการจัดการระบบรักษา ความมั่นคงปลอดภัย ในตลอดช่วงอายุสัญญา

ลำดับขั้นที่	กิจกรรม	กิจกรรมแบบชี้เฉพาะ
ดำเนินงาน	จ้างภายนอกตรวจสอบการปฏิบัติการ และขอบเขตของการให้บริการจัดจ้างภายนอกเพื่อตรวจสอบความถูกต้องของการดำเนินงานให้อยู่ในขอบเขตของข้อกำหนดของการประกวดราคาและราคาขั้นสุดท้ายของสัญญา	เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยของ ผู้ว่าจ้างทำการตรวจทานการปฏิบัติแนวทางของระบบรักษาความมั่นคงปลอดภัยในส่วนที่มีการทำการจัดจ้างภายนอกเพื่อตรวจสอบความถูกต้องในข้อกำหนดของการประกวดราคา และสรุปผลของราคาขั้นสุดท้ายของสัญญา
9.การต่อรอง และการปฏิบัติตามสัญญา	- ผู้ดูแลด้านการค้า เทคนิค และผู้เชี่ยวชาญด้านการจัดหาของทั้งผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก ทำการต่อรองและจัดหาข้อสรุปของสัญญา - การเปลี่ยนแปลงสัญญา และขอบเขตการเปลี่ยนแปลงการดำเนินการได้รับความเห็นชอบจากทั้ง 2 ฝ่าย และนำไประบุไว้ในสัญญา	- ผู้ที่มีคุณสมบัติ มีประสบการณ์และเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยของผู้ว่าจ้างตรวจสอบสรุปทิศทางของระบบรักษาความมั่นคงปลอดภัยกับผู้เชี่ยวชาญด้านการดำเนินการ และธุรกิจเพื่อให้แน่ใจว่าสัญญาได้มีการรวมไว้ซึ่ง การประเมินความเสี่ยง และความต้องการให้ปฏิบัติตามข้อตกลงในการเข้าถึงการจัดการระบบรักษาความมั่นคงปลอดภัย การควบคุมเฉพาะด้านและความเชื่อมั่น (การประกันภัย) - การเปลี่ยนแปลงสัญญา และขอบเขตการเปลี่ยนแปลงการดำเนินการได้รับความเห็นชอบจากทั้ง 2 ฝ่าย และนำไประบุไว้ในสัญญา
10.การสร้างการ	ผู้ให้บริการจัดจ้างภายนอกจัดสร้าง	- ผู้เชี่ยวชาญด้านการรักษาความ

ตารางที่ 4.3 (ต่อ) รายละเอียดเกี่ยวกับขั้นตอนการจัดการระบบรักษา ความมั่นคงปลอดภัย ในตลอดช่วงอายุสัญญา

ลำดับขั้นที่	กิจกรรม	กิจกรรมแบบชี้เฉพาะ
บริการ	ระบบต่างๆ และโครงสร้างขั้นพื้นฐานที่จำเป็นในการจัดการบริหารระบบความมั่นคงปลอดภัย	มั่นคงปลอดภัยของผู้ให้บริการจัดจ้างภายนอกจัดการบริหารระบบรักษาความมั่นคงปลอดภัยให้เป็นไปตามสัญญา และให้แน่ใจว่าการปฏิบัติงานในทุกขั้นตอนได้เป็นไปตามข้อเรียกร้องในสัญญา - ผู้ให้บริการจัดจ้างภายนอกให้ความเชื่อมั่น (การประกันภัย) กับผู้ว่าจ้างตามที่ได้ตกลงกันในสัญญา
11.การส่งต่อการให้บริการ	ผู้ให้บริการจัดจ้างภายนอกทำการส่งต่อการให้บริการด้านการปฏิบัติงานจากระบบที่มีอยู่แล้วให้ก้าวไปสู่เทคโนโลยีด้านการอำนวยความสะดวก การดำเนินการและผู้ปฏิบัติการใหม่	- ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยของ ผู้ให้บริการจัดจ้างภายนอกจัดการบริหารระบบรักษาความมั่นคงปลอดภัยให้เป็นไปตามสัญญา และให้แน่ใจว่าการปฏิบัติงานในทุกขั้นตอนได้เป็นไปตามข้อเรียกร้องในสัญญาทั้งก่อน ระหว่าง และหลังจากการส่งมอบ - ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยของ ผู้ให้บริการจัดจ้างภายนอกและผู้ว่าจ้างวางแผนและปฏิบัติงานร่วมกันในส่วนของกิจกรรมการส่งต่อระบบรักษาความมั่นคงปลอดภัย - ผู้ให้บริการจัดจ้างภายนอกให้ความเชื่อมั่น (การประกันภัย) กับผู้ว่าจ้างตามที่ได้ตกลงกันในสัญญา

ตารางที่ 4.3 (ต่อ) รายละเอียดเกี่ยวกับขั้นตอนการจัดการระบบรักษา ความมั่นคงปลอดภัย ในตลอดช่วงอายุสัญญา

ลำดับขั้นที่	กิจกรรม	กิจกรรมแบบชี้เฉพาะ
		- ผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอกร่วมมือและทำการตกลงเรื่องการตรวจทานความเชื่อมั่นของระบบรักษาความมั่นคงปลอดภัยอย่างเป็นทางการร่วมกัน
12.การดำเนินการ	ผู้ให้บริการจัดจ้างภายนอกปฏิบัติการดำเนินการตามระบบที่สอดคล้องกับสัญญาข้อตกลงที่ได้ทำร่วมกัน และมีการเฝ้าดูการปฏิบัติงาน	- ผู้ให้บริการจัดจ้างภายนอกปฏิบัติตามระบบรักษาความมั่นคงปลอดภัยตามสัญญาและแนวทางของการรักษาความมั่นคงปลอดภัย - ผู้ให้บริการจัดจ้างภายนอกให้ความเชื่อมั่น (การประกันภัย) กับผู้ว่าจ้างตามที่ได้ตกลงกันในสัญญา
13.การเปลี่ยนแปลง	ผู้ให้บริการจัดจ้างภายนอกจัดการการเปลี่ยนแปลงให้สอดคล้องกับสัญญาที่ว่าด้วยการจัดการการเปลี่ยนแปลง	- ผู้ให้บริการจัดจ้างภายนอกทำการจัดการปลี่ยนแปลง ที่เกี่ยวเนื่องกับระบบรักษาความมั่นคงปลอดภัย (ไม่ว่าที่เกิดจากการให้บริการ หรือปัจจัยด้านการรักษาความมั่นคงปลอดภัย) ให้สอดคล้องกับข้อตกลงในสัญญาที่ว่าด้วยหน้าที่ความรับผิดชอบในการเปลี่ยนแปลงด้านการรักษาความมั่นคงปลอดภัย และการเปลี่ยนแปลงการจัดการด้านบริการ
14.การสิ้นสุดสัญญา	ผู้ให้บริการจัดจ้างภายนอกทำงานร่วมกับ ผู้ให้บริการจัดจ้างภายนอกรายใหม่ในการส่งต่อระบบ เพื่อให้	ผู้ให้บริการจัดจ้างภายนอกส่งต่อระบบการจัดการความมั่นคงปลอดภัย ให้กับผู้ให้บริการจัดจ้าง

ตารางที่ 4.3 (ต่อ) รายละเอียดเกี่ยวกับขั้นตอนการจัดการระบบรักษา ความมั่นคงปลอดภัย ในตลอดช่วงอายุสัญญา

ลำดับขั้นที่	กิจกรรม	กิจกรรมแบบชี้เฉพาะ
	สอดคล้องกับสัญญาที่ว่าด้วยการสิ้นสุดสัญญาให้บริการ	ภายนอกรายใหม่เพื่อให้สอดคล้องกับสัญญา ระบบการจัดการความมั่นคงปลอดภัย การวางแผน การสิ้นสุดการให้บริการ

6. การจัดการการเปลี่ยนแปลง

สัญญาสำคัญส่วนใหญ่จำเป็นต้องมีการเปลี่ยนแปลงวิธีการ หรือหลักการ เช่น การเปลี่ยนแปลงอาจมีส่วนเกี่ยวข้องกับระบบรักษา ความมั่นคงปลอดภัย อาจเป็นได้ทั้งด้านขอบเขต หน้าที่ และการดำเนินการของระบบ หรืออาจเพราะว่าข้อเรียกร้องด้านระบบรักษา ความมั่นคงปลอดภัย เองมีการเปลี่ยนแปลง ดังนั้น คณะผู้บริหารการจัดการการเปลี่ยนแปลงควรเป็นผู้ที่มีคุณสมบัติ มีประสบการณ์และเป็นผู้เชี่ยวชาญด้านระบบรักษา ความมั่นคงปลอดภัยทั้งจาก ผู้ว่าจ้าง และผู้ให้บริการจัดจ้างภายนอก

ในการเปลี่ยนแปลงย่อมมีค่าใช้จ่ายสูง เพราะฉะนั้นในสัญญาควรระบุไว้อย่างชัดเจนว่า สำหรับการเปลี่ยนแปลงด้านการรักษา ความมั่นคงปลอดภัย ขั้นตอนใดบ้างที่ ผู้ให้บริการจัดจ้างภายนอก หรือผู้ว่าจ้าง เป็นผู้ออกค่าใช้จ่าย เช่น ผู้ว่าจ้างจ่ายหากมีการเปลี่ยนแปลงขอบเขต ของการจัดจ้างภายนอก

ตารางที่ 4.4 ด้านล่างบอกให้ทราบถึงภาวะในการรับผิดชอบการเปลี่ยนแปลงของแต่ละฝ่าย ซึ่งอาจขึ้นอยู่กับลักษณะของ risk-reward strategies และโครงร่างด้าน ธุรกิจ ของ ผู้ว่าจ้าง และผู้ให้บริการจัดจ้างภายนอก

ตารางที่ 4.4 ความรับผิดชอบของการเปลี่ยนแปลงของแต่ละฝ่าย

รับผิดชอบในค่าใช้จ่ายช่วงเริ่มทำสัญญา และค่าใช้จ่ายเพิ่มเติม	ประเภทของการเปลี่ยนแปลง
ผู้ว่าจ้าง	• ความหลากหลายในขอบเขตของสัญญา • ความหลากหลายในระดับของการให้บริการ • ความหลากหลายในเรื่องระบบ และการ

ตารางที่ 4.4 (ต่อ) ความรับผิดชอบของการเปลี่ยนแปลงของแต่ละฝ่าย

รับผิดชอบในค่าใช้จ่ายช่วงเริ่ม ทำสัญญา และค่าใช้จ่ายเพิ่มเติม	ประเภทของการเปลี่ยนแปลง
	ดำเนินการ ● ความหลากหลายในเรื่องระบบ และประสิทธิภาพการดำเนินการ ● ข้อกำหนดที่หลากหลายของ ผู้ว่าจ้างในพื้นที่การให้บริการ ● การเพิ่มขึ้นของการจัดการด้านความมั่นคงในเทคโนโลยีเฉพาะต่าง ๆ ของผู้ว่าจ้าง ● ผู้ว่าจ้างมีการเปลี่ยนแปลงนโยบาย และมาตรฐานของการจัดการด้านความมั่นคงปลอดภัย ● สาเหตุจากผู้ว่าจ้างมีการตรวจสอบเหตุการณ์ของความมั่นคงปลอดภัย
ผู้ให้บริการจัดจ้างภายนอก	● ผู้ให้บริการจัดจ้างภายนอก มีการเปลี่ยนแปลงการบริการด้านข้อกำหนดเกี่ยวกับเทคโนโลยี สถานที่ และบุคคลากร ● การเพิ่มขึ้นของการจัดการด้านความมั่นคงในเทคโนโลยีเฉพาะต่าง ๆ ของ ผู้ให้บริการจัดจ้างภายนอก ● ความหลากหลายที่มาจากผลกระทบทางด้านการรักษาความมั่นคงปลอดภัย และการคุกคามทางธุรกิจของ ผู้ให้บริการจัดจ้างภายนอก ● การรักษาความมั่นคงปลอดภัยของ ผู้ให้บริการจัดจ้างภายนอก หรือองค์กรที่ 3 ซึ่งส่งผลกระทบต่อระบบของ ผู้ให้บริการจัดจ้างภายนอกเอง หรือต่อระบบของผู้ว่าจ้าง

ตารางที่ 4.4 (ต่อ) ความรับผิดชอบของการเปลี่ยนแปลงของแต่ละฝ่าย

รับผิดชอบในค่าใช้จ่ายช่วงเริ่ม ทำสัญญา และค่าใช้จ่ายเพิ่มเติม	ประเภทของการเปลี่ยนแปลง
ต้องทำการตกลงกันระหว่าง 2 ฝ่าย	• การเปลี่ยนแปลงของการประเมินการคุกคาม • การเปลี่ยนแปลงด้านนิติบัญญัติ หรือข้อกำหนด • การรรักษา ความมั่นคงปลอดภัย จากภายนอก และการ ตรวจสอบเหตุ การณ์ของความมั่นคงปลอดภัย

7. การจัดการสถานการณ์ที่เกิดขึ้น

ผู้ว่าจ้างมีการทำสัญญาข้อตกลงกับ ผู้ให้บริการ จัดจ้างภายนอก ที่จะทำรายงานแก่ผู้ที่ถูกเลือกจาก ผู้ว่าจ้าง ให้ทำการติดต่อกับ ผู้ให้บริการ จัดจ้างภายนอก ถึงระยะเวลาขั้นพื้นฐาน และรูปแบบทั้งหมดของการรักษาความมั่นคงปลอดภัย ซึ่งประกอบด้วย

- การรายงานสถานะการณ์ที่เกิดขึ้นทั้งหมด
- การรายงานเหตุการณ์ที่น่าสงสัย (ผิดปกติ)
- การรายงานเหตุการณ์ที่พึงระวัง
- การรายงานเหตุการณ์ที่มีความผิดปกติ
- การรายงานข้อกำหนดที่เกี่ยวกับกฎหมาย หรือผู้มีอำนาจในการรักษา ความมั่นคงปลอดภัย
- การรายงานที่เกี่ยวข้องกับข้อห้ามของคำสั่งศาล

มีการกำหนดข้อตกลงในสัญญาให้มีองค์กรบุคคลที่ 3 เข้ามาตรวจสอบข้อมูลด้านการรักษาความมั่นคงปลอดภัย โดยองค์กรภายนอกนั้นต้องได้รับสิทธิในการดูแลส่งเสริมการรักษา ความมั่นคงปลอดภัย

ผู้ว่าจ้างมีการทำสัญญาข้อตกลงกับผู้ให้บริการจัดจ้างภายนอกควรให้มีการตรวจสอบระบบรักษาความมั่นคงปลอดภัย และการแก้ไขสถานการณ์ของ ผู้ให้บริการจัดจ้างภายนอก อนุญาตให้ผู้ว่าจ้าง และหรือ องค์กรบุคคลที่ 3 ได้ใช้เวลาอย่างสมเหตุสมผล ในการตรวจสอบระบบ เครื่อข่าย ซอฟต์แวร์ การบันทึก ข้อมูลอื่น ๆ และปัจจัย อื่น ๆ ที่เกี่ยวข้องกับการรักษา ความมั่นคงปลอดภัย ที่

ผู้ว่าจ้าง หรือองค์กรบุคคลที่ 3 ร้องขอ และผู้ให้บริการ จัดจ้างภายนอกให้ความร่วมมืออย่างเต็มที่ในการ ตรวจสอบ และหากการตรวจสอบได้พบข้อผิดพลาดด้านการรักษา ความมั่นคงปลอดภัยประการใด จะต้องจัดให้มีการปรับปรุงแก้ไขตามที่ได้ทำสัญญาตกลงกันไว้

ผู้ว่าจ้าง ทำข้อตกลงให้ ผู้ให้บริการ จัดจ้างภายนอกยินยอม จากผู้ว่าจ้าง ในการให้ข้อมูลข่าวสาร หรือระบบการทำงานต่าง ๆ ที่มีส่วนเกี่ยวข้องกับธุรกิจของผู้ว่าจ้างก่อนที่จะให้กับองค์กรที่ 3 รวมถึงผู้บังคับใช้กฎหมาย ข้อกำหนด หรือผู้มีอำนาจ ในการรักษา ความมั่นคงปลอดภัย ยกเว้นกรณีที่มีการร้องขอตามกฎหมาย หรือผู้มีอำนาจของราชการ หรือที่ระบุอยู่ใน ข้อตกลงการทำสัญญา

เพิ่มเติมระเบียบแบบแผนการให้บริการ ในเรื่องของปัญหาที่อาจจะเกิดขึ้น และการแก้ไขความหายนะ ผู้ว่าจ้างทำข้อตกลงกับ ผู้ให้บริการจัดจ้างภายนอก ว่าขั้นตอนที่ควรนำมาใช้ในการจัดการสถานการณ์ควรรวมไปถึงเรื่องของระบบวงจรไฟฟ้าขั ดข้อง ซึ่งจะคุกคามการทำงานของ ผู้ให้บริการจัดจ้าง ตามข้อเรียกร้องด้านการรักษาความมั่นคงปลอดภัย

8. การสิ้นสุดสัญญา

ผู้ว่าจ้างทำสัญญาตกลงกับผู้ให้บริการจัดจ้างภายนอก ว่าจะทำก ารจัดการกับระบบรักษาความมั่นคงปลอดภัยกันอย่างไร แม้ในระหว่างช่วงสิ้นสุดสัญญา กระบวนการสิ้นสุดสัญญาควรมีการทำสัญญาตกลงเพื่อ

- การส่งมอบ การบริการกลับไปสู่ ผู้ว่าจ้าง หรือผู้ที่มารับช่วงสัญ ญาต่อ ซึ่งยังคงไว้ซึ่งการจัดการระบบรักษาความปลอดภัย และความต้องการต่อความเสี่ยง อย่างมีประสิทธิภาพ
- ส่งมอบเอกสารทั้งหมดให้กับผู้ว่าจ้างไม่ว่าจะเป็นไฟล์ กระบวนการ โครงสร้าง และบันทึกที่เกี่ยวข้องกับการให้บริการแก่ผู้ว่าจ้าง
- ทำลายสำเนาเอกสาร และบันทึกต่างๆ ที่มีข้อมูลของ ผู้ว่าจ้างหรือหากมีการกักเก็บไว้ก็ให้เป็นไปตามข้อตกลงในสัญญาที่ว่าด้วยการกักเก็บและการรักษาความปลอดภัยของสำเนาข้อมูล

- ส่งมอบหรือทำลายข้อมูลทั้งหมดที่เก็บไว้ในแผ่นบันทึก หรือ เทป

- ออกประกาศรับรองโดยผู้อำนวยการขององค์กรผู้ให้บริการว่า ได้มีการทำลายข้อมูลของผู้ว่าจ้าง

- เก็บรักษาความลับและป้องกันข้อมูลข่ าวสารที่ข้อสัญญาได้อนุญาตให้ ผู้ให้บริการจัดจ้างภายนอกคงไว้ตลอดช่วงการสิ้นสุดสัญญา

