บทที่ 3

ระเบียบวิธีวิจัย

3.1 กรอบระเบียบวิธีวิจัย

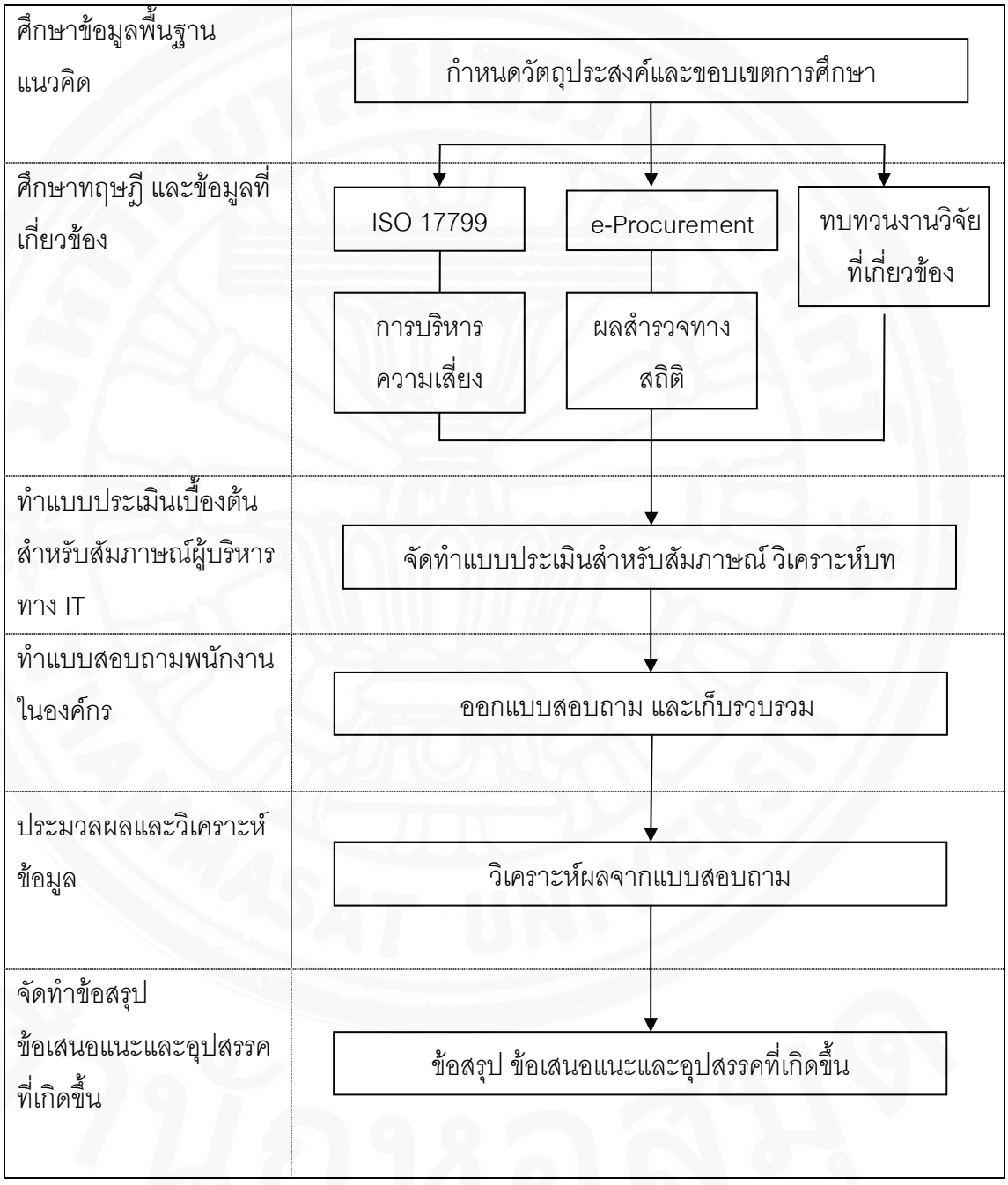
ในการศึกษาเพื่อสร้างมาตรฐานความปลอดภัยของข้อมูลขององค์กร และการลดความเสี่ยงการคุกคามข้อมูลสารสนเทศ โดยการนำมาตรฐานสากลมาประยุกต์ใช้ เพื่อให้บรรลุวัตถุประสงค์ที่กำหนดไว้สำหรับการวิจัยนี้ งานวิจัยฉบับนี้จึงใช้ระเบียบวิธีวิจัยเชิงพรรณนา (Descriptive research) และวิธีวิจัยเชิงสำรวจ (Exploratory research)