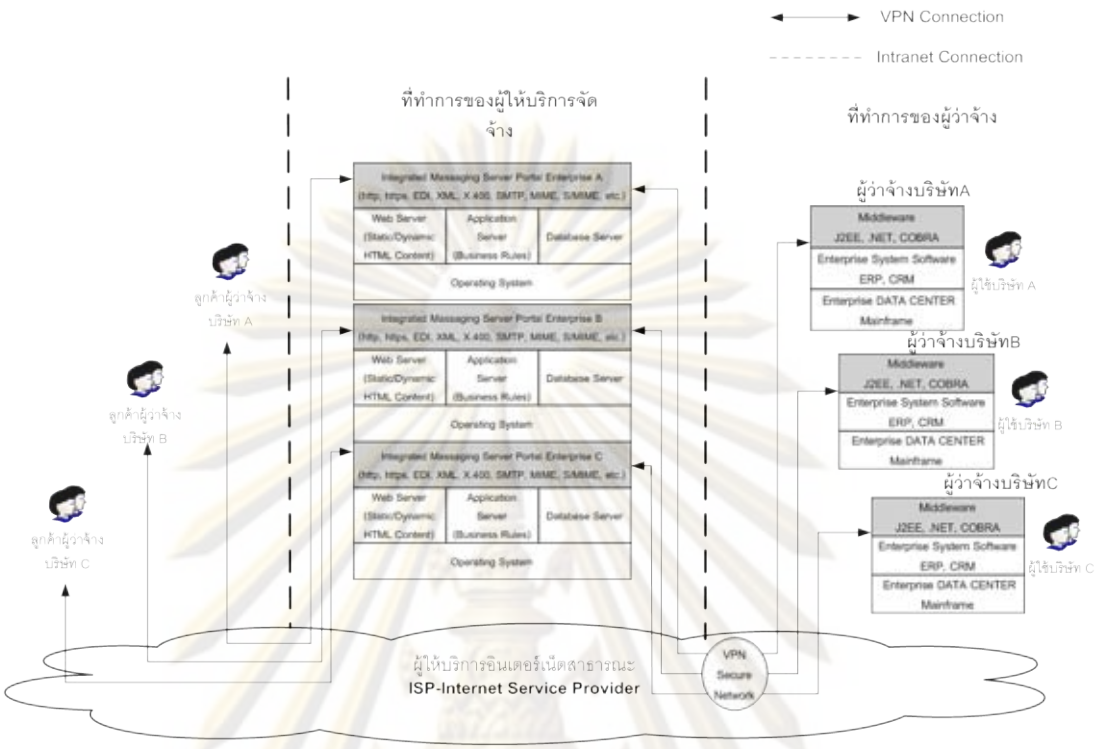
4.2.2 โครงสร้างการจัดจ้างภายนอกที่ทำการผู้ว่าจ้าง

โครงสร้างของการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง ผู้วิจัยนำโครงสร้างที่ รามาน [3] ได้นำเสนอเกี่ยวกับการให้บริ การจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้าง และได้มีการกำหนดระบบความมั่นคงความปลอดภัยที่เกี่ยวข้อง เพื่อสร้างความน่าเชื่อถือให้กับผู้ว่าจ้างและการบริการจัดจ้างที่มีประสิทธิภาพ โดยมีองค์ประกอบสองส่วนดังตาราง 4.6

1. สถาปัตยกรรมการให้บริการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง
2. การจัดการความมั่นคงปลอดภัยของผู้ให้บริการจัดจ้างภายนอก

4.2.2.1. สถาปัตยกรรมการให้บริการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง

กำหนดโครงสร้างของการให้บริการจัดจ้างภายนอกโดยแยกการให้บริการออกจากที่ทำการ (Premise) ของผู้ว่าจ้าง ซึ่งนำหลักการของซอมเมอร์และรามาน มาใช้ในการแยกระบบของผู้ให้บริการจัดจ้างภายนอก ให้อยู่นอกที่ทำการผู้ว่าจ้าง การเชื่อมต่อกันจะมีศูนย์กลางที่เป็นผู้ให้บริการ ระหว่างผู้ใช้ในที่ทำการของผู้ว่าจ้างกับบริษัทที่รับจัดจ้างภายนอก และระหว่างลูกค้าของผู้ว่าจ้างกับบริษัทที่รับจัดจ้างภายนอก เพื่อให้สามารถคอยติดตามตรวจจับการโจมตีที่ผ่านจากลูกค้าของผู้ว่าจ้างที่ใช้งานบนระบบอินเตอร์เน็ต และจากผู้ใช้ในที่ทำการของผู้ว่าจ้างด้วย โดยแสดงสถาปัตยกรรมในภาพรวม ดังแสดงไว้ในรูปที่ 4.4



รูปที่ 4.4 สถาปัตยกรรมการให้บริการของผู้ให้บริการจัดจ้างภายนอกโดยอยู่นอกที่ทำการผู้ว่าจ้าง

รูปแบบการให้บริการโปรแกรมประยุกต์ของผู้ให้บริการจัดจ้างภายนอก โดยอยู่นอกที่ทำการของผู้ว่าจ้างได้มีโครงสร้างดังรูปที่ 4.4 โดยผู้ให้บริการจัดจ้างภายนอกจะมีการ บริการศูนย์บริการโปรแกรมประยุกต์ บริการเครือข่าย และบริการซอฟต์แวร์ โดยมีรายละเอียดดังนี้

1. การให้บริการศูนย์บริการ โปรแกรมประยุกต์ ประกอบ ด้วยหลายส่วนที่ประกอบเป็นเซิร์ฟเวอร์ฟาร์ม ดังนี้

— กลุ่มเซิร์ ฟเวอร์ที่ทำหน้าที่ให้บริการเว็บ เป็นตัว กลางที่ทำหน้าที่ในการเชื่อมต่อระหว่างผู้ว่าจ้าง และผู้ให้บริการจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้าง ทำหน้าที่เป็นศูนย์กลางเชื่อมต่อระหว่าง โปรแกรมประยุกต์ ที่เรียกว่า มิดเดิลแวร์ (middleware) ซึ่งสามารถรองรับโปรแกรมได้หลายภาษา และรองรับเทคโนโลยี XML และทำหน้าที่แลกเปลี่ยนข้อมูลสารสนเทศระหว่างผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก และมีการบริการระบบความมั่นคงดังนี้

- การบริการการพิสูจน์ตัวจริง (authentication service)
- การบริการเชื่อมโยงตัวบุคคลกับการบริการ (identity mapping service)
- การบริการกำหนดสิทธิ์ (authorization service)
- การบริการนโยบาย (policy service)

- การแปลงหนังสือรับรอง (credential conversion service)
- การบริการตรวจสอบ (Audit Service)
- การบริการบรรยายลักษณะ (profile service)
- การบริการความเป็นส่วนตัว (privacy service)

— อุปกรณ์ทำหน้าที่ติดตาม (IDS-Intrusion Detection System) และเฝ้าระวังการจราจรที่เกิดขึ้นในระบบ และการทำงานรวมถึงความสัมพันธ์ที่เชื่อมต่อระหว่างผู้ให้บริการจัดจ้างภายนอกกับผู้ว่าจ้าง และมีการส่งข้อความแจ้งเตือนอัตโนมัติเมื่อเกิดเหตุการณ์ผิดปกติที่ได้มีการทำข้อตกลงกันไว้ให้แก่ผู้ดูแลระบบทั้งผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก มีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ

- ความพยายามในการบุกรุกผ่านระบบเครือข่าย
- การใช้งานในลักษณะที่ผิดปกติ
- การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

— กลุ่มเซิร์ฟ เวอร์ที่ทำหน้าที่ ให้บริก ารโปรแกรมประยุกต์ที่ทำห น้าที่ให้บริการแก่ผู้ว่าจ้างและลูกค้าของผู้ว่าจ้าง โ ดยมีผู้ให้บริการจัดจ้างภายนอกเป็ นผู้ดูแลและใช้มาตรฐาน ISO/IEC 27001 ในการจัดการด้านความปลอดภัย

— กลุ่มเซิร์พเวอร์ที่ทำหน้าที่ในการเก็บข้อมูล ไว้เพื่อทำงานกับระบบจัดการฐานข้อมูล เช่น SQL , Informix เป็นต้น โดยภายในเซิร์ฟเวอร์ มีทั้งฐานข้อมูลและตัวจัดการฐานข้อมู ล และใช้มาตรฐาน ISO/IEC 27001 ในการจัดการด้านความปลอดภัย

— ไฟวอลล์ เป็นเสมือน กำแพงกันระหว่างกลุ่มเซิร์ฟ เวอร์ และผู้ ใช้งานโดย มีการกำหนด ให้เฉพาะข้อมูลที่มีคุณลักษณะตรงกับเงื่อนไขที่ กำหนดไว้ผ่านเข้าออกระบบเครือข่ายภายในเท่านั้น และมีการจัดการด้านความปลอดภัยตามมาตรฐาน ISO/IEC 27001

2. การให้บริการ เครือข่าย ทำหน้าที่เชื่อมต่อระหว่างผู้ให้บริการจัดจ้างภายนอกกับผู้ว่าจ้าง โดยอาศัยส่งช่วงต่อให้กับผู้ให้บริการ เครือข่ายอินเตอร์เน็ต (ISP-Internet Service Provider) ซึ่งใช้เทคโนโลยีเอ็มพีแอลเอ็ส (MPLS- Multi Protocal Label Switching) ที่มีการส่งแบบ Streamline ทำให้สามารถรับประกันเกี่ยวกับปริมาณข้อมูลต่อเวลาได้เป็นอย่างดี เพื่อใช้งานในลักษณะ แบบทันกาล (Real-Time) รวมทั้งสามารถที่จะกำหนดระดับ คุณภาพ (QoS-Quality Of Service) และ

รองรับเทคโนโลยี วีพีเอ็น (VPN-Virtual Private Network) นั้นคือการสร้าง เครือข่าย เสมือนในการเชื่อมต่อระหว่างผู้ว่าจ้าง และผู้ให้บริการจัดจ้างภายนอกเพื่อเป็นการป้องกันข้อมูลของผู้ว่าจ้าง

3. การให้บริการซอฟ ต์แวร์ โดย ผู้ให้บริก ารจัดจ้างภายนอกทำหน้าที่จัดหาซอฟ ต์แวร์ที่ให้บริการกับผู้ว่าจ้างซึ่งมีทั้ง ซอฟ ตแวร์สำเร็จรูปที่ทำหน้าที่รองรับการให้บริการ และโปรแกรมประยุกต์ที่มีการพัฒนาขึ้นเอง ตามวัตถุประสงค์ของผู้ ว่าจ้าง รวมทั้งการบริการติดตั้ง การจัดการ การบำรุงรักษา และการจัดซื้อ

4.2.2.2 ระบบความมั่นคงปลอดภัยของผู้ให้บริการจัดจ้างภายนอก

การให้ความรับรองกับผู้ว่าจ้าง ว่าข้อมูลของผู้ว่าจ้าง นั้นจะมีความสมบูรณ์ เป็นความลับและปลอดภัย จะต้องมีการควบคุมรูปแบบความมั่นคงปลอดภัยเป็นสิ่งที่ต้องคำนึงอย่างมาก

เพื่อให้ โครงสร้างของระบบ ความมั่นคง ปลอดภัย มีการกำหนดแนวทาง การควบคุมการปฏิบัติงานและการรักษา ความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศของลูกค้า ได้อย่างมีประสิทธิภาพและมีมาตรฐานในระดับเดียวกัน ผู้ให้บริการจัดจ้างจึงได้วางแนวทางการควบคุมการปฏิบัติงานและการรักษา ความมั่นคงปลอดภัย ด้านเทคโนโลยีสารส นเทศให้กับผู้ว่าจ้าง โดยอ้างอิงจากมาตรฐาน ISO/IEC 27001 [13] มีองค์ประกอบดังต่อไปนี้

1. นโยบายความมั่นคงปลอดภัย มีการจัดให้มีนโยบาย ข้อกำหนด และการประกาศ ด้านการรักษาความมั่นคงปลอดภัยภายในองค์กรของผู้ให้บริการจัดจ้าง

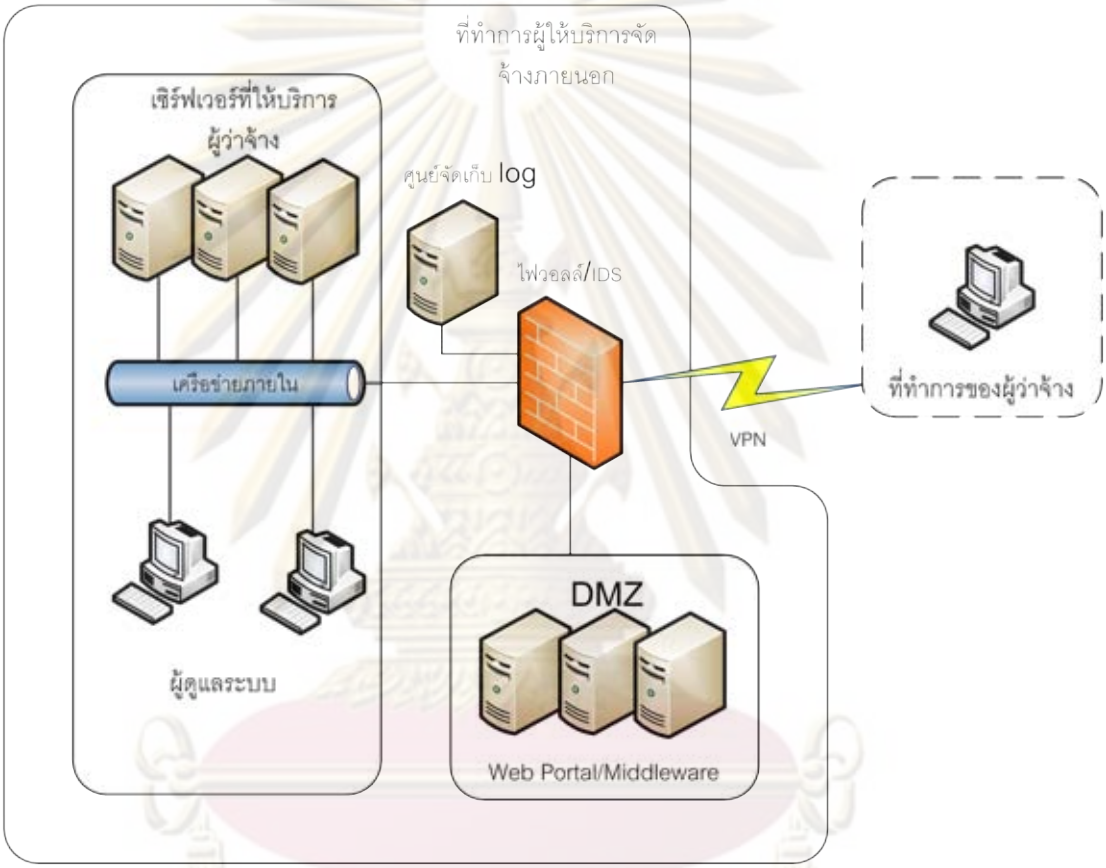
2. โครงสร้างทางด้านความมั่นคงปลอดภัย สำหรับองค์กร มีการจัดทำข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภั ยทั้งหมดที่เกี่ยวข้อง เช่น ข้อมูลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย ข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยที่ทำกับผู้ว่าจ้าง

3. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม โดยมี เนื้อหาค รอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และระบบป้องกันความเสียหายต่างๆ ที่ผู้ให้บริการจัดจ้างควรจัดให้มีภายในศูนย์คอมพิวเตอร์ โดยครอบคลุมประเด็นต่าง ๆ ดังนี้

- การควบคุมศูนย์คอมพิวเตอร์
- การป้องกันความเสียหายที่เกิดจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติ

4. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร ซึ่งประกอบด้วย

— ความมั่นคงปลอดภัย ระบบการเชื่องโยงภายนอก องค์กรระบบความมั่นคงปลอดภัยให้กับการเชื่อมต่อระหว่างผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก และเชื่อมโยงระหว่างส่วนง านต่าง ๆ ที่เกี่ยวข้องแสดงดังรูปที่ 4.5 โดยมีการกำหนดดังนี้



รูปที่ 4.5 แสดงผังโครงข่ายภายในของผู้ให้บริการจัดจ้างภายนอก

— ความมั่นคงปลอดภัย เครือข่าย ภายในองค์กรผู้ ให้บริการจัดจ้างภายนอก มีการกำหนดนโยบายเพื่อป้องกันการบุกรุกจากผู้ไม่ประสงค์ดี โดยมีการตรวจจับ เหตุผิดปกติในระบบเครือข่าย

— มีการควบคุมการปิดช่องโหว่ในระบบปฏิบัติการของเซิร์ฟเวอร์ และเครื่องคอมพิวเตอร์ภายในองค์กร รวมถึงการป้องกันไวรัส

— ความมั่นคงปลอดภัย ข้อมูล ครอบคลุมรายละเอียดเกี่ ยวกับแนวทางในการรักษาความมั่นคงปลอดภัยของข้อมูล และความเสี่ยงของการสูญหายของข้อมูล การสำรองข้อมูลระบบคอมพิวเตอร์

— มีกระบวนการตรวจสอบทานระบบความปลอดภัย โดยกำหนดหน้าที่ของผู้ตรวจทานอย่างชัดเจน และรับรองผู้ตรวจทานจากภายนอก

— การตรวจสอบและติดตามระบบ ความมั่นคงปลอด ภัยเพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่างๆ ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน

— การควบคุมความปลอดภัยของสื่อที่ใช้ในการบันทึกข้อมูล

5. การควบคุมการเข้าถึง มีการควบคุมการเข้าถึงข้อมูลสารสนเทศภายในองค์กร ประกอบด้วย

— การจัดการการเข้าถึงของผู้ใช้งาน

— การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

— การควบคุมการเข้าถึงเครือข่าย

— การควบคุมการเข้าถึงระบบปฏิบัติการ

— การควบคุมเข้าถึงโปรแกรมประยุกต์

— การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน และรหัสผ่าน

6. การจัดหา การพัฒนาดู และการบำรุงรักษาระบบสารสนเทศ เพื่อเพิ่มประสิทธิภาพของความมั่นคงปลอดภัยเพื่อให้ตรงตามมาตรฐานความปลอดภัย และความต้องการกับผู้ร้องขอ

— มีการศึกษาความต้องการของผู้ร้องขอ

— มีการเลือกกระบวนการของโปรแกรมประยุกต์เพื่อให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัย

— มีการจัดการความมั่นคงปลอดภัยกระบวนการติดตั้งโปรแกรมประยุกต์

— มีการจัดการเทคโนโลยีการตรวจหาและปิดช่องโหว่ในระบบ

7. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร ของผู้ให้บริการจัดจ้างภายนอกเพื่อเป็นการควบคุมความมั่นคงปลอดภัยของผู้ใช้งานในระบบ

— มีการระบวนการจัดการผู้ใช้งานที่เข้าใหม่

— มีการะบวนการจัดการผู้ใช้งานที่ดำเนินงานภายในองค์กร

— มีการะบวนการจัดการผู้ใช้งานที่ลาออก

8. การบริหารจัดการทรัพย์สินขององค์กร มีการจัดการทะเบียนคุมทรัพย์สินเพื่อมีการแสดงหน้าที่ความรับผิดชอบผู้แลทรัพย์สินขององค์กร

— มีการจัดทำทะเบียนคุมทรัพย์สินและผู้ดูแล

— มีการจัดกลุ่มของข้อมูล

9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

— มีการรายงานสถานะการณ์เกี่ยวกับ เหตุการณ์ที่ปกติ และเหตุการณ์ที่ไม่ปกติ

— มีการบริหารจัดการสถานะการณ์ และการพัฒนาประสิทธิภาพ

10. การบริหารความต่อเนื่องในการดำเนินธุรกิจ

— มีการจัดการรักษาการดำเนินธุรกิจให้มีความต่อเนื่อง เช่น การจัดการดำเนินการรักษาความมั่งคงปลอดภัย การทำเครื่องมือประเมินความเสี่ยง

— มีการสร้างความเข้าใจในการให้ความสำคัญของการรักษาการดำเนินธุรกิจให้มีความต่อเนื่องให้กับบุคคลากร และองค์กร

— มีการสร้างแผนการดำเนินการเพื่อให้ธุรกิจดำเนินงานต่อเนื่องได้ และมีการทดสอบอย่างสม่ำเสมอ

11. การปฏิบัติตามข้อกำหนด

— มีการปฏิบัติตามข้อตกลงหรือกฎหมายที่ ทางรัฐบาล หรือหน่วยงานภาครัฐเป็นผู้กำหนด หรือขึ้นอยู่กับกฎข้อบังคับของผู้ว่าจ้าง เช่น ตามกฎหมายเกี่ยวกับพระราชบัญญัติคอมพิวเตอร์ พ .ศ 2550 หรือ กฎข้อบังคับด้านความปลอดภัยที่อ้างอิงจากธนาคารแห่งประเทศไทย