โดยผู้วิจัยได้แบ่งขั้นตอนการทำวิจัยเป็นดังต่อไปนี้

1. การศึกษาข้อมูลพื้นฐาน แนวคิด กำหนดวัตถุประสงค์ของงานวิจัยและขอบเขตการศึกษา
2. การศึกษาทฤษฎี บทความ หนังสือ วารสารและข้อมูลทางเว็บไซต์ที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูล และการจัดการความเสี่ยงและการศึกษา รวบรวมงานวิจัยตัวอย่างเพื่อเป็นแนวทางในการจัดทำและศึกษาเพิ่มเติม
3. การจัดทำแบบประเมินเบื้องต้นด้านมาตรฐานความปลอดภัยขององค์กรเทียบกับมาตรฐาน ISO17799
4. การจัดทำแบบสอบถามพนักงานทั้งองค์กรเพื่อประเมินความเสี่ยงและหาจุดที่ควรปรับปรุงแก้ไขในองค์กรที่ทำการสำรวจ
5. การประมวลผลและวิเคราะห์ข้อมูล ผลที่ได้รับและอุปสรรคที่เกิดขึ้น
6. การจัดทำสรุปและข้อเสนอแนะสำหรับการดำเนินงานวิจัย

ภาพที่ 3.1

กรอบระเบียบวิธีวิจัย



3.2 แหล่งข้อมูลที่ศึกษา

เป็นการมุ่งเน้นเพื่อการศึกษาสำหรับการนำมาตรฐานสากลในการรักษาความปลอดภัยของข้อมูลและการลดความเสี่ยงที่อาจเกิดขึ้นแก่องค์กรที่ให้บริการในด้านการจัดซื้อออนไลน์ หรือองค์กรที่เป็นตลาดกลางอิเล็กทรอนิกส์ มาประยุกต์ใช้เพื่อให้เกิดประสิทธิภาพและประสิทธิผล รวมทั้งนำมาเพื่อหาแนวทางการป้องกันหรือแก้ไขปัญหาที่พบ โดยแหล่งข้อมูลสำคัญสำหรับการวิจัยนี้ประกอบด้วย 2 ส่วน คือ

3.2.1 แหล่งข้อมูลปฐมภูมิ (Primary data)

เป็นข้อมูลที่ได้มาจาก

1). การสัมภาษณ์บุคลากรที่เกี่ยวข้องในองค์กรที่ทำการศึกษาเบื้องต้น เพื่อการประเมินการดำเนินงานปัจจุบันเบื้องต้น (Check List)

2). การใช้แบบสอบถามจากพนักงานในองค์กรทั้งในระดับบริหารและระดับปฏิบัติการทั้งหมด เพื่อทำการสำรวจความเสี่ยงที่เกี่ยวการรักษาความปลอดภัยขององค์กร

3.2.2 แหล่งข้อมูลทุติยภูมิ (Secondary data)

เป็นข้อมูลที่ได้มาจาก

1). ข้อกำหนดมาตรฐาน ISO17799

2). งานวิจัยที่เกี่ยวข้อง

3). หนังสือ ตำรา Web Site เอกสารทางวิชาการ บทความในวารสารและของผู้เชี่ยวชาญที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ

4). ข้อมูลทางสถิติที่เกี่ยวข้องกับความเสี่ยงทางคอมพิวเตอร์

3.3 ตัวแปรที่ใช้ในการวิจัย

ตัวแปรสำหรับงานวิจัยนี้ประกอบด้วยตัวแปรอิสระ (Independent variable) และตัวแปรตาม (Dependent variable) รายละเอียดดังต่อไปนี้

3.3.1 ตัวแปรอิสระ (Independent variable)

ประกอบด้วย

1). ระดับอายุงานของพนักงานที่ตอบแบบสอบถาม

2). หน่วยงานที่สังกัดในองค์กร

3.3.2 ตัวแปรตาม (Dependent variable)