4.2.3. **การทำข้อตกลงร่วมกันของคู่สัญญาระหว่างผู้ว่าจ้ างและผู้ให้บริการจัดจ้างภายนอก**

ในการประเมินการจัดจ้างภายนอก ผู้ว่าจ้างในกรณีศึกษาให้ความสำคัญกับการทำ SLA เพื่อเป็นการสร้างความน่าเชื่อถือในการให้บริการของผู้ให้บริการจัดจ้างภายนอก ดังนั้นจึงมีการนำเสนอแนวทางการทำ SLA ที่อ้างอิงมาจากงานวิจัยของแทนจา และสเตฟาน [17]

SLA นั้นจะทำหน้าที่เพื่อแสดงรายละเอียดในหน้าที่ความรับผิดชอบของผู้ให้บริการจัดจ้างภายนอก ใน SLA นั้นจะระบุรายละเอียดการให้บริการของผู้ให้บริการจัดจ้างภายนอกเพื่อเป็นการ

รับประกันความเสี่ยงและความมั่นคงปลอดภัย ให้แก้ผู้ว่าจ้าง องค์ประกอบและการออกแ บบ SLA จะขึ้นอยู่กับความต้องการของผู้ว่าจ้าง ลักษณะธุรกิจของผู้ว่าจ้าง การพัฒนาโปรแกรม คอมพิวเตอร์ ความต้องการภายในองค์กรของผู้ว่าจ้าง ความสามารถ ในการรองรับความต้องการ รวมถึงเป้าหมายขององค์กร ซึ่งจะต้องสามารถตรวจสอบและวัดได้ เพื่อให้ความมั่นใจกับผู้ว่าจ้าง SLA ของผู้ให้บริการจัดจ้างภายนอกที่ให้บริการโปรแกรมคอมพิวเตอร์ที่อยู่นอกที่ทำการของผู้ว่าจ้างมีการแบ่งออกเป็นหัวข้อดังนี้

1. SLA ของระบบเครือข่าย ซึ่งรูปแบบการให้บริการจัดจ้างภายนอกอยู่นอกที่ทำการของผู้ว่าจ้างนั้นต้องอาศัยระบบ เครือข่าย ในการเชื่อมต่อระบบเพื่ อให้บริการกับผู้ว่าจ้าง ดังนั้น SLA ของระบบ เครือข่าย จะครอบคลุม เครือข่าย ที่เชื่อมต่อระหว่างผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก ประสิทธิภาพของเครือข่าย ที่ผู้บริการจัดจ้างเป็นผู้จัดให้ ดังนั้นสิ่งสำคัญของการทำ SLA มีดังนี้

- ความพร้อม ของระบบ เครือข่าย (availability network) การทำงานของระบบเครือข่ายนั้นสามารถวัดได้จากเปอร์เซ็นต์ของเวลาการทำงานระบบ เครือข่าย ผลรวมของเวลาที่ เครือข่ายทำงานอยู่ ที่ผู้ว่าจ้างและลูกค้าของผู้ว่าจ้างสามารถใช้งานระบบได้ ความเหมาะสมในการรับประกันของความพร้อมใช้งานของระบบ เครือข่าย นั้นขึ้นอยู่กับชนิดของ โปรแกรมที่ให้บริการกับผู้ว่าจ้าง และประเภทของธุรกิจของผู้ว่าจ้าง
- ปริมาณงานของระบบ เครือข่าย (network throughput) ปริมาณงานของระบบเครือข่าย ณ ช่วงเวลาหนึ่งคือผลรวมของแบนวิด (bandwidth) ที่มีอยู่ ความเป็นไปได้ที่เกิดความล่าช้า (delay) และความหนาแน่นของการจราจรใน เครือข่าย ซึ่งปกติแล้วการทำงานของระบบ เครือข่าย ขึ้นอยู่กับ เครือข่าย หลัก (backbone) ดังนั้นประสิทธิภาพของ เครือข่ายหลักก็จะส่งผลกับประสิทธิภาพในการให้บริการ เครือข่ายของผู้ให้บริการจัดจ้างภายนอก
- ความมั่นคงปลอดภัยระบบเครือข่าย (security network) ความมั่นคงปลอดภัย ระบบเครือข่าย นั้นผู้ว่าจ้างให้ความสำคัญมาก และยังร วมถึงการดูแลรักษา ความมั่นคงปลอดภัย ของข้อมูลด้วย ดังนั้น SLA จึงมีการกำหนดวิธีการรักษา ความมั่นคงปลอดภัย ไฟวอลล์ การเข้าระหัส VPN การจัดเก็บบันทึกสถานะการณ์ การตรวจจับความผิดปกติในระบบเครือข่าย ซึ่งจะต้องมีการจัดขึ้นจริง

- การสูญหายของข้อมูลบนเครือข่าย (data loss) เมื่อข้อมูลบนเครือข่ายมีปริมาณมากเกินกว่าจะรับได้ มักจะเกิดเหตุการณ์ข้อมูลสูญหาย หรือเกิดความล่าช้าได้ ซึ่งการรับประกันข้อมูลสูญหาย ความล่าช้าของข้อมูล เป็นสิ่งสำคัญอย่างมากสำหรับโปรแกรม ประยุกต์ที่ทำงานแบบ ทันกาล ดังนั้น SLA ของการจัดจ้างภายนอกนั้นทั่วไปแล้วจะมีการรับประกันข้อมูลสูญหาย 99% ของข้อมูลที่ส่งมาแบบทัน กาล ซึ่งมีการยอมรับได้ที่ข้อมูลสูญหายได้ไม่เกิน 1% แต่ขึ้นอยู่กับประเภทของธุรกิจด้วย

2. SLA ของศูนย์ให้บริการโปรแกรมคอมพิ วเตอร์ (SLA hosting) รูปแบบการให้บริการโปรแกรมคอมพิวเตอร์ของผู้ให้บริการจัดจ้างภายนอกมีโครงสร้างอยู่นอกที่ทำการของผู้ว่าจ้างจะมีการให้บริการศูนย์บริการโปรแกรมคอมพิวเตอร์ ซึ่งการให้บริการนั้นแสดงรายละเอียดของการทำงานอยู่ใน SLA มีดังนี้

- การทำงานของเซิร์พเวอ ร์ (server availability) ซึ่งรวมถึงการทำงานทั้ง ฮาร์ ทแวร์ และ ระบบปฏิบัติการ ซึ่งสามารถวัด การทำงานของเซิร์ฟเวอร์ ได้จากเปอร์เซ็นต์ ของเวลา ที่เซิร์ ฟเวอร์ สามารถทำงานได้ เกณฑ์มาตรฐานจะอยู่ระหว่าง 99%-100% ขึ้นอยู่กับการจัดการระบบเซิร์พเวอร์ ความพร้อมใช้งานของเซิ ร์พเวอร์เป็นสิ่งสำคัญในการให้บริการโปรแกรมคอมพิวเตอร์ของผู้ให้บริการจัดจ้างภายนอก จึงต้องมีการพิจารณาเป็นพิเศษและรวมถึงชนิดของโปรแกรมคอมพิวเตอร์ที่ให้บริการ และความต้องการทางธุรกิจของผู้ว่าจ้าง
- การสำรองข้อมูล (backup data) ข้อมูลของลูกค้าเป็นสิ่งสำคัญอย่า งยิ่ง ดังนั้นการสำรองข้อมูลจึงเป็นสิ่งสำคัญจึงต้องมีการสำรองข้อมูลลงเทป ทุกวันหรือทุกสัปดาห์ ขึ้นอยู่กับสถานะของโปรแกรมคอมพิวเตอร์ที่ให้บริการ แล ะรูปแบบธุรกิจของผู้ว่าจ้าง และต้องมีการนำไปจัดเก็บยังสถานที่ปลอดภัยอย่างน้อยเป็นเวลา 60 วัน ซึ่งการกำหนดรูปแบบก ารสำรองข้อ มูลนั้นนอกจากจะขึ้นกับโปรแกรมคอมพิวเตอร์ และรูปแบบธุรกิจของผู้ว่าจ้างแล้ว ผู้ว่าจ้างและผู้ให้บริการจัดจ้างต้องมีการทำข้อตกลงกันในการทำ SLA ที่เกี่ยวกับการสำรองข้อมูล
- ความมั่นคงปลอดภัย ของเซิร์ฟเวอร์ทางกายภาพ (physical server security) ความมั่นคงปล อดภัย ทางกายภาพของศูนย์ข้อมูล จะต้องมีการควบคุมการเข้าถึงข้อมูล โดยมีการ ยืนยันชื่อผู้ใช้ และมีการติดตั้ ง กล้องวงจะปิด ตู้จัดเก็บเซิร์ ฟเวอร์และอุปกรณ์ต่าง ๆ มีระบบแจ้งเตือนจากภัยที่อาจเกิดขึ้นทุกประเภท ผู้ให้บริการจัดจ้างมี

การจัดการตรวจสอบของศูนย์ข้อมูลทั้งหม ด ซึ่งต้องเพียงพอต่ อความต้องการของผู้ว่าจ้างในทุกๆ ด้าน

3. SLA ของโปรแกรม คอมพิวเตอร์ (application SLA) SLA ของโปรแกรมคอมพิวเตอร์สามารถวัดได้จากประสิทธิภาพของโปรแกรมคอมพิวเตอร์ ผู้ให้บริการจัดจ้างภายนอกต้องมีการแสดงรายละเอียดของขอบเขตหน้าที่ความรับผิดชอบอย่างชัดเจน ซึ่งประกอบด้วยประสิทธิภาพในการวัดประสิทธิภาพของโปรแกรมคอมพิวเตอร์ และบทลงโทษสำหรับความล้มเหลวในระดับที่ได้มีการทำการตกลงกันไว้ระหว่างผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก

- ความพร้อมใช้งานของโปรแกรมคอมพิวเตอร์ (application availability) คือผู้ใช้งานสามารถเชื่อ มต่อกับศูนย์ข้อมูลได้ และสามารถใช้งานโปรแกรมคอมพิวเตอร์ได้ตามความต้องการ ปัญหาความขัดข้องของโปแกรมคอมพิวเตอร์มีหลายสาเหตุ แต่ส่วนมากเกิดจากความผิดพลาดของ เครือข่าย ที่เชื่อมต่อ เซิร์ ฟเวอร์ หรือเกิดจากความขัดข้องของตัวโปรแกรมคอมพิวเตอร์เอ ง ในการวัดความพร้อมใช้งานของโปแ กรมคอมพิวเตอร์ สามารถวัดได้จากเวลาทั้งหมดในการทำงานของโปรแกรมคอมพิวเตอร์ที่เป็นชั่วโมงหรือนาที และเวลาในการหยุดให้บริการเพื่อซ่อมบำรุงโปรแกรมคอมพิวเตอร์ ซึ่งควรที่จะอ้างอิงถึงความพร้อมใช้งานจากมุมมองของผู้ใช้
- ประสิทธิภาพของโปรแกรมคอ มพิวเตอร์ (application performance) ในการตรวจวัดประสิทธิภาพของโปรแกรมคอมพิวเตอร์เป็นไปได้ค่อนข้างยาก แต่โดยทั่วไปแล้วในการวัดประสิทธิภาพของโปรแกรมคอมพิวเตอร์โดยวัด ความเร็วในตอบสนองของโปรแกรมคอมพิวเตอร์ อัตราส่งข้อมูล โดยเฉพาะอย่างยิ่งสำหรับระบบที่เป็นออนไลน์ ซึ่งควรรวมอยู่ในการทำ SLA ด้วย
- ความมั่นคงปลอดภัย ของโปรแกรมคอมพิวเตอร์ (application security) ผู้ให้บริการจัดจ้างภายนอกมีการทำข้อตกลงใน SLA ว่ามีการรักษา ความมั่นคงปลอดภัย ให้กับโปรแกรมคอมพิวเตอร์เช่น ไฟวอลล์ เทคโนโลยี SSL การจัดการไวรัส เครือข่าย และการยืนยันตัวบุคคล ว่าได้มีการอ้างอิงถึงด้วย
- การยกระดับโปรแกรมคอมพิวเตอร์ (software upgrades) ควรมีการกำหนดอยู่ใน SLA คือมีการกำหนดเวอร์ชั่นของโปรแกรมคอมพิวเตอร์ ที่ผู้ให้บริการรองรับอยู่ และกำหนดเวอร์ชั่นของโปรแกรมคอมพิวเตอร์ที่ทำการส่งมอบที่ได้มีการยกระดับโปรแกรมคอมพิวเตอร์ล่าสุด

4. SLA การบริการดูแลและผู้ให้บริการช่วยเหลือ (customer care/help desk SLA) โดยทั่วไปแล้วการให้บริการดูแลทั้งทางด้านเทคนิค (helpdesk) และไม่ใช้ทางเทคนิค (customer care) ให้แก้ผู้ว่าจ้าง การบริการนี้แสดงให้เห็นในการทำ SLA ที่เกี่ยวกับบุ คคล มีการกำหนดสำหรับการช่วยเหลือ และดูแลให้กับผู้ว่าจ้างมีดังนี้

- ความพร้อมใช้งาน (availability) SLA นี้จะประกอบด้วยการตกลงร่วมกันระหว่างผู้ว่าจ้างและผู้ให้บริการจัดจ้างภา ยนอก ซึ่งมีการกำหนดคุณสมบัติต่า งๆ เช่น เวลาในการให้ความช่วยเหลือได้ (คิดเป็นชั่วโมง) และ ความเร็วในการตอบคำถามได้ ซึ่งในบางกรณีจะมีการทำข้อตกลงเกี่ยวกับ อัตราการตอบสนองให้กับผู้ใช้ได้ (คือผู้ใช้ที่รอเพื่อขอความช่วยเหลือจากผู้บริการให้ความช่วยเหลือ)
- เวลาในการแก้ปัญหา (problem resolution time) ซึ่งขึ้นอยู่กับประเภทหรือชนิดของโปรแกรมคอมพิวเตอ ร์ ซึ่งถ้าใช้เวลาน้อยในการแก้ไขปัญหานั้นจะเป็นผลดีกับธุรกิจของผู้ว่าจ้าง และรูปแบบในการติดต่อสื่อสารระหว่างผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก เช่น โทรศัพท์ จดหมายอิเล็คทรอนิกส์ โปรแกรมเว็บ มีการจัดลำดับของปัญหาและต้นกำเนิดของปัญหา
- ความพึงพอใจของผู้ว่าจ้ างและลูกค้า (customer satisfaction) ขึ้นอยู่กับคุณภาพของการบริการที่ให้กับผู้ว่าจ้าง โดยผู้ให้บริการ และผู้ให้ความช่วยเหลือ เช่น การให้ข้อมูลที่ถูกต้อง มีการตอบส นองอย่างรวดเร็ว ความมีมารยาท แล ะความมีมนุษยสัมพันธ์ที่ดี

5. ส่วนเพิ่มเติมของการทำ SLA (additional SLA categories) นอกจากที่การทำ SLA ส่วนใหญ่มักจะมีการรับรองด้านการบริการทั่วไป เช่น ความพร้อมใช้งานโปรแกรมคอมพิวเตอร์ ความพร้อมในการรองรับความช่วยเหลือ แล้วยังมีส่วนอื่นที่ต้องคำนึงอีกมากมายซึ่งบางที่ผู้ให้บริการจัดจ้างภายนอกไม่สามารถควบคุมได้ เช่น ผู้ ให้บริการจัดจ้างภายนอกที่ให้บริการโปรแกรมที่ทำงานบนเว็บ และอยู่นอกที่ทำการของผู้ว่าจ้างนั้นจะต้องมี เครือข่ายเพื่อใช้ในการติดต่อระหว่างผู้ว่าจ้างและศูนย์ข้อมูลที่อยู่ที่ทำการของผู้ให้บริการจัดจ้างภายนอก ซึ่ง เครือข่าย นั้นต้องพึ่งพาผู้จัดหาให้บริการ เครือข่าย (supplier) อีกทีหนึ่ง จึงทำให้ไม่สามรถควบคุมได้ ดังนั้นผู้ให้บริการจัดจ้างภายนอกทำการนำเอารายละเอียดทั้งหมด SLA ที่เกี่ยวข้องที่ได้ทำกับผู้ว่าจ้างไปอยู่ในการทำ SLA ระหว่างผู้ให้บริการจัดจ้างภายนอกกับผู้จัดหาให้บริการ เครือข่าย เพื่อเป็นการรับประกันให้กับผู้ ว่าจ้าง ซึ่งส่วนเพิ่มเติมการทำ SLA นั้นจะเป็นตัวช่วยให้การทำ SLA มีประสิทธิภาพมากขึ้นด้วย การแบ่งหมวดของส่วนเพิ่มเติมมีดังนี้

- การเพิ่มข้อปฏิบัติในการแก้ไขปัญหา ซึ่งประกอบด้วย กระบวนการ และบุคคลที่ทำหน้าที่รองรับชนิดของปัญหาการบริการ ต้องถูกเพิ่มเข้าไปใน SLA ด้วย ซึ่งจะต้องมีกระบวนการที่เฉพาะเมื่อเกิดเหตุการที่เกิดการขัดแย้ง จะต้องมีการแต่งตั้งบุคคลที่ 3 เข้ามามีหน้าที่ในการปราณีประนอม และตรวจสอบก ระบวนการของ SLA ในกรณีที่การปราณีประนอมไม่สำเร็จ SLA จะต้องยึดเอากฎหมายเป็นตัวในการแก้ปัญหาความขัดแย้ง
- เมื่อผู้ให้บริการจัดจ้างภายนอกทำหน้าที่ในการดูแลและรักษาระบบเป็นประจำ ถ้าเกิดเหตุการณ์ระบบขัดข้องขึ้นมา จะต้องมีมาตรการเพื่อบรรเทาเหตุการณ์ที่เกิดขึ้นในการสร้างความน่าเชื่อถือให้กับผู้ว่าจ้าง ในการทำ SLA จะต้องมีการทำข้อตกลงในการมีค่าชดเชยจากความเสียหายโดยตรงเมื่อเกิดเหตุการณ์ระบบขัดข้องขึ้นมา
- เมื่อถึงเวลาครบสัญญาแล้ว ซึ่งโดยทั่วไปแล้วจะอยู่ในระยะเวลาประมาณ 1-3 ปี จะต้องมีการพูดคุยเรื่องของการเปลี่ยนแปลงขอบเขตของการให้บริการใหม่ โดยทั้งผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก จะต้องมีการทบทวน SLA ใหม่ จากการบันทึกเหตุการณ์ที่เกิดขึ้นเป็นประจำ (เช่น เหตุการณ์ที่เกิดขึ้นในแต่ละ ปี หรือเหตุการณ์ที่เกิดขึ้นบ่อยๆ)

4.2.4 กระบวนการสร้างประสิทธิภาพการดำเนินการด้านความมั่นคงปลอดภัย

ด้วยโครงสร้าง ของระบบบริหารที่ต้องมีการวางแผน การดำเนินการ ตรวจสอบ และการพัฒนา หรือที่เราเรียกว่า PDCA (Plan คือการวางแผน Do คือการปฏิบัติ Check คือการตรวจสอบ Act คือกำหนดมาตรฐาน) นั้นจะทำให้การจัดการเรื่องความมั่นคงของสารสนเทศ มีประสิทธิผลเต็มที่ และทำให้องค์กรมั่นใจที่จะให้ระบบสารสนเทศมาเป็นเครื่องมือในการดำเนินธุรกิจ รวมถึงเพิ่มโอกาสทางธุรกิจจากการใช้สารสนเทศมากขึ้น

1. กำหนดระบบบริหารจัดการความมั่นคงปลอดภัย โดยองค์กรควรกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยและกำหนดนโยบายความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี นอกจากนี้ ยังต้องกำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร ระบบความเสี่ยง วิเคราะห์และประเมินความเสี่ยง ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงการดำเนินการที่เป็นไปได้ เลือกวัตถุประสงค์และมาตรการทางด้านความปลอดภัยเพื่อจัดการกับความเสี่ยง ขออนุมัติและความเห็นชอบสำหรับควา มเสี่ยงที่ยังหลงเหลืออยู่ในระบบบริหารจัดการความมั่นคงปลอดภัย ขอการ

อนุมัติเพื่อลงมือปฏิบัติและดำเนินการ และสุดท้ายคือ จัดทำเอกสาร SoA (Statement of Applicability) แสดงการใช้งานมาตรฐานตามที่แสดงไวในส่วนของมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางด้านอิเล็กทรอนิกส์

2. ลงมือปฏิบัติและดำเนินการระ บบบริหารจัดการความมั่นคงปลอดภัย โดยองค์กรควรจัดทำแผนการจัดการความเสี่ยง ลงมือปฏิบัติตามแผนการจัดการความเสี่ยงและตามมาตรฐานที่เลือกไว้ กำหนดวิธีการในการวัดความสัมฤทธิ์ผลของมาตรการที่เลือกมาใช้งาน จัดทำและลงมือปฏิบัติตามแผนการอบรมและสร้างความตระหนัด บริหารจัดการดำเนินงานและบริหารทรัพยากรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย รวมถึงจัดทำและลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่นๆ ซึ่งช่วยในการตรวจจับและรับมือกับเหตุการณ์ทางด้านความมั่นคงปลอดภัย

3. เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย โดยองค์กรควรลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่นๆ สำหรับการเฝ้าระวังและทบทวน ดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ วัดความสัมฤทธิ์ผลของมาตรการทางด้านความมั่นคงปลอดภัย ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้กับระดับความเสี่ยงที่เหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ ดำเนินการตรวจสอบและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย ปรับปรุงแผนทางด้านความปลอดภัยโดยนำผลของการเฝ้าระวังและทบทวนกิจกรรมต่างๆ มาพิจารณาร่วมด้วย และบันทึกการดำเนินการซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

4. บำรุงรักษาและปรับปรุงระบบบริหารจัดการด้านความมั่นคงปลอดภัย โดยองค์กรควรปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้ รวมถึงการใช้ มาตรการเชิงแก้ไขป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและองค์กรอื่น แจ้งการปรับปรุงและดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้อง และตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

โดยกรณีศึกษาใช้แ นวทางของ Balance ScoreCard เป็นเครื่องมือในการตรวจสอบเพื่อใช้ในการปรับปรุงพัฒนาให้ดีขึ้น

BSC-Balance ScoreCard ด้านความปลอดภัยของผู้ให้บริการจัดจ้างภายนอก ในการประเมินการจัดจ้างภายนอก ผู้ให้บริการจัดจ้างภายนอกในกรณีศึกษาให้ความสำคัญกับการทำ BSC เพื่อเป็นการเพิ่มประสิทธิภาพในการให้บริการการจัดจ้างภายนอก ดังนั้นจึงมีการนำเสนอ

แนวทางการทำ BSC ที่อ้างอิงมาเอกสารเผยแพร่ของสถาบัน ISACA ในการวัดประสิทธิภาพการจัดจ้างภายนอกโดยใช้ BSC [19]

BSC เป็นเครื่องมือที่ช่วยนักบริหารเพื่อกำหนดเป้าหมายยุทธศาสตร์ และแนวมางไปสู่ การบรรลุวัตถุประสงค์ตลอดจนติดตามตรวจสอบ ควบคุมกิจกรรมต่าง ๆ เพื่อให้สัมฤทธิ์ผล โดยมีการกำหนดมุมมอง 4 ด้านที่จะแสดงให้เห็นความสำคัญต่าง ๆ ขององค์กรดังนี้

1. มุมมองทางด้านการเงิน
2. มุมมองทางด้านลูกค้า
3. มุมมองทางด้านกระบวนการภายใน
4. มุมมองทางด้านนวัตกรรมและการเรียนรู้

ซึ่งแต่ละมุมมองมีรายละเอียดดังนี้

— มุมมองทางด้านการเงิน ของการให้บริการจัดจ้างภายนอกเพื่อให้บริการโปรแกรมเว็บคอมพิวเตอร์จะต้องสะท้อนให้เห็นถึงการสนับสนุนกับการบริการผู้ใช้ซึ่งเป็นลูกค้า โดยต้นทุนของระบบ การแสดงส่วนของต้นทุนทางด้าน IT ของการให้บริการจัดจ้างภายนอกโดยทั่วไปจะมีต้นทุนบางส่วนที่ถูกซ่อนไว้ จึงเป็นเหตุให้มีการนำวิธีการ total cost of ownership มาใช้เพื่อประเมินค่าใช้จ่ายขององค์กร ดังนั้นจึงจำเป็นที่จะต้องแบ่งแยกระหว่างต้นทุนโดยตรงและต้นทุนโดยอ้อม ต้นทุนโดยตรงคืองบประมาณที่ใช้ สำหรับฮาร์ดแวร์และซอฟต์แวร์ การปฏิบัติ และการจัดการ จาก ชนิดของต้นทุนโดยตรงที่มีการพิจารณาสำหรับระบบคลังข้อมูลได้แก่

- ฮาร์ดแวร์และซอฟต์แวร์ต่างๆ
- เจ้าหน้าที่ทางด้าน IT และ การบริการ
- การสนับสนุนและการบำรุงรักษา

ในทางตรงกันข้าม ต้นทุนทางอ้อมคือต้นทุนที่ไม่ใช่ งบประมาณซึ่งเป็นสาเหตุจากระบบปฏิบัติการหรือการใช้ที่ปราศจากประสิทธิภาพ ต้นทุนทางอ้อมอาจจะมีสาเหตุมาจากขาดการวางแผนเมื่อเกิดปัญหาการหยุดการให้บริการ ซึ่งมีผลต่อการจัดการการตัดสินใจ นอกจากนั้นส่วนสนับสนุนอื่นๆ ของต้นทุนทางอ้อมคือการปฏิบัติของผู้ใช้ปราศจากประ สิทธิภาพการดำเนินการให้มุมมองทางด้านการเงินสำเร็จจำเป็นต้องมีการรวมทุกองค์ประกอบของเค้าโครงเกี่ยวกับการขายและต้นทุนในมุมมองทางด้านการเงิน

— มุมมองทางด้านลูกค้า การนิยามมุมมองทางด้านลูกค้าของการบริการจัดจ้างภายนอกที่เกี่ยวข้องกับการ บริการ โดยปกติวัตถุประสงค์ ทางยุทธศาสตร์ สำหรับในส่วนนี้จะจัดเตรียมสารสนเทศเกี่ยวกับการจัดการ ในการประเมินค่าความสำเร็จของวัตถุประสงค์นี้ ตัวชี้วัด

ที่เป็นไปได้สำหรับวัตถุประสงค์นี้คือร้อยละของการตัดสินใจที่ครอบคลุมธุรกิจหรือร้อยละของตำแหน่งเกี่ยวกับการสนับสนุนการจัดการผลิตภัณฑ์สารสนเทศที่เกี่ยวกับการบริการให้กับผู้ว่าจ้าง นอกจากนี้ร้อยละของระบบปฏิบัติการ ที่ให้บริการอาจจะเป็นตัวชี้วัดที่สัมพันธ์กันได้ ความจำเป็นในการวัดค่าความพอใจของผู้ใช้กับการบริการระบบสารสนเทศ ซึ่งสามารถถูกประเมินค่าโดยผ่านทางการสำรวจซึ่งเป็นดัชนีในการคำนวณค่าความพึงพอใจของลูกค้าและข้อมูลเกี่ยวกับพฤติกรรมผลของมุมมองด้านลูกค้า ดังมุมมองทางด้านลูกค้าเกี่ยวกับความมั่นคงปลอดภัยตัวอย่างเช่น

- จำนวนของการหยุดการให้บริการกับผู้ว่าจ้างเนื่องจากเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัย
- จำนวนของโครงการที่ต้องหยุด หรือที่ความล่ าช้าในการดำเนินการเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัย

— มุมมองทางด้านกระบวนการภายใน เน้นไปในสภาวะภายในองค์กรสำหรับสนับสนุนความพึงพอใจของลูกค้าด้วยการบริการจัดจ้างภายนอก โดยมุมมองทางด้านกระบวนการภายในจะครอบคลุมกระบวนการภายในทั้งหมด และความต้องการ ประสิทธิภาพ และผลของการดำเนินงานทางด้านความมั่นคงปลอดภัยของลูกค้า รวมทั้งข้อตกลงร่วมกันในเรื่องของกฎหมายและข้อบังคับ ดังตัวอย่างเช่น

- เวลาในการจัดการเมื่อมีผู้ใช้งานเข้ามาเพิ่ม
- จำนวนของการรายงานที่เกี่ยวกับสถานะการด้านความมั่นคงปลอดภัยที่เกิดขึ้น
- จำนวนของก ารจัดการเหตุการณ์ที่เกิดขึ้นเกี่ยวกับความมั่นคงปลอดภัยโดยไม่มีผลกระทบกับระบบโดยรวม
- ระบบความมั่นคงปลอดภัยตรงกับความต้องการของผู้ว่าจ้างรึไม่

— มุมมองทางด้านนวัตกรรมและการเรียนรู้ มุมมองนี้จะสะท้อนความยืดหยุ่นสำหรับความต้องการ ณ เวลาปัจจุบันและความต้องการในอนา คต โดยความยืดหยุ่นทางเทคนิคนี้มีสาเหตุมาจากรูปแบบของซอฟต์แวร์และฮาร์ดแวร์ที่ถูกนำมาใช้สำหรับการพัฒนาระบบสารสนเทศและระบบความมั่นคงปลอดภัย

ความเป็นองค์กรที่ยืดหยุ่นได้ของการบริการจัดจ้างภายนอกจะถูกควบคุมโดยคุณสมบัติของพนักงาน โดยเฉพาะเจ้าหน้าที่ทางเทคนิคที่ ให้การบริการ จะต้องมีความรู้ทางธุรกิจอย่างเพียงพอเพื่อที่จะเข้าใจความต้องการเกี่ยวกับการบริการของผู้ว่าจ้าง และสามารถติดต่อสื่อสารกับผู้ว่าจ้างได้เครื่องมือในการวัดคุณภาพของพนักงานได้แก่ประสบการณ์จากโครงงานซึ่งมีลักษณะ

ใกล้เคียง นอกจากนี้ เจ้าหน้าที่ทางเทค นิคที่ให้การบริการจะต้องก้าวไปพร้อมกับการพัฒนาทาง เทคนิค ซึ่งสิ่งที่กล่าวนี้สามารถวัดได้จากจำนวนวันของการฝึกอบรมต่อพนักงาน สำหรับในส่วน ของผู้ใช้ก็จะต้องมีการฝึกอบรมที่พอเพียงเช่นกัน โดยวัดได้จากจำน วนวันของการฝึกอบรมต่อผู้ใช้ ดังตัวอย่างเช่น

- เวลาในการทำให้โครงการบรรลุผลและตรงกับความต้องการของผู้ว่าจ้าง
- ความเร็วในการตรวจพบการคุกคามรูปแบบใหม่ ๆ

4.2.5 **การบริหารจัดการระบบสารสนเทศตามพระราชบัญญัติคอมพิวเตอร์** 2550

ซึ่งว่าด้วยเรื่องของการกระทำความผิด ที่เกี่ยวกับคอมพิวเตอร์ เช่น ถ้าทำผิดในกรณีทำให้ เสียหาย ทำลาย แก้ไ ขเปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ ของผู้อื่นโดยมิชอบต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้ง ปรับ รวมถึงข้อพระราชบัญญัติในมาตราที่ ๒๖ ที่บอกไว้ว่า ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจร ทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณี จำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้า สิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ดังนั้นผู้ให้บริการจัดจ้าง ภายนอกที่ให้บริการข้อมูลคอมพิวเตอร์ผ่าน โปรแกรมประยุกต์ มี หน้าที่เก็บรักษาข้อมูลการจราจรทางคอมพิวเตอร์ของผู้ที่มาใช้บริการจากผู้ให้บริการ จัดจ้าง ภายนอกในรูปแบบต่างๆ ที่เรียกว่า “ข้อมูลจราจรทางคอมพิวเตอร์”

โดยที่ข้อมูลจราจรทางคอมพิวเตอร์นั้นหมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารข องระบบคอมพิวเตอร์ ซึ่งแสดงถึงแห ล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ซึ่ง ข้อมูลที่เกี่ยวข้องกับการติดต่อสื่ อสารของระบบคอมพิวเตอร์โดยตามปกติของการติดตั้งระบบ เครือข่ายคอมพิวเตอร์ในองค์กรจ ากเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ ต่างๆ ทำหน้าที่ควบคุมและ ให้บริการการของเซิร์ฟเวอร์ และการใช้งานอินเตอร์เนต

ตามกำหนดของ พรบ . คอมพิวเตอร์ 2550 ผู้ให้บริการจัดจ้างภายนอก ต้องทำการเก็บ Log ไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น

การเก็บ Log หลัก ที่จำเป็นขององค์กรสามารถจำแนกการเก็บ Log ออกเป็น 4 ข้อใหญ่ เพื่อเป็นตัวอย่างสำหรับการจัดทำการเก็บ Log สามารถจำแนกออกได้ดังนี้

- การใช้งานอินเทอร์เน็ตขอ งพนักงานภายในองค์กรหรือผู้ใช้ทุกคนที่อยู่ภา ยใต้ระบบเครือข่าย ที่มีการออก ไปสู่การใช้งานอินเทอร์เน็ตภายนอก โดย Log ที่เก็บจะต้องระบุ URL ที่เข้าใช้ ตามด้วยเวลาที่เข้าใช้ เป็นต้น
- Log ของ Web Server ที่เก็บเนื้อหา (content) ข้อมูล โปรแกรม ที่ให้บริการสำหรับ ผู้ว่าจ้าง
- Log ของการเข้าถึงระบบเครือข่ายในองค์กร หรือการ Log-in เข้าระบบ ว่าผู้ใช้คนนั้นเข้ามาในระบบเวลาใด เพื่อจะนำ Log ที่ได้ไปเปรียบเทียบกับ Log เว็บเซิร์ฟเวอร์
- Log ของการรับส่ง Email ทั้งหมด ไม่ว่าจะเป็น Email Address จากผู้ใดถึงใคร เวลาในการรับส่ง รวมไปถึงเนื้อหาในการรับส่งของ Email

การดำเนินการจัดการเกี่ยวกับระบบสารสนเทศที่เกี่ยวกับพระราชบัญญัติ คอมพิวเตอร์ 2550 จะมีหลักขั้นตอนดำเนินงานเพื่อให้เป็นผลสำเร็จได้ดังนี้

- การวางแผนการดำเนินงาน โดยอันดับแรกของการวางแผนการดำเนินงานคือการกำหนดวัตถุประสงค์ของก ารทำ พรบ. คอมพิวเตอร์ 2550 เนื่องจากการวางระบบสารสนเทศ ล้วนส่งผลกระทบถึงภาพรวมของระบบทั้งหมด ดังนั้นการวางแผนควรกำหนดขอบเขตให้ชัดเจนว่าวัตถุประสงค์ของโครงการนี้มีขอบเขตแค่ไหน ต้องการแค่ให้เป็นไป ตามพรบ. คอมพิวเตอร์ 2550 ซึ่งประเด็นลักษณะนี้ผู้บริหารองค์กรแล ะผู้บริหารระบบต้องประชุมร่วมกันเพื่อกำหนดแนวทางดังกล่าว และนำแนวทางนั้นไปกำหนดเรื่องของระยะเวลา งบประมาณ (money) ผู้รับผิดชอบโครงการ (man) เพื่อนำไปหาวิธีในการดำเนินงานต่อไป (method)
- การดำเนินงานตามแผน ขั้นตอนนี้ใช้เทคนิคของการบริหารโครงการต่างๆ เข้ามาช่ว ย เช่นมีการทำ Work Breakdown Structure ของงานออกมาเป็นส่วนๆ ตามประเภทของเนื้องานเช่น ส่วนของฮาร์ดแวร์ ประเภท ไฟวอลล์หรือ Proxy ที่จะนำมาเก็บ Log หรือถ้าเป็นส่วนซอ ฟท์แวร์ก็ลงรายละเอียดเช่น การติดตั้ง ระบบปฏิบัติการ การติดตั้งโปรแกรม และที่สำคัญคือส่วนของนโยบา ยองค์กรที่จะทำให้องค์กร เป็นไปตามข้อกำหนดของพรบ. คอมพิวเตอร์ 2550
- การประเมินแผน และการตรวจสอบ โดยในส่วนนี้ เกี่ยวกับการตรวจทานโครงการ มีการตรวจสอบความคืบหน้า และดูผลสำเร็จของงานเมื่อเทียบกับแผนงานที่วางไว้ หรือตั้งคณะทำงานเพื่อตรวจสอบสำหรับองค์กร

- การนำผลมา พัฒนาแผน โดยขั้นตอนนี้ก็คือการนำผลการประเมินมาวิเคราะห์ว่า มีโครงสร้างหรือขั้นตอนการปฏิบัติงานใดที่ควรปรับปรุงหรือพัฒนาสิ่งที่ดีอยู่แล้วให้ดียิ่งขึ้นไปอีก ถ้ามีโครงการในลักษณะนี้เกิดขึ้นอีก ต้องควรปฏิบัติอย่างไร

4.2.6 แนวทางความปลอดภัย ให้บริการด้านการเงิน ด้วยวิธีอิเล็กทรอนิกส์ ตามระเบียบของธนาคารแห่งประเทศไทย พ.ศ 2544

เมื่อผู้ให้บริการจัดจ้างภายนอกให้บริการกับผู้ว่าจ้างที่เป็นสถาบันการเงิน นั้นผู้ให้บริการจัดจ้างต้องคำนึงถึงข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยของการให้บริการอิเล็คทรอนิกส์ โดยอ้างอิงกับธนาคารแ ห่งประเทศไทย เพื่อให้ครอบคลุมในประเด็นความมั่นคงปลอดภัยที่สอดคล้องกับผู ว่าจ้างที่เป็นสถาบันการเงิน ดังกรณีศึกษา ซึ่งมีรายละเอียดดังนี้

ธนาคารแห่งประเทศไทยได้นำระบบการสื่อสารด้วยวิธีอิเล็กทรอนิกส์ มาใช้ในการให้บริการแก่สถาบันการเงิน ซึ่งมีอยู่แล้วหรือจะจัดให้มีขึ้นในอนาคต ในการนี้ หากมีกรณีที่จะต้องทำธุรกรรม ระหว่างกันขึ้นจะก่อให้เกิดความผูกพันกันทางสัญญาก็จำเป็นต้องจัดให้มีระบบและกระบวนการเพื่อความปลอดภัยในการรับและส่งข้อมูลระหว่างกัน โดยผู้ให้บริการจัดจ้างภายนอกที่ให้บริการกับสถาบันการเงิน ต้องคำนึงถึงคว ามปลอดภัยที่อ้างอิงกับระเบียบของธนาคารแห่งประเทศไทย ซึ่งมีดังนี้

1. นิยาม

“ธปท.” หมายถึง ธนาคารแห่งประเทศไทย

“ผู้ใช้บริการ” หมายถึง สถาบันการเงินหรือนิติบุคคลอื่นใดที่ได้รับอนุญาตจาก ธปท. ให้ใช้บริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์

“บริการด้านการเงิน ด้วยวิธีอิเล็กทรอนิกส์ ” หมายถึง ระบบบริการสื่อสารข้อความด้วยวิธีอิเล็กทรอนิกส์ ในการทำธุรกรรมด้านการเงินระหว่าง ธปท. กับผู้ใช้บริการ ตามที่ ธปท. กำหนด

“บริการด้านการเงิน” หมายถึง บริการด้านระบบการชำระเงิน บริการด้านเงินฝากและตราสารหนี้ บริการด้านตลาดการเงิน

“คอมพิวเตอร์แม่ข่าย” หมายถึง ระบบคอมพิวเตอร์ของ ธปท.