ซึ่งเป็นตามมาตรฐาน ISO17799 ประกอบด้วย

1). การรับรู้ด้านนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ

2). การรับรู้ด้านโครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กรและที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก

3). การรับรู้ด้านหน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กรและการจัดหมวดหมู่สารสนเทศ

4). การสร้างความมั่นคงปลอดภัยในระบบสารสนเทศทั้งก่อนการจ้างงานและในระหว่างการจ้างงาน

5). การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมขององค์กร

6). การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

7). การให้ความสำคัญและมาตรฐานการควบคุมการเข้าถึง

8). การพบปัญหาทางการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศในองค์กร

9). การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

10). การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

11). การปฏิบัติตามข้อกำหนดขององค์กร

3.4 เครื่องมือที่ใช้ในการวิจัย

เนื่องจากงานวิจัยฉบับนี้เป็นงานวิจัยที่มุ่งหวังการนำมาตรฐาน แนวคิดและทฤษฎีเข้ามาประยุกต์ใช้โดยการจัดทำการวิจัยขึ้นมา เพื่อแสดงให้องค์กรทั้งระดับผู้บริหารและระดับปฏิบัติการ เห็นภาพและเห็นความสำคัญของการรักษาความปลอดภัยของข้อมูล โดยเครื่องมือที่ใช้ในการวิจัย ประกอบด้วย

3.4.1 การศึกษามาตรฐานISO17799

รวมทั้งทฤษฎีที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลภายในองค์กร และการศึกษาเอกสารของข้อมูลการสำรวจรวมถึงสถิติต่างๆเพื่อใช้ประกอบข้อมูลด้านความเสี่ยงและภัยคุกคามต่างๆที่เกิดขึ้นในปัจจุบัน (Documentation)

3.4.2 การใช้แบบประเมินเบื้องต้น (Check List)

เพื่อให้ทราบถึงสภาพขององค์กรที่ทำการศึกษา ในปัจจุบันว่ายังขาดการจัดการด้านความปลอดภัยของข้อมูลในเรื่องใดบ้าง โดยการทำแบบสัมภาษณ์กับผู้มีส่วนเกี่ยวข้องด้าน IT ในระดับผู้บริหารและผู้มีส่วนเกี่ยวข้องในการรักษาความปลอดภัยด้านข้อมูลขององค์กร โดยอิงการประเมินตามมาตรฐาน ISO17799

3.4.3 การใช้แบบสอบถาม (Questionnaire)

เพื่อใช้ในการวิเคราะห์ข้อมูล และศึกษาแนวทางการประยุกต์ใช้ มาตรฐานสากล ISO 17799 ในการรักษาความปลอดภัยของระบบสารสนเทศในองค์กร ที่ให้บริการด้านการจัดซื้อออนไลน์ (e-Procurement) และเพื่อจัดทำข้อสรุปในส่วนที่องค์กรควรพัฒนาและปรับปรุง โดยแบ่งเป็น 3 ส่วนหลักๆ คือ

1). คำถามข้อมูลทั่วไป สำหรับการเก็บข้อมูลเบื้องต้นของผู้ตอบแบบสอบถามเพื่อใช้แยกกลุ่มของผู้ตอบแบบสอบถาม และสำหรับนำไปพิจารณาผลของงานวิจัยตามสมมุติฐาน ข้อมูลที่ใช้ได้แก่ ระยะเวลาการทำงานในองค์กรปัจจุบันและหน่วยงานที่ทำ

2). <u>คำถามข้อมูลในการแสดงความคิดเห็น ด้านการรักษาความปลอดภัยระบบสารสนเทศขององค์กร</u> (โดยในที่นี้ระบบสารสนเทศ ประกอบไปด้วย ข้อมูล ระบบคอมพิวเตอร์และระบบเครือข่ายต่างๆในองค์กร) ซึ่งคำถามอิงตามนโยบายด้านการรักษาความปลอดภัยสารสนเทศ ISO 17799 โดยแบ่งคำถามเป็น 11 ข้อใหญ่ตามมาตรฐานดังกล่าว