“คอมพิวเตอร์ลูกข่าย” หมายถึง ระบบคอมพิวเตอร์ของผู้ใช้บริการ

“ชุดคำสั่งของ ธปท.” หมายถึง ชุดคำสั่งสำหรับคอมพิวเตอร์ลูกข่ายที่ ธปท. จัดหาให้ผู้ใช้บริการ

“กระบวนการเพื่อความปลอดภัยในการรับและส่งข้อมู ลระหว่างกัน” หมายถึง กระบวนการในการบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ที่ ธปท.จัดให้มีขึ้นเพื่อ

- ยืนยันว่าข้อความที่ผู้ใช้บริการหรือ ธปท. ได้ส่งผ่านบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์เป็นข้อความของผู้ใช้บริการหรือของ ธปท. จริง อีกทั้งสามารถทำการพิสูจน์ตัวตนและยืนยันว่าผู้ปฏิบัติงานในบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์เป็นบุคคลที่ได้รับสิทธิในการปฏิบัติงานจริง

- ยืนยันว่าข้อความที่ ผู้ใช้บริการหรือ ธปท. ได้รับผ่านบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์เป็นข้อความเดียวกับที่ผู้ใช้บริการหรือ ธปท.ได้ส่งจริง และป้องกันมิให้บุคคลอื่นที่ไม่เกี่ยวข้องล่วงรู้ข้อมูลที่แท้จริงในการรับและส่งข้อมูลระหว่างคอมพิวเตอร์แม่ข่ายกับคอมพิวเตอร์ลูกข่าย

- กำหนดเวลา ณ จุดใดจุดหนึ่ง ซึ่งทั้ง ธปท. และผู้ใช้บริการไม่สามารถยกเลิก เพิกถอนข้อความที่ตนส่งไปได้

- มีระบบการบันทึกหลักฐาน (log file) เกี่ยวกับข้อมูลหรือข้อความที่รับส่งในแต่ละบริการ ใช้ตรวจสอบความครบถ้วนของจำนวนรายการที่ส่งผ่านบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ได้

“ผู้มีอำนาจลงนาม” หมายถึงบุคคลที่ได้รับมอบหมายจากผู้ใช้บริการ ที่จะเป็นผู้กำหนดหรือเพิกถอนตัวบุคคลที่จะ ทำหน้าที่เป็น ผู้รับรอง (Certifier) ในบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์

“ผู้รับรอง” หมายถึง บุคคลที่ได้รับมอบหมายจากผู้มีอำนาจลงนามให้เป็นผู้กำหนดหรือเพิกถอนผู้ปฏิบัติงาน (Officer) ในบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์

“ผู้ปฏิบัติงาน” หมายถึง บุคคลที่ได้รับมอบหมายจาก ผู้รับรองให้เป็นผู้ปฏิบัติงานในบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์

“ มาตรการรักษาความปลอดภัย ” หมายถึง มาตรการในการป้องกันมิให้บุคคลซึ่งไม่ได้รับมอบหมายเข้าใช้คอมพิวเตอร์ลูกข่าย

“คู่มือการใช้งาน” หมายถึง คู่มือการใช้งานบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ที่ ธปท. จัดหาให้ผู้ใช้บริการ

2. สิทธิ์และหน้าที่ของผู้ใช้บริการ

— ผู้ใช้บริการรับรู้ เข้าใจและยอมรับในประสิทธิภาพ ขอบเขตความสามารถและข้อจำกัดของกระบวนการเพื่อความปลอดภัยในการรับส่งข้อมูลหรือข้อความระหว่างกัน และยอมรับว่าบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์มีมาตรการที่รัดกุมเพียงพอสำหรับป้องกันความผิดพลาดและการทุจริตต่างๆ แล้ว ธปท.

— ผู้ใช้บริการต้องจัดหาคอมพิวเตอร์ลูกข่าย อุปกรณ์อื่น ๆ และชุดคำสั่งตามที่ ธปท. กำหนดสงวนสิทธิ์ ที่จะปรับปรุงหรือแก้ไขเพิ่มเติมกระบวนการเพื่อความปลอ ดภัยในบริการด้านการเงินตามที่เห็นสมควร

— ผู้ใช้บริการต้องดำเนินการเกี่ยวกับคอมพิวเตอร์ลูกข่ายซึ่งใช้กับระบบบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ ดังต่อไปนี้

- เชื่อมโยงคอมพิวเตอร์ลูกข่ายกับคอมพิวเตอร์แม่ข่ายเพื่อการใช้บริการด้านการเงิน
- ดูแลรักษาคอมพิวเตอร์ลูกข่ายให้อยู่ในสภาพใช้งานได้ดีตลอดเวลา
- จัดให้คอมพิวเตอร์ลูกข่ายมีระบบป้องกันไวรัสคอมพิวเตอร์ที่มีประสิทธิภาพ

ทั้งนี้ ธปท. อาจกำหนดมาตรฐานตามที่เห็นสมควรก็ได้

— ผู้ใช้บริการต้องปฏิบัติตามพิธีปฏิบัติ คู่มือการใช้งานและแนวทางการปฏิบัติงานที่ ธปท. กำหนด ในกรณีที่พิธีปฏิบัติ คู่มือการใช้งานและแนวทางการปฏิบัติงานขัดหรือแย้งกับระเบียบนี้ให้ถือว่าระเบียบนี้เป็นใหญ่และให้ปฏิบัติตามระเบียบนี้

— ผู้ใช้บริการต้องจัดให้มีแผนสำรองตามมาตรฐานที่ยอมรับโดยทั่วไปเมื่อมีเหตุที่ทำให้ไม่สามารถใช้บริการด้านการเงินตามปกติได้

— ผู้ใช้บริการต้องจัดให้มีมาตรการรักษาความปลอดภัยและระบบควบคุมภายในตามมาตรฐานที่ยอมรับโดยทั่วไป

— ผู้ใช้บริการต้องรักษาไว้เป็นความลับซึ่งกระบวนการเพื่อความปลอดภัยในการใช้บริการด้านการเงิน ชุดคำสั่งของธนาคาร คู่มือการใช้งาน เว้นแต่เป็นการเปิดเผยเท่าที่จำเป็นเพื่อประโยชน์ในการปฏิบัติงาน ผู้ใช้บริการต้องเก็บรักษาข้อมูลอันเกี่ยวเนื่องด้วยกระบวนการเพื่อความปลอดภัยในการใช้บริการด้านการเงิน ชุดคำสั่งของธนาคาร และคู่มือการใช้งานมิให้สูญหาย ในกรณีที่มีการเปิดเผยหรือสูญหาย ผู้ใช้บริการต้องแจ้งให้ ธปท. ทราบโดยพลัน

— ผู้ใช้บริการอา จขอให้ ธปท. ระงับการให้บริการแก่ตนเป็นการชั่วคราวภายใต้หลักเกณฑ์วิธีการและเงื่อนไขที่ ธปท.กำหนด แต่ต้องรับผิดชอบในข้อความที่ได้ส่งให้กับ ธปท. และ ธปท. ได้รับก่อนที่ธปท. จะระงับการให้บริการ

— ผู้ใช้บริการอาจขอชุดคำสั่งของ ธปท. คู่มือการใช้งานชุดใหม่ได้ตามหลัก เกณฑ์วิธีการและเงื่อนไขที่ ธปท. กำหนด

— ในกรณีที่คอมพิวเตอร์แม่ข่ายขัดข้อง คอมพิวเตอร์ลูกข่ายขัดข้อง หรือการสื่อสารระหว่างคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่ายขัดข้องไม่ว่า ธปท. จะแจ้งให้ผู้ใช้บริการทราบ

หรือผู้ใช้บริการแจ้งให้ธปท . ทราบ แล้วแต่กรณี ให้ผู้ใช้บริการปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดในระเบียบธนาคารแห่งประเทศไทยว่าด้วยบริการประเภทนั้น ๆ

— ห้ามมิให้ผู้ใช้บริการแก้ไขชุดคำสั่งของ ธปท.

— ผู้ใช้บริการต้องยินยอมและอำนวยความสะดวกแก่เจ้าหน้าที่ของ ธปท. ในการตรวจสอบคอมพิวเตอร์ลูกข่าย มาตรการรักษาความปลอดภัย ระบบการควบคุมภายใน เอกสารหลักฐานที่เกี่ยวข้อง และอื่นๆ ตามที่ ธปท. เห็นสมควร

— ผู้ใช้บริการจะต้องชี้แจงหรือมอบเอกสารหรือหลักฐานอื่นใดให้แก่ ธปท. เมื่อ ธปท. ขอความร่วมมือ

— ผู้ใช้บริการต้องเก็บรักษาเอกสารหลักฐานตามที่ ธปท. กำหนด

3. การเข้าใช้ระบบบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์

— ในการขอใช้ระบบบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ ผู้ใช้บริการต้องปฏิบัติคือ

● ให้ผู้ใช้บริการทำหนังสือแต่งตั้งผู้มีอำนาจลงนาม ตามแบบที่ ธปท. กำหนด เพื่อทำหน้าที่กำหนดหรือเพิกถอนบุคคลที่จะทำหน้าที่เป็นผู้รับรองระบ บบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์

● ให้ผู้มีอำนาจลงนามทำหนังสือแต่งตั้งผู้รับรองตามแบบที่ ธปท. กำหนด

● ให้ผู้รับรองทำหนังสือ แต่งตั้งผู้ปฏิบัติงานตามแบบที่ ธปท. กำหนดการเพิกถอนตัวบุคคลที่ได้รับแต่งตั้งตามข้อข้างต้นให้สถาบันการเงินทำหนังสือ ตามแบบที่ ธปท. กำหนด

— ธุรกรรมใดๆ ที่เกี่ยวข้องในระบบบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ที่เกิดจากการกระทำของผู้มีอำนาจลงนาม ผู้รับรอง หรือผู้ปฏิบัติงานให้ถือเป็นการกระทำของ การใช้บริการซึ่งมีผลบังคับตามระเบียบนี้ทั้งสิ้น

4. ระบบการให้ข้อมูลข่าวสารทางอิเล็กทรอนิกส์

— ธปท. อาจให้ข้อมูลข่าวสาร เพื่อเป็นการเผยแพร่ข้อมูลข่าวสารของบริการที่ ธปท. จัดให้มีขึ้นในระบบบริการด้านการเงินให้แก่ผู้ใช้บริการทางอิเล็กทรอนิกส์

— ธปท. ได้มีบริการการติดต่อสื่อสารทางจดหมายอิเล็กทรอนิกส์ ระหว่าง ธปท. กับผู้ใช้บริการ เพื่อใช้ในการติดต่อประสานง านในกรณีต่าง ๆ เพิ่มเติม โดยบริการดังกล่าวถือเป็นบริการเสริมที่ผู้ใช้ระบบจะสามารถเลือกใช้หรือไม่ก็ได้

— ในการให้ข้อมูลข่าวสารหรือการติดต่อสื่อสารข้างต้น ผู้ใช้บริการควรส่งเฉพาะข้อความที่เกี่ยวกับการดำเนินธุรกิจตามปกติเท่านั้นและผู้ใช้บริการต้องรับผิดชอบในข้อ ความที่ตน

ส่งด้วย ทั้งนี้ ผู้ใช้บริการจะส่งข้อความที่มีลักษณะเป็นรหัสลับหรือข้อความที่ขัดต่อกฎหมายหรือความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนไม่ได้

— ในการที่ผู้ใช้บริการขอให้ ธปท. ประกาศข้อความแก่ผู้ใช้บริการทั้งหลายของบริการด้านการเงิน ผู้ใช้บริการต้องปฏิบัติตามวิธีการที่ ธปท. กำหนด และต้องรับผิดในความเสียหายที่อาจเกิดจากข้อความที่ขอให้ประกาศนั้น ทั้งนี้ ธปท. สงวนสิทธิที่จะออกประกาศในเวลาใดตามที่เห็นสมควร หรือไม่ดำเนินการให้ถ้าเห็นว่าไม่เหมาะสมก็ได้

5. การระงับไปแห่งการใช้บริการ

— ธปท. อาจระงับการให้บริการด้านการเงิน บางบริการหรือทุกบริการ ในเวลาใดก็ได้ตามแต่ ธปท. เห็นสมควร โดย ธปท. จะแจ้งให้ผู้ใช้บริการทราบล่วงหน้าเป็นเวลาพอสมควร

— ในกรณีที่การใช้บริการบางประเภทหรือทุกประเภท เป็นอันต้องระงับไปผู้ใช้บริการต้อง

- มอบชุดคำสั่งของ ธปท. คู่มือการใช้งาน และเอกสารอื่นๆ ตามที่ ธปท. กำหนดคืนให้แก่ ธปท.
- ทำลายชุดคำสั่งของ ธปท. ที่ได้บรรจุลงในคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการ
- รักษาความลับอันเกี่ยวเนื่องกับการใช้บริการ แม้ว่าการใช้บริการจะระงับไปแล้วก็ตาม

บทที่ 5

ผลการประเมินแนวทางการจัดจ้างภายนอก

การวิจัยเชิ งคุณภาพเกี่ยวกับโครงสร้างของรูปแบบความมั่นคงปลอดภัยการจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้าง โดยใช้กรอบโครงสร้างความมั่นคงปลอดภัยธรรมมาภิบาล ดังนี้

1. บทวิเคราะห์จากการสัมภาษณ์กลุ่มงานวิจัยของแนวทางรูปแบบความมั่นคงปลอดภัยการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง
2. ประเมินการลดทรัพยากร และค่าใช้จ่ายของผู้ให้บริการจัดจ้าง
3. การประเมินแนวทางของ รูปแบบความมั่นคงปลอดภัยสำหรับจัดจ้าง การ บริการภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง
4. การประเมินผลประโยชน์ของผู้ให้บริการจัดจ้างได้รับจากการ จัดจ้างภายนอก โดยอยู่นอกที่ทำการของผู้ว่าจ้าง

5.1 บทวิเคราะห์จากการสัมภาษณ์กลุ่มงานวิจัยของแนวทางรูปแบบความมั่นคงปลอดภัยการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง

จากการสัมภาษณ์กลุ่มบุคคลที่เกี่ยวข้องในกรณีศึกษา ได้มีการสรุปประเด็น ที่เกี่ยวข้องออกเป็น 5 ข้อซึ่งมีรายละเอียดดังนี้

1. แนวทางความมั่นคงปลอดภัยการจัดจ้างภายนอก ครอบคลุมความต้องการด้านความปลอดภัยของผู้ว่าจ้างได้ ทำให้มีความน่าเชื่อถือ แต่ปัจจัยที่ผู้ว่าจ้างนำมาใช้ประกอบการตัดสินใจเลือกผู้ให้บริการจัดจ้าง โดยองค์ประกอบหลายด้าน ซึ่งมีรายละเอียดดังนี้

- ประสบการณ์การทำงานของบริษัทที่ให้บริการจัดจ้างกับรูปแบบธุรกิจของผู้ว่าจ้าง
- นโยบายการดำเนินงานของบริษัทที่ให้บริการจัดจ้างภายนอก
- การปกป้องความลับของข้อมูลลูกค้า
- การเปิดเผยข้อมูลทั่วไปของบริษัทที่ให้บริการจัดจ้างภายนอก เพื่อสามารถตรวจสอบความมั่นคงและความน่าเชื่อถือ
- ความพร้อมและความทันสมัยของอุปกรณ์ด้านเทคโนโลยีสารสนเทศ
- ใบรับรองประสิทธิภาพการทำงานหรือประวัติการทำงาน
- บริษัทที่เป็นผู้รับช่วงต่อในการให้บริการจัดจ้างภายนอก

2. การประเมินรูปแบบแนวทางการจัดการความมั่นคงปลอดภัยของการจัดจ้างภายนอก ที่อ้างอิงจากเอกสารเผยแพร่ของสถาบัน NCTT นั้นมีรูปแบบความมั่นคงปลอดภัย ที่ทำให้ทราบแนวทางความมั่นคงปลอดภัยในการจัดจ้างภายนอก แต่ไม่ครอบคลุมตามความต้องการของผู้ว่าจ้างในกรณีศึกษาได้ จำเป็นต้องมีส่วนเพิ่มเติม เพื่อครอบ คลุมประเด็นที่องค์ กรผู้ว่าจ้างให้ความสำคัญ ซึ่งต้องมีการเพิ่มในส่วนการจั ดการความมั่นคงปลอดภัยภายในองค์กรของผู้ให้บริการจัดจ้างภายนอก และการทำข้อตกลงร่วมกันของคู่สัญญาระหว่างผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก

3. รูปแบบการให้บริการจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้าง โดยมีการเชื่อ มต่อโดย ใช้เทคโนโลยี VPN สอดคล้องกับระบบความปลอดภัยขององค์กรผู้ว่าจ้างของกรณีศึกษา โดยต้องมีการคำนึงถึงการจัดการความ มั่นคงปลอดภัยกับผู้รับช่วงต่อการจัดจ้างภายนอก เพื่อให้ความน่าเชื่อถือแก่ผู้ว่าจ้าง

4. ในกรณีที่ องค์กรของกรณีศึกษาในส่วนของผู้ว่าจ้าง มีการใช้ การจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง นั้นมีการ พิจารณาความเสี่ย งที่เกิดจากผู้ให้บริการจัดจ้างภายนอก ตั้งแต่การรักษาความถูกต้องของข้อมูล ระบบป้องกันภัย ระบบสำรองฉุกเฉิน ระบบการตรวจสอบที่เป็นมาตรฐานสากล ดังนั้นผู้ให้บริการจัดจ้างภายนอก ใช้มาตรฐาน ISO/ICE 27001 ในการจัดการด้าน ความปลอดภัย เพราะสอดคล้องกับมาตรฐานของผู้ว่าจ้างในกรณีศึกษา

5. เพื่อเป็นการเสริมประสิทธิภาพด้านความมั่นคงปลอดภัยตลอดช่วงในการให้บริการของผู้ให้บริการจัดจ้างภายนอกจำเป็นต้องตรวจวัดประสิทธิภาพ โดยมีการทำ Balance ScoreCard เพราะ จะเป็นการ จัดหาแนวทางแก้ไขและปรับปรุงการดำเนินงาน ด้านความปลอดภัย โดยพิจารณาจากผลที่เกิดขึ้นของกระบวนการทำงานภายในองค์กร และผลกระทบจาก ผู้ว่าจ้างนำมาปรับปรุงสร้างกลยุทธ์ให้มีประสิทธิภาพดีและประสิทธิผลดียิ่งขึ้น เพื่อสร้างความน่าเชื่อถือให้กับผู้ว่าจ้าง

5.2 ประเมินการลดทรัพยากร และค่าใช้จ่ายของผู้ให้บริการจัดจ้าง

จากกรณีศึกษาบริษัทที่ให้บริการสนับสนุนด้านสารสนเทศให้กับสถาบันการเงิน ได้มีการจำลองเหตุการณ์ และประเมิณค่าใช้จ่ายจากตัวอย่าง โดยมีการกำหนดดังนี้

ตารางที่ 5.1 ตารางเปรียบเทียบค่าใช้จ่ายการให้บริการโปรแกรมประยุกต์โดยผู้ให้บริการจัดจ้างอยู่ที่ทำการของผู้ว่าจ้างกับผู้ให้บริการจัดจ้างอยู่นอกที่ทำการของผู้ว่าจ้าง

การจัดจ้างภายนอกอยู่ที่ทำการของผู้ว่าจ้าง			การจัดจ้างภายนอกอยู่นอกที่ทำการของผู้ว่าจ้าง		
ข้อมูลที่เกิดขึ้นจริง ผู้ให้บริการจัดจ้างภายนอกให้บริการโปรแกรมประยุกต์ทั้งหมด 4 โปรแกรม โดยแต่ละโปรแกรมใช้ 1 เซิร์ฟเวอร์ 1 ผู้ดูแลระบบ มีลักษณะการดำเนินงานต่างกัน และมีสิ่งแวดล้อมที่ต่างกันโดยมีการให้บริการจัดจ้างในการดูแลระบบอยู่ประจำแต่ละโปรแกรม			ข้อมูลจากการจำลองเหตุการณ์ (อ้างอิงจากข้อมูลที่เกิดขึ้นจริง) ผู้ให้บริการจัดจ้างภายนอกให้บริการโปรแกรมประยุกต์ทั้งหมด 4 โปรแกรม ซึ่งแต่ละโปรแกรมประยุตก์มีลักษณะการดำเนินงานต่างกัน และมีสิ่งแวดล้อมที่ต่างกันโดยมีการให้บริการจัดจ้างในการดูแลระบบอยู่ที่ทำการของผู้ให้บริการจัดจ้าง		
ค่าใช้จ่ายที่เกี่ยวข้อง	จำนวน/หน่วย	จำนวนเงิน (บาท)	ค่าใช้จ่ายที่เกี่ยวข้อง	จำนวน/หน่วย	จำนวนเงิน (บาท)
1. ค่าใช้จ่ายเกี่ยวกับฮาร์ตแวร์					
— เซิร์ฟเวอร์ หน่วยประมวลผล 1/3.0 GHz หน่วยบันทึกความจำ 4 G	4	600,000	— เซิร์ฟเวอร์ หน่วยประมวลผล 2/3.0 GHz หน่วยบันทึกความจำ 8 G	2	440,000
— ฮาร์ดดิสขนาดความจุ 320 G	4	120,000	— ฮาร์ดดิสขนาดความจุ 720 G	2	120,000
2. ค่าใช้จ่ายเกี่ยวกับเครื่อข่าย					
— เครือข่าย	0	0	— เครือข่าย MPLS(4 Mb/s)	2	75,000
3. ค่าใช้จ่ายเกี่ยวกับซอฟต์แวร์					
— ค่าลิขสิทธิ์ Windows Server	4	68,000	— ค่าลิขสิทธิ์ Windows Server	2	34,000
4. ค่าใช้จ่ายเกี่ยวกับผู้ดูแลระบบ(Windows)					
— ค่าดูแลระบบ/เดือน	4	200,000	— ค่าดูแลระบบ/เดือน	2	100,000

ตารางที่ 5.1 ตารางเปรียบเทียบค่าใช้จ่ายการให้บริการโปรแกรมประยุกต์โดยผู้ให้บริการจัดจ้างอยู่ที่ทำการของผู้ว่าจ้างกับผู้ให้บริการจัดจ้างอยู่นอกที่ทำการของผู้ว่าจ้าง

การจัดจ้างภายนอกอยู่ที่ทำการของผู้ว่าจ้าง			การจัดจ้างภายนอกอยู่นอกที่ทำการของผู้ว่าจ้าง		
5. ค่าใช้จ่ายอื่นๆ					
— ต้นทุนในการดำเนินงาน ISO/IEC 27001	-	N/A	— ต้นทุนในการดำเนินงาน ISO/IEC 27001	-	100,000
— ค่าใช้จ่ายการทำ VPN Cisco ASA 5505	-	-	— ค่าใช้จ่ายการทำ VPN Cisco ASA 5505	1	5,5000
— ค่าสถานที่ตั้งเครื่องเซิร์ฟเวอร์(รวมค่าน้ำ ค่าไฟ)/เดือน	-	-	— ค่าสถานที่ตั้งเครื่องเซิร์ฟเวอร์(รวมค่า น้ำ ค่าไฟ)/เดือน	2	5,000
— ค่าเดินทางเพื่อให้บริการกับผู้ว่าจ้าง/เดือน	4	26,400	— ค่าเดินทางเพื่อให้บริการกับผู้ว่าจ้าง/เดือน	-	-
รวม		1,014,400	รวม		929,000

จากการประเมินค่าใช้จ่ายการดำเนินงานให้บริการโปรแกรมประยุกต์ให้แก่ผู้ว่าจ้างโดยอยู่นอกที่ทำการของผู้ว่าจ้าง นั้นผู้ให้บริการจัดจ้างภายนอกส่วนมากแล้วจะมีโครงสร้างพื้นฐานอยู่บ้างแล้ว ทำให้ลดต้นทุนได้อีก ในส่วนกระบวนการดำเนินงานตามมาตรฐาน ISO/IEC 27001 นั้นเป็นการประเมินจากทรัพยากรในการดำเนินงานตามมาตรฐาน ISO/IEC27001

จากตารางที่ 5.1 เรื่องของค่าใช้จ่ายด้านคุณสมบัติฮาร์ดแวร์ในส่วนของการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้างใช้การประเมินจากการลดเซิร์ฟเวอร์ครึ่งหนึ่งและเพิ่มประสิทธิภาพให้เป็นสองเท่า ส่วนในการประเมินค่าใช้จ่ายในการดูแลระบบ วัดจากการลงเวลาจริงในงานด้านดูแลระบบของกรณีศึกษา ซึ่งมีการลงเวลาสำหรับการทำงานด้านการดูแลระบบเพียง 60% ของงานจริงต่อการดูแล 1 โปรแกรมประยุกต์ ดังนั้นในการดูแลระบบสามารถลดจำนวนคนดูแลระบบได้เมื่อมีการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง

ดังนั้นจากผลรวมการประเมินค่าใช้จ่ายในตารางที่ 5.1 จะแสดงให้เห็นว่าการที่ย้ายการจัดจ้างภายนอกออกจากที่ทำการของผู้ว่าจ้างสามารถช่วยในการลดทรัพยากร และค่าใช้จ่ายในการดำเนินการให้บริการแก่ผู้ว่าจ้าง

5.3 การประเมินแนวทางของรูปแบบความมั่นคงปลอดภัยสำหรับจัดจ้างการบริการภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง

งานวิจัยนี้ทำการประเมินผลการสังเคราะห์รูปแบบการจัดจ้างภายนอกโดยการนำเอาเครื่องมือในการตรวจสอบความมั่นคงปลอดภัยของผู้ว่าจ้างของกรณีศึกษา (ซึ่งใช้งานจริงในปัจจุบันของสถาบันการเงิน) นำมาเชื่อมโยงกับหัวข้อของแนวทางโครงสร้างความมั่นคงปลอดภัยของการจัดจ้างที่อยู่นอกที่ทำการของผู้ว่าจ้างโดยผลการประเมินได้แสดงไว้ในตารางที่ 5.2

ตารางที่ 5.2 แสดงการจับคู่ระหว่างเครื่องมือในการตรวจสอบความมั่นคงปลอดภัยของผู้ว่าจ้างกับแนวทางโครงสร้างความมั่นคงปลอดภัยของการจัดจ้างที่อยู่นอกที่ทำการของผู้ว่าจ้าง

หัวข้อการตรวจสอบความปลอดภัยของผู้ว่าจ้าง			หัวข้ออ้างอิงกับแนวทางโครงสร้างความมั่นคงปลอดภัยของการจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้าง
1	การควบคุมความปลอดภัยทางกายภาพ		ข้อที่ 3 ในหัวข้อ 4.2.2.2
2	การควบคุมการเข้าถึงข้อมูล	2.1 การพิสูจน์ และการรับรองผู้ใช้งาน	ข้อที่ 5 ในหัวข้อ 4.2.2.2
		2.2 การกำหนดและการป้องกันทรัพยากร	ข้อที่ 5 ในหัวข้อ 4.2.2.2
		2.3 การจัดการผู้ดูแลระบบและความปลอดภัย	ข้อที่ 5 ในหัวข้อ 4.2.2.2
		2.4 ระบบบันทึกการพยายามการเข้าใช้ระบบ	ข้อที่ 7 ในหัวข้อ 4.2.1

ตารางที่ 5.2 (ต่อ) แสดงการจับคู่ระหว่างเครื่องมือในการตรวจสอบความมั่นคงปลอดภัยของผู้ว่าจ้างกับแนวทางโครงสร้างความมั่นคงปลอดภัยของการจัดจ้างที่อยู่นอกที่ทำการของผู้ว่าจ้าง

หัวข้อการตรวจสอบความปลอดภัยของผู้ว่าจ้าง			หัวข้ออ้างอิงกับแนวทางโครงสร้างความมั่นคงปลอดภัยของการจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้าง
		2.5 การรายงานการฝ่าฝืนเพื่อเข้าสู่ระบบ	ข้อที่ 7 ในหัวข้อ 4.2.1
3	การตรวจสอบสถานะของความปลอดภัย	3.1 กระบวนการการตรวจสอบระบบความปลอดภัยของระบบ	ข้อที่ 4 ในหัวข้อ 4.2.2.2
		3.2 มีการตรวจทานพฤติกรรมของระบบ	ข้อที่ 4 ในหัวข้อ 4.2.2.2
		3.3มีการกำหนดหน้าที่ของผู้รับผิดชอบด้านความปลอดภัยของทั้งสองฝ่าย	ข้อที่ 1 ในหัวข้อ 4.2.1
		3.4 รับรองการตรวจสอบจากหน่วยงานที่มีความน่าเชื่อถือ	ข้อที่ 4 ในหัวข้อ 4.2.2.2
4	การจัดการเหตุการณ์ด้านความปลอดภัย		ข้อที่ 7 ในหัวข้อ 4.2.1
5	กระบวนการช่วยเหลือด้านความถูกต้อง และมั่นคงปลอดภัย	5.1 มีการจัดลำดับความรุนแรงของระบบความปลอดภัย	-
		5.2 การกำหนดเวลาในการแจ้งข้อมูลเกี่ยวกับความปลอดภัย	-
		5.3 การกำหนดเวลาในการจัดเตรียมด้านความปลอดภัย	-

ตารางที่ 5.2 (ต่อ) แสดงการจับคู่ระหว่างเครื่องมือในการตรวจสอบความมั่นคงปลอดภัยของผู้ว่าจ้างกับแนวทางโครงสร้างความมั่นคงปลอดภัยของการจัดจ้างที่อยู่นอกที่ทำการของผู้ว่าจ้าง

หัวข้อการตรวจสอบความปลอดภัยของผู้ว่าจ้าง			หัวข้ออ้างอิงกับแนวทางโครงสร้างความมั่นคงปลอดภัยของการจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้าง
6	ระบบความปลอดภัยของโปรแกรมประยุกต์	6.1 กำหนดระบบความปลอดภัยบนโปรแกรมประยุกต์	ข้อที่ 5 ในหัวข้อ 4.2.2.2
		6.2 การกำหนดใช้ซอฟแวร์ที่ถูกกฎหมาย	-
		6.2 ระบบความปลอดภัยของผู้ใช้งาน	ข้อที่ 5 ในหัวข้อ 4.2.2.2
7	การควบคุมโครงข่าย	7.1 การพิสูจน์ และรับรองผู้ใช้งานบนระบบเครือข่าย	ข้อที่ 5 ในหัวข้อ 4.2.2.2
		7.2 การตรวจจับผู้ไม่ได้รับอนุญาตบนระบบเครือข่าย	ข้อที่ 4 ในหัวข้อ 4.2.2.2
		7.3 การเชื่อมต่อเครือข่ายกับนอกเขตที่ทำการ	ข้อที่ 4 ในหัวข้อ 4.2.2.2
8	การจัดการระบบความปลอดภัยบนไฟวอลล์		ข้อที่ 4 ในหัวข้อ 4.2.2.2
9	การจัดการบริการความปลอดภัย	9.1 การตรวจหาช่องโว่บน TCP/IP โปรโตคอล	ข้อที่ 4 ในหัวข้อ 4.2.2.2
		9.2 การตรวจจับและเฝ้าระวังของศูนย์ข้อมูล	ข้อที่ 4 ในหัวข้อ 4.2.2.2
		9.3 การรับประกันระบบความปลอดภัย	ข้อที่ 3 ในหัวข้อ 4.2.1

ตารางที่ 5.2 (ต่อ) แสดงการจับคู่ระหว่างเครื่องมือในการตรวจสอบความมั่นคงปลอดภัยของผู้ว่าจ้างกับแนวทางโครงสร้างความมั่นคงปลอดภัยของการจัดจ้างที่อยู่นอกที่ทำการของผู้ว่าจ้าง

หัวข้อการตรวจสอบความปลอดภัยของผู้ว่าจ้าง			หัวข้ออ้างอิงกับแนวทางโครงสร้างความมั่นคงปลอดภัยของการจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้าง
10	การจัดการเมื่อมีความเปลี่ยนแปลง	10.1 ความต้องการทั่วไปของการเปลี่ยนแปลงความปลอดภัย	ข้อที่ 6 ในหัวข้อ 4.2.1
		10.2 มาตรการเกี่ยวกับการเปลี่ยนแปลงระบบ	ข้อที่ 6 ในหัวข้อ 4.2.1
11	การกำหนดนโยบายเกี่ยวกับความปลอดภัย		ข้อที่ 1 ในหัวข้อ 4.2.2.2

จากตารางที่ 5.2 จะเห็นว่าเครื่องมือในการตรวจสอบความมั่นคงปลอดภัยของผู้ว่าจ้าง ส่วนใหญ่จะสอดคล้องกับการดำเนินงานด้านความรักษาความปลอดภัยภายในองค์กรขอ งผู้ให้บริการจัดจ้างเป็นส่วนใหญ่ ซึ่งอ้างอิงจากมาตรฐานของ ISO/IEC 27001 แสดงให้เห็นถึงผู้ว่าจ้างให้ความน่าเชื่อถือกับผู้ให้บริการจัดจ้างภายนอกที่มีการจัดการด้านความปลอดภัยที่ได้รับยอมรับที่เป็นมาตรฐานสากล

จากตารางที่ 5.2 เห็นว่าแนวทางความมั่นคงปลอดภัยการจั ดจ้างภายนอก นั้นไม่สามารถอ้างอิงได้ 1 หัวข้อจากทั้งหมด 11 หัวข้อ แสดงว่าแนวทางความมั่นคงปลอดภัยการจัดจ้างภายนอกสามารถตอบสนองตรงตามความมั่นคงปลอดภัยของผู้ว่าจ้างได้ 90.9%

5.4 การประเมินผลประโยชน์ของผู้ให้บริการจัดจ้างได้รับจากการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง

จากผลการศึกษาการรวบรวม ข้อมูลเกี่ยวกับแนวทางความมั่นคงปลอดภัยของการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง สามารถสรุปผลประโยชน์ที่ผู้ให้บริการจัดจ้างภายนอกได้รับ ซึ่งแสดงให้เห็นโดยทำการเปรียบเทียบระหว่างรูปแบบการจัดจ้างภายนอกที่อยู่ ภายในที่ทำ

การของผู้ว่าจ้างกับรูปแบบการจัดจ้างภายนอกที่อยู่นอกที่ทำการของผู้ว่าจ้าง ดังแสดงในตารางที่ 5.3

ตารางที่ 5.3 ตารางเปรียบเทียบผลประโยชน์ที่ได้จากการบริการจัดจ้างภายนอกระหว่าง ผู้ให้บริการจัดจ้างภายนอกโดยอยู่ที่ทำการของผู้ว่าจ้าง กับผู้ให้บริการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง

ผลประโยชน์ที่ได้จากการบริการจัดจ้างภายนอก	ผลประโยชน์ที่ได้รับ	
	ผู้ให้บริการจัดจ้างภายนอกโดยอยู่ที่ทำการของผู้ว่าจ้าง	ผู้ให้บริการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง
ลดค่าใช้จ่ายเกี่ยวกับซอฟต์แวร์	×	✓
ลดค่าใช้จ่ายเกี่ยวกับการติดตั้งและดูแลรักษาซอฟต์แวร์	×	✓
ลดค่าใช้จ่ายเกี่ยวกับฮาร์ดแวร์	×	✓
ลดค่าใช้จ่ายเกี่ยวกับการป้องกันความมั่นคงปลอดภัยของผู้ว่าจ้าง	×	✓
ความน่าเชื่อถือของผู้ว่าจ้าง	✓	×

เมื่อมีการจัดจ้างภายนอก โดยอยู่นอกที่ทำการของผู้ว่าจ้างจะช่วย ลดค่าใช้จ่ายในส่วนของซอฟต์แวร์ ฮาร์ดแวร์ การติดตั้ง และการบำรุงรักษา ให้กับผู้ให้บริการจัดจ้างภายนอก และยังช่วยลดค่าใช้จ่ายด้านความมั่นคงปลอดภัยให้กับผู้ว่าจ้างอีกด้วย แต่การจัดจ้างภายนอกโดยอยู่ภายในที่ทำการของผู้ว่าจ้างจะมีความน่าเชื่อถือกว่าเพราะอยู่ภายใต้ การดูแลความมั่นคงปลอดภัยของผู้ว่าจ้างเอง

บทที่ 6

สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยนี้เป็น การศึกษาเกี่ยวกับ แนวทางของ รูปแบบความมั่นคงปลอดภัย สำหรับจัดจ้างภายนอก โดยอยู่นอกที่ทำการของผู้ว่าจ้าง เพื่อสร้างความเชื่อมั่นในความมั่นคงปลอดภัย ให้กับผู้ว่าจ้างโดยการนำเอามาตรฐานเข้ามาจัดการด้านความมั่นคงปลอดภัย และโครงสร้างการบริการโปรแกรมที่มีความปลอดภัยให้กับผู้ว่าจ้าง

6.1 สรุปผลการวิจัย

งานวิจัย แนวทางรูปแบบความมั่นคงปลอดภัยสำหรับจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้าง จากรูปแบบความมั่นคงปลอดภัยการจัดจ้างภายนอก สามารถนำไปใช้เพื่อตอบสนองความต้องการของผู้ว่าจ้างที่มีความต้องการความปลอดภัยสำหรับข้อมูลขององค์กร อย่างเช่น ธนาคาร สถาบันการเงินได้ อีกทั้งผู้ให้บริการจัดจ้างภายนอกสามารถนำรูปแบบความปลอดภัยไปใช้เพื่อสร้างความน่าเชื่อถือให้กับลูกค้าได้ และยังสามา รถลดทรัพยากรบุคคลในการให้บริการจัดจ้างภายนอกเพื่อเข้าไปดูและระบบของลูกค้าได้ จากตารางที่ 5.3 เปรียบเทียบผลประโยชน์ที่ได้จากการบริการจัดจ้างภายนอกระหว่างผู้ให้บริการจัดจ้างภายนอกโดยวางระบบอยู่ในที่ทำการของผู้ว่าจ้างกับผู้ให้บริการจัดจ้างภายนอกโดยวางระบบอยู่นอกที่ทำการของผู้ว่าจ้าง

จากผลการประเมินในตารางที่ 5.2 แสดงการจับคู่ระหว่างเครื่องมือในการตรวจสอบความมั่นคงปลอดภัยของผู้ว่าจ้างกับแนวทางโครงสร้างความมั่นคงปลอดภัยของการจัดจ้างที่อยู่นอกที่ทำการของผู้ว่าจ้างเห็นว่ามีข้อตรงกันกับในส่วนของระบบความมั่นคงปลอดภัยของผู้ให้บริการจัดจ้างภายนอกมากที่สุด ซึ่งแสดงให้เห็นว่าผู้ว่าจ้างให้ความสำคัญกับการดำเนินงานด้านความมั่นคงปลอดภัยภายในองค์กรของผู้ให้บริการจัดจ้างภายนอกมากที่สุด