3). <u>คำถามข้อมูลในการแสดงความคิดเห็น ด้านการวิเคราะห์ความเสี่ยงของการรักษาความปลอดภัยในองค์กร</u> โดยถามเฉพาะพนักงานที่มีหน้าที่ดูแลทางด้าน ระบบสารสนเทศหรือหน่วยงานทาง IT เท่านั้น ในส่วนนี้คำถามจะถูกแบ่งออกเป็น 3 ส่วนตามปัจจัยด้านความปลอดภัยของข้อมูลได้แก่ ด้าน Confidentiality – สิทธิในการเข้าถึงเข้ามูลต่างๆ, ด้าน Integrity – ความถูกต้องสมบูรณ์ของข้อมูล, ด้าน Availability - การเข้าถึงข้อมูลต่างๆได้เมื่อต้องการ

โดยคำถามทั้ง 3 ส่วนแบ่งคำถามในลักษณะแบบให้ผู้ตอบแสดงความคิดเห็นใน 2 มุมมองคือ

- ให้ประเมินความเป็นไปได้หรือโอกาสในการเกิดความเสี่ยง (Likelihood of risk) ต่อระบบข้อมูลสารสนเทศภายในองค์กร โอกาสที่จะเกิดเหตุการณ์อันก่อให้เกิดความเสี่ยงขององค์กร ซึ่งแบ่งออกเป็น 5 ระดับ และแต่ละระดับมีความหมายดังนี้

1. ระดับต่ำมากที่สุดหรือไม่เกิด หมายถึง เหตุการณ์นั้นๆแทบไม่มีโอกาสที่จะเกิดขึ้นในองค์กรหรือมีโอกาสที่จะเกิดในองค์กรได้ยาก เนื่องจากองค์กรมีระบบป้องกันที่มีประสิทธิภาพเพียงพอ

2. ระดับต่ำ หมายถึง เหตุการณ์นั้นๆ ไม่มีแนวโน้มในการเกิดแต่มีโอกาสหรือโอกาสนั้นสามารถเกิดได้ต่ำ เนื่องจากมีระบบป้องกันที่ดี

3. ระดับปานกลาง หมายถึง เหตุการณ์นั้นๆ พอจะมีโอกาสเกิดขึ้นในองค์กรได้เนื่องจากมีระบบป้องกันที่ดีแต่อาจพบข้อบกพร่องได้

4. ระดับสูง หมายถึง เหตุการณ์นั้นๆ มีโอกาสที่จะเกิดในองค์กรได้อย่างมากเนื่องจากมีระบบป้องกันที่ไม่มีประสิทธิภาพพอ

5. ระดับสูงมาก หมายถึง เหตุการณ์นั้นๆ มีโอกาสที่จะเกิดในองค์กรได้สูงมากหรือเนื่องจากไม่มีระบบป้องกันเลย

- ให้ประเมินระดับผลกระทบหรือความรุนแรงของความเสี่ยง (Impact level of risk) หากเกิดความเสี่ยงขึ้นในองค์กร กรณีที่เกิดเหตุการณ์ซึ่งก่อให้เกิดความเสี่ยงขึ้นในองค์กร โดยระดับผลกระทบหรือความรุนแรงของความเสี่ยงที่เกิดขึ้น จะแบ่งออกเป็น 5 ระดับ และแต่ละระดับมีความหมายดังนี้

1. ระดับต่ำสุด หมายถึง เหตุการณ์ที่เกิดขึ้นไม่ส่งผลกระทบต่อระบบและความมั่นคงขององค์กร หรือส่งผลเพียงเล็กน้อย องค์กรสามารถดำเนินธุรกิจต่อไปได้ตามปกติไม่มีผลกระทบต่อการดำเนินงาน

2. ระดับต่ำสุด หมายถึง เหตุการณ์ที่เกิดขึ้นกระทบต่อการดำเนินงานขององค์กรน้อยมาก ระบบผิดปกติบางครั้งบางคราว มูลค่าความเสียหายต่ำ

3. ระดับปานกลาง หมายถึง เหตุการณ์ที่เกิดขึ้นบ้าง และองค์กรยังสามารถดำเนินธุรกิจต่อได้ ระบบได้รับความเสียหายเล็กน้อย, ระบบผิดปกติเล็กน้อยหรือระบบที่ไม่ใช่ระบบหลักหรือสภาพแวดล้อมที่ไม่ใช่สภาพแวดล้อมหลักถูกทำลาย มูลค่าความเสียปานกลางแต่ต้องมีการเฝ้าสังเกตเหตุการณ์อยู่ตลอด