ดังนั้นการให้ความสำคัญกับความเชื่อมั่นของ ผู้ว่าจ้างเป็นส่วนที่สำคัญ สูงสุด เพราะข้อมูลสำคัญของผู้ว่าจ้างนั้นถูกดำเนินการจัดการภายใต้ผู้ให้บริการจัดจ้างภายนอก ดังนั้นผู้ให้บริการจัดจ้างภายนอก ต้องมีมาตรฐานในการบริการ และกระบวนการจัดการที่ได้มาตรฐาน ที่มีการยอมรับในแง่ของผู้ให้บริการจัดจ้างภายนอก ต้องให้ความสำคัญกับ การสร้างมาตรฐาน ที่มีความต่อเนื่อง และ ตลอดของช่วงสัญญา เพราะข้อมูลสารสนเทศขอ งผู้ว่าจ้าง ต้องอยู่ ภายใต้การดูแลของผู้ให้บริการจัดจ้าง ภายนอก อีกทั้งมีการทำข้อตกลงเกี่ยวกับ SLA ด้วยแล้วจึง สามารถสร้างความน่าเชื่อถือให้กับผู้ว่าจ้างได้

6.2 ข้อเสนอแนะ

1. เมื่อมีการกำหนดการดำเนินการด้านความมั่น คงปลอดภัยที่เป็นไปตามมาตรฐาน อย่างเช่น ISO/IEC 27001 แล้ว เพื่อเป็นการยืนยันว่ามีการดำเนินการจริงนั้นควรมีการดำเนินการเพื่อให้ได้รับใบรับรองที่ได้ความเชื่อถือ เพื่อเป็นข้อยืนยันให้กับผู้ว่าจ้าง

2. การสร้างความน่าเชื่อถือให้กับผู้ว่าจ้าง ในกรณีที่ผู้ให้บริก ารจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้างนั้นนอกจากกระบวนการความมั่นคงปลอดภัย แล้วยังจำเป็นต้องมีกระบวนการให้บริการที่มีประสิทธิภาพและมีมาตรฐาน จะเป็นตัวช่วยในการสร้างความน่าเชื่อถือให้กับผู้ว่าจ้างมากขึ้น

6.3 ประโยชน์ที่ได้รับจากงานวิจัย

1. ผู้ให้บริ การจัดจ้างภายนอก โดยอยู่ นอกที่ทำการของผู้ว่าจ้าง สามาถนำ แนว ทางความมั่นคงปลอดภัยไปใช้เพื่อเป็นแนวทางและปรับใช้เข้ากับองค์กรของผู้ให้บริการจัดจ้างภานอกหรือให้เข้ากับองค์กรผู้ว่าจ้างได้ เพื่อสร้างความน่าเชื่อถือให้กับผู้ว่าจ้าง

2. การให้บริการจัดจ้างภายนอกโ ดยอยู่นอกที่ทำการของผู้ว่าจ้างสามารถลดค่าใช้จ่ายที่เกี่ยวกับการให้บริการแก้ผู้ว่าจ้างมากกว่าการให้บริการจัดจ้างภายนอกโดยอยู่ที่ทำการของผู้ว่าจ้าง

3. ทำให้ทราบว่าในการเลือกผู้ให้บริการจัดจ้างภายนอกผู้ว่าจ้างใช้องค์ประกอบหลายด้านในการพิจารณา โดยระบบความมั่ นคงความปลอดภัยเป็นส่วนให้ความสำคัญระดับต้น สำหรับธุรกิจด้านสถาบันการเงิน

รายการอ้างอิง

[1] Sommer, R.A., Business process flexibility: a driver for outsourcing, Industrial Management and Data System, 2003.

[2] Camarinha-Matos, L.M. and H. Afsarmanesh, Virtual Enterprise Modeling and Support Infrastructures: Applying Multi-agent System Approaches, ACM Lecture Notes in Artificial Intelligence LNAI, 2001.

[3] Groves, J., Outsourced Security for Application Service Providers, Elsevier Science, 2001.

[4] Raman, B., et al, The SAHARA Model for Service Composition Across Multiple Providers, ACM Proceeding of the First International Conference on Pervasive Computer, 2002.

[5] Fan Jing Meng, Xiao Yang He, Shun Xing Yang, Peng Ji, A Unified Framework for Outsourcing Governance, The 9th IEEE International and the 4th IEEE International Conference and E-Servicees, 2007.

[6] IDC, IDC APJ Continuum Survey, 2007, Available from: http://www.idc.com/research/reshome.jsp [2007, August 21].

[7] C Colwill, A Gray, Creating an effective security risk model for outsourcing decisions, BT Technilogy Journal, 2007

[8] NISCC, Outsourcing:Security Governance Framework for IT Managed Service Provision, Available: http://www.cpni.gov.uk, 2005.

[9] Paul Williams, Andersen, Information Security Gouvernance, Information Security Technical Report, Vol6, 2001.

[10] National Institute of Standards and Technology, Available from: http://csrc.nist.gov/index.html [2008,Fubuary 10].

[11] OCTAVE Information Security Risk Evaluation, Available from: http://www.cert.org/octave [2008,Fubuary 10].

[12] The Risk Management Standard, Available from: http://www.standards.org.au/default.asp [2008,Fubuary 10].

[13] International Organization for Standardization, Available from: http://www.iso.org/iso/home.htm [2008,Fubuary 10].

[14] IT Infrastructure Library, Available from: http://www.itil.org.uk [2008,Fubuary 10].

[15] Qualitative Research, Available from: http://en.wikipedia.org/wiki/Qualitative_research [2009,Sebtember 10].

[16] Borko Furht, Boca Raton, Chris Phoenix, Fort Lauderdale, John Yin, Zijad Aganovic, An Innovative Internet Architecture for Application Service Providers, Proceedings of the 33rd Hawaii International Conference on System Sciences, 2000.

[17] Tanja Falkowski, Stefan Voß, Application Service Providing as Part of Intelligent Decision Support for Supply Chain Management, IEEE Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), 2002.

[18] Kenneth R. Walsh, Analyzing the application ASP concept technologies, economies, and strategies, COMMUNICATIONS OF THE ACM Vol. 46, No. 8, 2003.

[19] Framework for Measuring and Reporting Performance of Information Security Programs in Offshore Outsourcing, Available from: http://www.itgi.org [2009,Sebtember 10].

ภาคผนวก

ภาคผนวก
ผลงานตีพิมพ์

งานประชุมวิชาการนานาชาติ การวิจัยเทคโนโลยีสารสนเทศเพื่อการพัฒนาประเทศที่ยั่งยืน ครั้งที่ 2 (2nd National Conference on Information Technology 2008) ระหว่างวันที่ 6 - 7 พฤศจิกายน 2551 ณ มหาวิทยาลัยรังสิต เมืองกรุงเทพมหานคร ประเทศไทย ในบทความเรื่อง รูปแบบความมั่นคงปลอดภัยสำหรับการจัดจ้างการบริการจากภายนอก

รูปแบบความมั่นคงปลอดภัยสำหรับการจัดจ้างการบริการจากภายนอก

SECURITY MODEL FOR SERVICE OUTSOURCING

พลสินธ์ มูลสิงห์, ยรรยง เต็งอำนวย
ห้องปฏิบัติการวิศวกรรมระบบสารสนเทศ
ศูนย์เชี่ยวชาญเฉพาะทางวิศวกรรมซอฟแวร์
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
254 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กทม. 10330
E-mail: Ponsint.M@Student.Chula.ac.th, Yunyong.T@chula.ac.th

บทคัดย่อ

ในปัจจุบันองค์กรขนาดใหญ่ที่มีความต้องการขยายงานเพื่อเติบโต นั้นจำเป็นต้องมีการจัดจ้างภาย นอก แต่การที่มีการจัดจ้างภายนอกเข้ามาทำงานในองค์กรอาจทำให้เกิดความเสี่ยงของข้อมูลขององค์กรได้ ดังนั้นงานวิจัยนี้นำเสนอรูปแบบการให้บริการของการจัดจ้างภายนอก เพื่อให้บริการกับผู้ว่าจ้างที่ต้องการของความมั่นคงสูง โดยติดตั้งบริการอยู่ภายนอกเครือข่ายหรือที่ทำกา รของผู้ว่าจ้าง โดยมีความน่าเชื่อถือให้กับผู้ว่าจ้าง และผู้ว่าจ้างต้องสามารถควบคุมติดตามได้ และสามารถขยายเติบโตได้ง่ายสำหรับการให้บริการที่มีการจัดจ้างภายนอก และช่วยให้สามารถลดทรัพยากรของบริษัทที่ให้บริการการจัดจ้างภายนอกที่มีจำนวนลูกค้าที่ต้องให้บริการหลา ยรายได้ โดยรูปแบบความปลอดภัยสำหรับการจัดจ้างการบริการภายนอกผู้วิจัยได้แบ่งออกเป็นสองส่วน คือ การจัดการระบบความปลอดภัยการจัดจ้างภายนอก และ โครงสร้างการจัดจ้างภายนอก โดยอยู่นอกที่ทำการของผู้ว่าจ้าง โดยอ้างอิงจาก ธรรมาภิบาลด้านความปลอดภัยทางสารสนเทศ (ISG - information security governance)

คำสำคัญ : ระบบความมั่นคง, การจัดจ้างภายนอก

Abstract

This article is designed to describe security model outsourcing for customer that required high security. Security model is an off-premise organization which provided trust to customer also ensures security during this outsourcing process. For an outsource, the security model give convenience to outsource, connect network system between outsource and customer, saving resource when providing business to multi customers.

Keyword: Outsourcing, off-premise, security model

1. บทนำ

ในปัจจุบันบริษัทหรือองค์กรขนาดใหญ่ไม่อาจปฏิเสธได้ว่า การจัดจ้างภายนอกเพื่อบริการด้านระบบงานสารสนเทศแก่ลูกค้าเป็นหนึ่งในปัจจัยที่ขับเคลื่อนและขยายการเจริญเติบโต

แต่เนื่องจากการจัดจ้างภายนอกเพื่อทำระบบเทคโนโลยีสารสนเทศนั้น ความมั่นคงและความลับข้อมูลของลูกค้าของผู้ว่าจ้างเป็นเรื่องที่ต้องให้ความสำคัญ จึงต้องให้ผู้รับจ้างจากภายนอกเข้ามาติดตั้งอุปกรณ์ โปรแกรมปฏิบัติงาน และมีบุคลากรมาประจำอยู่ภายในเครือข่ายหรือที่ทำการของผู้ว่าจ้าง ซึ่งเป็นผลให้เกิดความเสี่ยงในด้านความปลอดภัยต่อผู้ว่าจ้างได้โดยเฉพาะอย่างยิ่งผู้ว่าจ้างที่ต้องมีระบบความปลอดภัยของข้อมูลสูง เช่น ธนาคาร สถาบันการเงิน อีกทั้งยังเป็นค่าใช้จ่ายที่สูงสำหรับผู้ว่าจ้าง และในส่วนของบริษัทที่ให้บริการจัดจ้างภายนอก โดยเฉพาะหากบริษัทมีจำนวนผู้ว่าจ้างในการให้บริการหลายราย ทำให้ต้องใช้ทรัพยากรเป็นจำนวนมาก ทั้งระบบเครื่องกำลังคน และค่าใช้จ่ายในการเดินทาง เพื่อให้ตอบสนองความต้องการของผู้ว่าจ้างได้

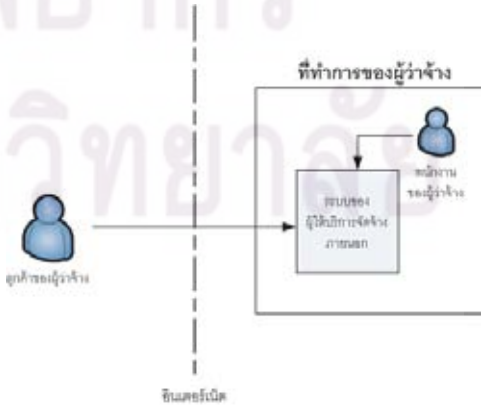
ดังนั้นจึงควรมีรูปแบบในการจัดจ้างภายนอกเพื่อทำระบบเทคโนโลยีสารสนเทศให้บริการแก่บุคคลากร และลูกค้าของผู้ว่าจ้างโดยที่มีการติดตั้งเครื่องระบบงานและข้อมูลอยู่ภายนอกเครือข่ายหรือนอกที่ทำการของผู้ว่าจ้าง รวมทั้งมีระบบความมั่นคงปลอดภัยสำหรับข้อมูลของผู้ว่าจ้าง

2. การจัดจ้างภายนอกเพื่อทำระบบเทคโนโลยีสารสนเทศ

ในปัจจุบันพบว่า ทุกผู้ว่าจ้างเริ่มให้ความสำคัญกับงานทางด้านไอที และมีการลงทุนทั้งด้านเครื่องมืออุปกรณ์ ฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่าย รวมถึงการพัฒนาบุคลากรเป็นจำนวน มาก [1] ขณะเดียวกันแรงผลักดันของระบบเศรษฐกิจใหม่ที่พึ่งพาข้อมูลข่าวสารมากขึ้นทำให้ผู้ว่าจ้างส่วนใหญ่ที่ไม่ได้มีสายการผลิตหรือเป้าหมายหลักที่เกี่ยวกับเทคโนโลยีสารสนเทศเกิดขาดแคลนบุคลากรที่มีความรู้ความสามารถดังจะเห็นได้จากการตั้งแผนกไอทีในองค์กรของผู้ว่าจ้างซึ่งหาบุคลากรได้ยากเพราะผู้มีความรู้ความสามารถไม่อยากทำงานในหน่วยงานไอทีเหล่านั้นทำให้งานทางไอทีไม่ประสบผลสำเร็จถ้าองค์กรทำการพัฒนาและดำเนินงานเหล่านี้เอง

ดังนั้นองค์กรต่าง ๆ จึงเริ่มให้ความสนใจหน่วยงานให้บริการจากภายนอก ซึ่งอาจเป็นบริษัทหรือธุรกิจที่ให้บริการพัฒนาเทคโนโลยีสารสนเทศที่มีความรู้ความชำนาญ สามารถพัฒนาระบบงานให้เสร็จได้เร็ว มีคุณภาพ และควบคุมค่าใช้จ่าย การว่าจ้างเช่นนี้เรียกว่าการ จัดจ้างภายนอก (outsourcing) การเรียกใช้บริการในลักษณะนี้เริ่มเป็นที่รู้จักกันอย่างแพร่หลาย และมีบริษัทเข้ามาดำเนินธุรกิจจำพวกนี้มากขึ้น [1]

ปัจจุบันความต้องการในการใช้งานทางด้านระบบเทคโนโลยีสารสนเทศมีความหลากหลายมากขึ้น เช่นการตั้งเว็บไซต์ให้กับผู้ว่าจ้าง การบริหารเซิร์ฟเวอร์ การทำระบบบริการลูกค้า เช่น ระบบออนไลน์ในรูปแบบบริการเชิงอิเล็คทรอนิกส์ ต่าง ๆ ดังนั้นจึงมีการดำเนินการโดยบริษัทที่ให้บริการจัดจ้างภายนอกมีการดูแลฮาร์ดแวร์ ซอฟต์แวร์ เซิร์ฟเวอร์ เครือข่าย และอุปกรณ์ประกอบต่าง ๆ ให้ทั้งหมด โดยให้ผู้ว่าจ้างเป็นผู้ใช้งาน โครงสร้างในระบบธุรกิจของการบริการจึงมีรูปดังรูปที่ 1



รูปที่ 1: การให้บริการผ่านการจัดจ้างภายนอก

3. การจัดจ้างภายนอกเพื่อให้บริการภายในที่ทำการ

การที่มีการจัดจ้างภายนอกเข้ามาให้บริการเทคโนโลยีสารสนเทศภายในที่ทำการของผู้ว่าจ้างนั้นทำให้เกิดผลกระทบหลายด้านกับองค์กร [2] ดังแสดงรูปที่ 2

รูปที่ 2: ผลกระทบกับธุรกิจเมื่อมีการจัดจ้างภายนอก

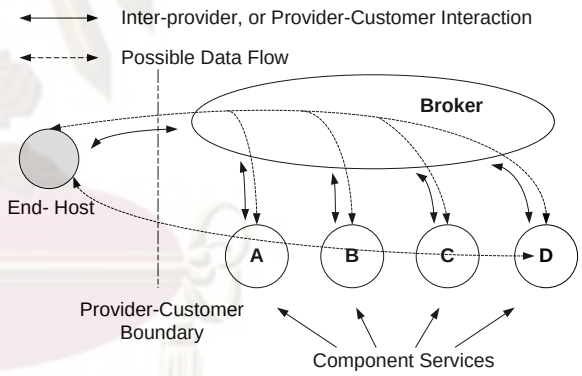
จากรูปที่แสดงจะเห็นได้ว่าผลกระทบที่เกิดขึ้นเฉพาะผู้ว่าจ้างนั้นมีอยู่สองส่วนคือ

- Security
- Loss of control

ส่วนที่เหลือจะเป็นผลกระทบที่เกิดขึ้นกับทั้งสองฝ่ายและจากการข้อมูลของ Computer Security Institute [3] ได้ทำการสำรวจเมื่อปี ค.ศ. 2007 พบว่ามีการโจมตีจากภายในองค์กรถึง 61% ของการโจมตีทั้งหมดแสดงให้เห็นว่าการที่มีการจัดจ้างภายนอกที่เข้ามาอยู่ในที่ทำการของผู้ว่าจ้างนั้นมีความเสี่ยงในระบบความปลอดภัยของผู้ว่าจ้างหรือลูกค้าได้

4. รูปแบบความปลอดภัยการให้บริการจัดจ้างภายนอก

การให้บริการจัดจ้างภายนอกโดยอยู่นอกที่ทำการของผู้ว่าจ้างนั้น ซอมเมอร์ [3] ได้เสนอรูปแบบการให้บริการที่มีความยืดหยุ่นที่สามารถเชื่อมต่อกับระบบอีอาร์พี (ERP – Enterprise Resource Plan) ได้ง่าย สะด วก และมีความมั่นคงปลอดภัย ซึ่งสามารถนำไปใช้กับการทำการจัดจ้างภายนอกได้ ส่วนรามาน และคณะ [4] ได้นำเสนอโครงสร้างของการผนวกการให้บริการของ Application Service Provider (ASP) โดยมีการให้บริการร่วมกันแก่ลูกค้าโดยใช้ Broker Model คือรูปแบบการร่วมกันให้บริการของผู้ ให้บริการ (provider) หลายรายโดยมีผู้ให้บริการรายหนึ่งทำหน้าที่เป็นตัวแทน (broker) และทำหน้าที่ให้บริการเพื่อประโยชน์ของลูกค้า และมีการให้บริการแบบ end to end ดังรูปที่ 3



รูปที่ 3: ระบบพื้นฐานของโครงสร้าง broker

โบรกเกอร์ (broker) รับหน้าที่เป็นผู้รวบรวมการบริการ ซึ่งโบรกเกอร์จะให้บริการตามลักษณะงานของแต่ละผู้ให้บริการที่อยู่ภายใต้ โบรกเกอร์ เพราะลั กษณะการให้บริการของแต่ละผู้ให้บริการที่อยู่ภายใต้ โบรกเกอร์เดียวกันอาจไม่ เชื่อถือซึ่งกันและกัน ซึ่งเป็นจำกัดของการแลกเปลี่ยนข้อมูลภายใน broker model

5. รูปแบบความปลอดภัยสำหรับการจัดจ้างการบริการจากภายนอก

การสร้างความเชื่อมั่นในระบบความปลอดภัยให้กับลูกค้าเมื่อมีการให้บริการจัดจ้างภายนอกนั้น ต้องมีรูปแบบระบบความปลอดภัยที่มีมาตรฐานโดยผู้วิจัยได้สร้างรูปแบบความปลอดภัยเมื่อมีการจัดจ้า งภายนอกโดยอ้างอิงจาก ระบบภิบาลด้านความปลอดภัยสารสนเทศ เพราะระบบสารสนเทศนั้นปัจจุบันได้นำมาใช้กันอย่างแพร่หลายกับทุกบริษัทหรือองค์กรทั่วไป ในการเติบโต ต้องอาศัยระบบสารสนเทศอีกด้วย แต่ก็มีโอกาสให้เกิดความเสี่ยงตามมากับประโยชน์ที่ได้รับ ดังนั้นจึงต้องมีระบบกา รจัดการที่ครอบคลุมภัยที่จะเกิดขึ้นกับระบบสารสนเทศในทุก ๆ ด้านของบริษัทหรือองค์กร และคณะกรรมการและผู้บริหารต้องการความมั่นใจว่าได้มีการจัดการกับความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศรวมอยู่ในนโยบายและแผนขององค์กรแล้ว อีกทั้งต้องมีความเหมาะสมและเป็นประโยชน์สู งสุดกับบริษัทหรือองค์กร