4. ระดับสูง หมายถึง เหตุการณ์ที่เกิดขึ้นมีผลต่อดำเนินธุรกิจขององค์กร ในแง่ของการทำงาน ระบบได้รับความกระทบกระเทือน, สูญเสียข้อมูล ก่อให้เกิดความผิดพลาดภายในองค์กร มูลค่าความเสียหายสูง ต้องหาวิธีป้องกัน ควบคุมและแก้ปัญหาเมื่อเกิดเหตุการณ์ขึ้น,

5. ระดับสูงมาก หมายถึง เหตุการณ์ที่เกิดขึ้นส่งผลกระทบต่อองค์กรอย่างมาก ธุรกิจเกิดการชะงักเนื่องจากระบบไม่สามารถทำงานได้, สูญเสียข้อมูลสำคัญ, ระบบถูกรบกวนหรือสภาพแวดล้อมถูกทำลายอย่างรุนแรง กระทบต่อธุรกิจ มูลค่าความเสียหายสูงมาก ต้องหาวิธีป้องกัน ควบคุมและแก้ปัญหาเมื่อเกิดเหตุการณ์ขึ้นโดยเร่งด่วน

แล้วนำมาปรับและให้คะแนนเพื่อใช้เมตริกซ์การประเมินความเสี่ยงแบบ 3x3 ตามตารางที่ 2.1 ในการประเมินความเสี่ยง

3.5 การเก็บรวบรวมข้อมูล

3.5.1 แหล่งข้อมูลปฐมภูมิ (Primary data)

1). แบบประเมินการดำเนินงานปัจจุบันเบื้องต้น (Check List)

เกี่ยวกับกระบวนการและรูปแบบการทำงาน รวมถึงเทคโนโลยีที่ใช้ในการนำมาจัดการด้านความปลอดภัยของข้อมูล เก็บโดยจัดทำแบบประเมินและทำการการสัมภาษณ์บุคลากรระดับผู้บริหารที่เกี่ยวข้องและดูแลโดยตรงทาง IT

2). แบบสอบถาม(Questionnaire)

เพื่อทำการสอบถามและสำรวจปัจจัยที่อาจเป็นความเสี่ยงในการรักษาความปลอดภัยขององค์กร เก็บโดยการจัดทำเป็นเอกสารและขออนุญาตจากผู้บริหาร ก่อนส่งให้กับพนักงานในองค์กรที่ทำการศึกษาในการตอบแบบศึกษา

3.5.2 แหล่งข้อมูลทุติยภูมิ (Secondary data)

1). หนังสือ ตำรา Web Site เอกสารทางวิชาการ บทความทางวิชาทั้งในประเทศและต่างประเทศ

2). งานวิจัยที่เกี่ยวข้อง กฎหมายและพระราชบัญญัติที่เกี่ยวข้อง

3.6 การวิเคราะห์ข้อมูล

จากการวิเคราะห์ข้อมูลที่มีทั้งวิธีการวิจัยเชิงพรรณนาในการหาค่าสถิติพื้นฐานของผู้ตอบแบบสอบถามโดยการคำนวณหาค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และ ค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) และวิธีการวิจัยเชิงสำรวจ เพื่อหาแนวทางในการพัฒนาและปรับปรุงเพื่อลดความเสี่ยง รวมถึงการหาปัจจัยความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศ เมื่อประมวลผลและวิเคราะห์ข้อมูลเสร็จ ผู้วิจัยจะนำข้อมูลมาวิเคราะห์ตามสมมติฐานเปรียบเทียบผล พร้อมจัดทำเอกสารรายงานสรุปผลที่ได้เป็นภาพรวมขององค์กรและเสนอแนวทาง ในการประยุกต์ใช้มาตรฐานด้านการรักษาความปลอดภัยข้อมูล ISO17799 กับการบริหารความเสี่ยง แก่องค์กรที่ให้บริการด้านการจัดซื้อจัดหาออนไลน์ที่ทำการสำรวจ