โดยงานวิจัยนี้มีการแบ่งออกเป็นสองส่วน ด้วยกัน คือ การจัดการระบบความปลอดภัยการจัดจ้างภายนอก และ โครงสร้างการจัดจ้างภายนอก โดยอยู่นอกที่ทำการของผู้ว่าจ้าง

5.1. การจัดการระบบความปลอดภัยของการจัดจ้างภายนอก

การจัดการความปลอดภัยของการจั ดจ้างภายนอกนั้นมีการแบ่งออกเป็น 5 ขั้นตอนซึ่งแบ่งออกเป็นดังนี้

- การประเมินความเสี่ยง (Risk Assessment) ก่อนที่จะมีการตกลงการจัดจ้างภายนอกนั้นต้องมีการประเมินความเสี่ยงที่จะเกิดขึ้นกับองค์กรของผู้ว่าจ้าง และผู้ให้บริการจัดจ้าง เพื่อให้ทั้งสองฝ่ายมีความเข้าใจตรงกันในความต้องการของระบบความมั่นคงขององค์กร ในการประเมินความเสี่ยงอ้างอิงจาก The NISCC guide to risk management [6] ซึ่งประกอบด้วย 6 ขั้นตอนดังนี้

1. ระบุกระบวนการทางด้านธุรกิจ และรูปแบบการใช้งานทั้งหมดขององค์กร
2. ระบุกระบวนการทางธุรกิจ กลยุทธ์ทางเทคนิค โครงสร้าง ของแต่ละหน่วยงาน
3. นำระบบของแต่ละหน่วยงานทั้งหมดมารวมออกมาจะได้ ตัวประเมินผลกระทบของธุรกิจ เพื่อใช้ในการวัดระดับของผลกระทบทางธุรกิจ
4. ทำการประเมินการโจมตีระบบความมั่นคง
5. ตรวจสอบจุดอ่อนของระบบ
6. ระบุช่องว่างระหว่างระดับความเสี่ยงในปัจจุบัน กับระดับความเสี่ยง ที่องค์กรได้ตั้งไว้

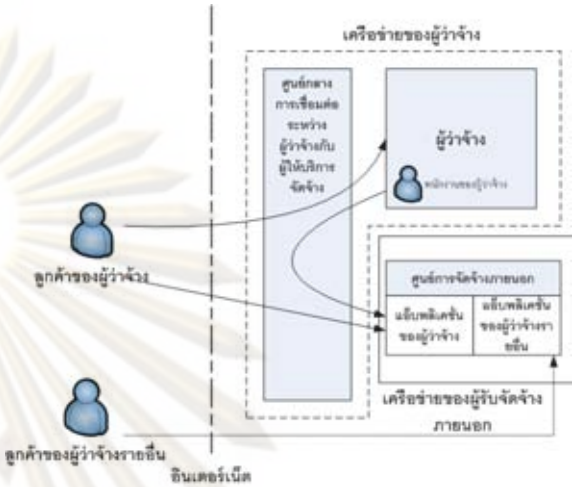
- การทำความเข้าใจและข้อตกลงของความต้องการระบบความปลอดภัยทั้งสองฝ่าย คือการทำสัญญาข้อตกลงในระบบความปลอดภัยของทั้งสองฝ่าย โดยผู้ว่าจ้างจะได้มีหลักฐานเป็นลายลักษณ์อักษรที่สอดคล้องกับความต้องการด้านระบบความปลอดภัยของผู้ว่าจ้าง ซึ่งประกอบด้วย เรื่องของระบบการจัดการด้านความมั่นคง กฎหมาย กฎข้อบังคับ โครงสร้าง
- การควบคุมการจัดจ้างภายนอก คือการควบคุมระบบความปลอดภัยให้เป็นไปตามที่ได้มีการตกลงไว้ของทั้งสองฝ่าย โดยมีการนำเอามาตรฐานการจัดการระบบสารสนเทศ ISO27001 ISMS [7] เข้ามาใช้จะประกอบด้วยขอบเขตทั้งหมด

ที่เกี่ยวกับการจัดจ้างภายนอก รวมทั้งบุคคลที่เกี่ยวข้อง และกระบวนการด้านความปลอดภัย

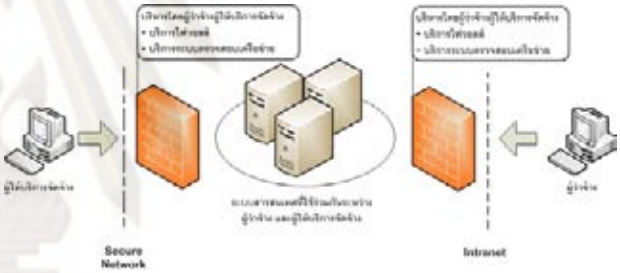
- การจัดการกับเหตุการณ์ที่จะเกิดขึ้น มีการทำรายงานให้กับผู้ว่าจ้าง ที่เกี่ยวกับการบริการที่เกี่ยวข้องกับระบบความปลอดภัย ซึ่งประกอบด้วย
  - เหตุการณ์ที่เกิดขึ้น
  - เหตุการณ์ที่น่าสงสัย
  - ความผิดปกติที่เกิดขึ้น
  - ข้อตกลงโดยกฎข้อบังคับขององค์กร การรักษาความปลอดภัย
  - การปฏิบัติตามคำสั่งของบุคคลากร หรือการละเมิดกฎข้อบังคับของบุคคลากรภายในองค์กร
- การเปลี่ยนแปลงระบบความปลอดภัย ซึ่งมีผลกระทบกับระบบความมั่นคง ดังนั้นจะต้องมีการทำสัญญาที่ชัดเจนของ ทั้งสองฝ่าย เมื่อมีการเปลี่ยนแปลงระบบความมั่นคง ซึ่งต้องมีการกำหนดขั้นตอนและผู้ที่มีความรับผิดชอบหน้าที่อย่างชัดเจน

5.2. โครงสร้างการจัดจ้างภายนอกที่ทำการผู้ว่าจ้าง

เราสามารถกำหนดโครงสร้างของการให้บริการจัดจ้างภายนอกโดยแยกการให้บริการออกจากที่ทำการ (premise) ของผู้ว่าจ้าง ซึ่งนำหลักการของซอมเมอร์และรามาน มาใช้ในการแยกระบบของผู้ให้บริการจัดจ้างภายนอก อยู่นอกที่ทำการผู้ว่าจ้าง การเชื่อมต่อกันจะมีศูนย์กลางที่เป็นผู้ให้บริการ ระหว่างผู้ใช้ในที่ทำการของผู้ว่าจ้างกับบริษัทที่รับจัดจ้างภายนอก และระหว่างลูกค้าของ ผู้ว่าจ้างกับบริษัทที่รับจัดจ้างภายนอก เพื่อให้สามารถคอยติดตามตรวจจับการโจมตีที่ผ่านจากลูกค้าของผู้ว่าจ้างที่ใช้งานบนระบบอินเตอร์เน็ต และจากผู้ใช้ในที่ทำการของผู้ว่าจ้างด้วย โดยแสดงสถาปัตยกรรมในชั้นต้นดังรูปที่ 4



รูปที่ 4: รูปแบบการให้บริการผ่านผู้ให้บริการจัดจ้างภายนอก



ศูนย์กลางการเชื่อมต่อคั่นระหว่างผู้ว่าจ้างกับผู้ให้บริการจัดจ้างภายนอก และระหว่างลูกค้าของผู้ว่าจ้างกับผู้ให้บริการจัดจ้างภายนอก โดยศูนย์กลางจะอยู่ภายใต้เครือข่ายในที่ทำการของผู้ว่าจ้างโดยใช้มาตรฐาน ISO 17002 ในการบริหารความปลอดภั ย โครงสร้างของศูนย์กลาง การเชื่อมต่อ ดังรูปที่ 5 จะประกอบด้วย ไฟวอลล์ (firewall) และ ไอดีเอส (IDS - intrusion detection system)

รูปที่ 5: โครงสร้างระบบศูนย์กลางเชื่อมต่อระหว่างผู้ให้บริการจัดจ้างและผู้ว่าจ้าง

- ระบบไฟวอลล์ (firewall system) มีการวิเคราะห์และควบคุม เส้นทางของการสื่อสารข้อมูล ซึ่งเป็นไปตาม นโยบายความมั่นคงความปลอดภัยของผู้ว่าจ้าง และ การจัดเก็บบันทึกข้อมูล (log) ของความปลอดภัยที่เกี่ยวข้องทั้งหมด มีการแจ้งเตือนไปยังผู้ดูแลความปลอดภัยของระบบ การจัดการระบบไฟวอลล์นั้นต้องมีความมั่นใจเกี่ยวกับการที่ผู้ใช้งานที่ไม่ได้รับอนุญาต หรือไม่ได้รับการยืนยันตัวตนนั้นจะไม่มีสิทธิผ่านระบบไฟวอลล์ได้

- ระบบการตรวจจับในเครือข่าย (intrusion detection system) เป็นระบบที่ทำการตรวจจับพฤติกรรมที่เกิดขึ้นในระบบเครือข่ายและจัดเก็บบันทึกเป็นรายงานเพื่อนำมาวิเคราะห์รู ปแบบของพฤติกรรมผิดปกติที่อาจเกิดขึ้นในระบบซึ่งจำส่งผลบันทึกให้กับผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก

มีการกำหนดความรับผิดชอบด้านความปลอดภัยที่สามารถมีการตรวจสอบได้ทั้งสองฝ่าย

ฝ่ายผู้ว่าจ้าง

ผู้บริหารอวุโส	• กำหนดแนวทางความปลอดภัยขององค์กร
ผู้จัดการIT	• ร่วมกำหนดแนวทางความปลอดภัย • ทำความเข้าใจทั้งสองฝ่ายในความต้องการด้านความปลอดภัยขององค์กร
ฝ่ายปฏิบัติการ	• ตรวจสอบระบบความปลอดภัยและกำหนดการเข้าถึงข้อมูล

ฝ่ายผู้ให้บริการจัดจ้างภายนอก

ผู้บริหารอวุโส	• กำหนดแนวทางความปลอดภัยขององค์กร
ผู้จัดการIT	• รับความต้องการด้านความปลอดภัยของผู้ว่าจ้าง • กำหนดระบบความปลอดภัยขององค์กร
ฝ่ายปฏิบัติการ	• ตรวจสอบระบบความความปลอดภัยและกำหนดการเข้าถึงข้อมูลขององค์กร

มีการกำหนดวัฏจักรของการเปลี่ยนแปลงระบบความปลอดภัย

- กำหนดความต้องการระบบความปลอดภัย โดยผู้ว่าจ้างเป็นผู้กำหนดซึ่งจะต้องมีค วามเข้าใจใน

ระบบด้านความปลอดภัยและมีประสบการณ์เพื่อให้ประโยชน์สูงสุดกับองค์กรของผู้ว่าจ้าง

- ตรวจสอบความต้องการระบบความปลอดภัย โดยร่วมกันทั้งสองฝ่ายทั้งผู้ว่าจ้างและผู้ให้บริการจัดจ้างภายนอก เพื่อทำการตกลงความเข้าใจในความต้องการความปลอดภัย และวิเคราะห์ผลกระทบกับองค์กรทั้งสองฝ่าย

- ปฏิบัติการตามความต้องการเปลี่ยนแปลงระบบความปลอดภัย โดยผู้ให้บริการจัดจ้างภายนอกตามความตกลงที่ได้กำหนดกันไว้ทั้งสองฝ่าย

ความปลอดภัยของระบบปฏิบัติการ จะอยู่ในส่วนของผู้ให้บริการจัดจ้างภายนอกจึงต้องมีระบบความปลอดภัยสูง โดยมีการให้ความสำ คัญดังนี้

- การพิสูจน์ตัวตน และการยืนยันตัวตน กระบวนการยื่นยันตัวบุคคลนั้นจะต้องสามารถพิสูจน์ได้ว่าไม่มีการแอบอ้างของบุคคลอื่นในการใช้งานในระบบ

- การควบคุมการเข้าถึง มีการตรวจวัดในการป้องกันจากผู้ใช้งาน จากการเข้าถึงข้อมูลในส่วนที่ไม่ได้เกี่ยวข้อง

- ความถูกต้องของข้อมูล ความสัมพันธ์ระหว่างข้อมูลต้นทางที่แตกต่าง ควรต้องไม่มีการเปลี่ยนแปลง และการแลกเปลี่ยนข้อมูลระหว่าง process ที่แตกต่างกันต้อง ไม่เปลี่ยนแปลงของข้อมูล

- ความน่าเชื่อถือของการให้บริการ บางช่วงเวลาที่มีงานเร่งด่วนเข้ามาเป็นจำนวนมาก เครื่องมือต้องมีการจัดการเพื่อป้องกันไม่ให้เกิดการทำงานเกินจนไม่สามารถทำงานต่อได้

- การบันทึกเหตุการณ์ที่เกิดขึ้น มีการเก็บบันทึกเหตุการณ์ที่เกิดขึ้นต่างๆ เพื่อใช้ในการยืนยันในพฤติกรรมของผู้ใช้งาน

- การวิเคราะห์เหตุการณ์ ทุกๆวันจะเกิดพฤติกรรมมากมาย ซึ่งมีการจัดเก็บไว้นั้นเพียงพอต่อการนำมาเพื่อวิเคราะห์ความปลอดภัยในภายหลังได้

- Re-use การนำกลับมาใช้ใหม่ของส่วนประกอบในระบบปฏิบัติการ อย่างเช่น ตัวบันทึกข้อมูล ที่มีการนำกลับมาใช้ใหม่ ก็ต้องมีการเก็บรักษาความปลอดภัยไว้เป็นอย่างดี

- ความไว้วางใจในโปรแกรมประยุกต์ โปรแกรมประยุกต์นั้นต้องคำนึงถึงความปลอดภัยในข้อมูลที่เป็นความลับของผู้ว่าจ้าง และข้อมูลของลูกค้า และต้องแน่ใจว่าเป็นไปตามความต้องการของความปลอดภัยของผู้ว่าจ้าง

- มีกระบวนการเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูล ซึ่งในการเปลี่ยนแปลงสิทธิของผู้ใช้งานในแต่ละครั้งต้องไม่สามารถทำการเปลี่ยนได้เพียงคนเดียว ต้องมีกระบวนการด้านความปลอดภัยเพื่อขอในการเปลี่ยนแปลงสิทธิของผู้ใช้งาน

ความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

- มีการจัดสรรพื้นที่ที่เหมาะสมให้กับอุปกรณ์ประมวลผลสารสนเทศ และควบคุมการเข้า-ออกอย่างเหมาะสม

- มีระบบการป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม เช่น ไฟไหม้ แผ่นดินไหว น้ำท่วม หรือเหตุการณ์อื่นที่เกิดจากมนุษย์และธรรมชาติ
- มีระบบกำลังไฟสำรอง เพื่อป้องกันการเกิดไฟฟ้าขัดข้อง เพื่อให้ระบบดำเนินการต่อไปได้
- มีการควบคุมอุณหมิที่เหมาะสมต่ออุปกรณ์ประมวลผลสารสนเทศ และความชื้นเพื่อป้องกันความเสียหายกับอุปกรณ์ประมวลผลสาสนเทศ
- มีการสำรองข้อมูลทุกวัน แล้วบันทึกลงเทปแล้วนำไปจัดเก็บยังศูนย์สำรอง เพื่อป้องกันการสูญหายของข้อมูล

6. ผลการทดลอง

ได้มีการจัดทำกรณีศึกษาจากรูปแบบความปลอดภัยการให้บริการจัดจ้างภายนอกและได้นำ Information Security Governance Assessment [8] เพื่อประเมิณในองค์กรของผู้ว่าจ้างโดย กลุ่มเป้าหมายที่มีความต้องการความปลอดภัยสูง จะได้ผลลัพท์จากการประเมินนั้นอยู่ในเกณฑ์ดี

7. สรุปผล

จากรูปแบบความปลอดภัยการจัดจ้างภายนอก สามารถนำไปใช้เพื่อตอบสนองความต้องการของผู้ว่าจ้างที่มีความต้องการความปลอดภัยสำหรับข้อมูลขององค์กร อย่างเช่น ธนาคาร สถาบันการเงิน อีกทั้งผู้ให้บริการจัดจ้างภายนอกสามารถนำรูปแบบความปลอดภัยไปใช้เพื่อสร้างความน่าเชื่อถือให้กับลูกค้าได้ และยังสามารถลดทรัพยากรบุคคลในการให้บริการจัดจ้างภายนอกเพื่อเข้าไปดูแลระบบของลูกค้าได้

แต่ในการสร้างความน่าเชื่อถือในระบบความปลอดภัยสำหรับการจัดจ้างภายนอกนั้นไม่เพียงแต่การป้องกันในด้านเทคนิคเพียงอย่างเดียว ผู้ให้บริการจัดจ้างต้องมีระบบการจัดการด้านความปลอดภัย (security management) และนำมาตรฐานความปลอดภัยที่เป็นที่ยอมรับเช่น ISO 27001 เข้ามาใช้ เพื่อสร้างความน่าเชื่อถือให้กับผู้ว่าจ้าง หรือลูกค้าได้

7. รายการอ้างอิง

[1] IDC, IDC APJ Continuum Survey, 2007, Avalable: http://www.idc.com/research/reshome.jsp, Access date: August 21, 2007.

[2] Fan Jing Meng, Xiao Yang He, Shun Xing Yang, Peng Ji, A Unified Framework for Outsourcing Governance, The 9th IEEE International Conference on E-Commerce Technology and the 4th IEEE International Conference and E-Services, 2007. Computer Security Institute Survey 2007, Avalable : http://www.gocsi.com, Access date : June 10, 2008.

[3] Sommer, R.A., Business process flexibility: a driver for outsourcing, Industrial Management and Data System, 2003.

[4] Raman, B., et al, The SAHARA Model for Service Composition Acroses Multiple Providers, ACM Proceeding of the First International Conference on Pervasive Computer, 2002.

[5] The NISCC guide to risk management, Available:

http://www.niscc.gov.hk/niscc/docs/re-20050804-00653.pdf?lang=en, Access date: Auguest04, 2005.

[6] International Organization for Standardization, Available: http://www.iso.org/iso/home.htm, Access date: Fubuary10, 2008.

[7] Information Security Governance Assessment, Available: http://www.niscc.gov, Access date: October, 2008.

ประวัติผู้เขียนวิทยานิพนธ์

นายพลสินธ์ มูลสิงห์ เกิดเมื่อวันที่ 9 สิงหาคม พ.ศ. 2521 ที่จังหวัดนนทบุรี สำเร็จการศึกษาหลักสูตร วิศวกรรมศาสตร บัณฑิต (วศ.บ.) สาขา วิชา วิศวกรรมไฟฟ้ากำลัง คณะวิศวกรรมศาสตร์ มหาวิทยาลัย ศรีปทุม เมื่อปีการศึกษา 2541 และเข้าศึกษาต่อหลักสูตร วิทยาศาสตร มหาบัณฑิต สาขา วิชา วิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิว เตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อปีการศึกษา 2549 ปัจจุบันทำงานบริษัทที่ให้การสนับสนุนสถาบันการเงินแห่งหนึ่ง มีหน้าที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยขององค์กรเพื่อเป็นไปตามมาตรฐาน และตรงความต้องการของผู้ว่าจ้าง