

สารบัญ

	หน้า
บทคัดย่อ	(1)
กิตติกรรมประกาศ	(2)
สารบัญตาราง	(10)
สารบัญภาพประกอบ	(14)
 บทที่	
1. บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการวิจัย	3
1.3 ขอบเขตของการวิจัย	3
1.4 ประโยชน์ที่คาดว่าจะได้รับ	3
2. กรอบแนวคิดทางทฤษฎีและงานวิจัยที่เกี่ยวข้อง (Literature review)	5
2.1 แนวคิดสำหรับการจัดการด้านความปลอดภัยของข้อมูล	5
2.1.1 ISMF 7 (Information Security Management Framework)	5
2.1.2 ISO27001/17799:2005	7
2.1.2.1 มาตรฐาน ISO27001/17799:2005	7
2.1.2.2 ประโยชน์ของ ISO27001/17799:2005	10
2.2 การบริหารความเสี่ยง (Risk Management)	10
2.2.1 มาตรฐาน NIST	11
2.2.1.1 มาตรฐาน NIST 800-30	11

2.3 การจัดซื้อออนไลน์ (e-Procurement).....	19
2.3.1 คำจำกัดความ.....	19
2.3.2 e-Procurement	20
2.3.2.1 องค์ประกอบหลัก.....	20
2.3.2.2 วัตถุประสงค์ของการจัดซื้อจัดหาออนไลน์.....	21
2.3.3 คุณสมบัติและหน้าที่หลักของผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์ (e-Marketplace Service Provider).....	21
2.4 กฎหมายที่เกี่ยวข้อง	22
2.4.1 พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544.....	22
2.4.2 ประกาศกระทรวงพาณิชย์ เรื่องการให้ผู้ประกอบการพาณิชย์กิจ ต้องจดทะเบียน.....	22
2.4.2.1 วัตถุประสงค์ของการจดทะเบียน.....	23
2.4.2.2 ผู้ที่มีหน้าที่จดทะเบียนพาณิชย์อิเล็กทรอนิกส์	23
2.4.2.3 ประโยชน์ของการจดทะเบียนพาณิชย์อิเล็กทรอนิกส์	23
2.5 ผลสำรวจทางสถิติ	24
2.6 งานวิจัยที่เกี่ยวข้อง.....	29
3. ระเบียบวิธีวิจัย (Methodology)	31
3.1 กรอบระเบียบวิธีวิจัย	31
3.2 แหล่งข้อมูลที่ใช้ศึกษา.....	33
3.2.1 แหล่งข้อมูลปฐมภูมิ	33
3.2.2 แหล่งข้อมูลทุติยภูมิ	33
3.3 ตัวแปรที่ใช้ในการวิจัย	33
3.3.1 ตัวแปรอิสระ.....	34
3.3.2 ตัวแปรตาม	34
3.4 เครื่องมือที่ใช้ในการวิจัย	35
3.4.1 การศึกษามาตรฐานISO17799.....	35
3.4.2 การใช้แบบประเมินเบื้องต้น (Check List).....	35

3.4.3	การใช้แบบสอบถาม (Questionnaire)	35
3.5	การเก็บรวบรวมข้อมูล	37
3.5.1	แหล่งข้อมูลปฐมภูมิ	37
3.5.2	แหล่งข้อมูลทุติยภูมิ	38
3.6	การวิเคราะห์ข้อมูล.....	38
4.	ผลการวิจัยและวิเคราะห์ข้อมูล.....	39
4.1	ผลการวิเคราะห์เชิงพรรณนา	39
4.1.1	ลักษณะประชากรของกลุ่มตัวอย่าง	39
4.1.2	ผลสำรวจความคิดเห็น ด้านการรักษาความปลอดภัยระบบ สารสนเทศในองค์กรตามมาตรฐาน ISO17799.....	46
4.1.2.1	ผลสำรวจด้าน นโยบายความมั่นคงปลอดภัยสำหรับ สารสนเทศ (Information security policy)	46
4.1.2.2	ผลสำรวจด้าน โครงสร้างทางด้านความมั่นคงปลอดภัย ภายในองค์กร (Internal organization) และที่เกี่ยวข้อง กับลูกค้าหรือหน่วยงานภายนอก (External parties)....	48
4.1.2.3	ผลสำรวจด้าน หน้าที่ความรับผิดชอบต่อทรัพย์สินของ องค์กร (Responsibility for assets) และการจัด หมวดหมู่สารสนเทศ (Information classification).....	49
4.1.2.4	ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยก่อนการ จ้างงาน (Prior to employment) และในระหว่างการจ้าง งาน (During employment)	50
4.1.2.5	ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยทาง กายภาพและสิ่งแวดล้อม (Physical and environmental security)	51
4.1.2.6	ผลสำรวจด้าน การบริหารจัดการด้านการสื่อสารและการ ดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)	52

4.1.2.7	ผลสำรวจด้าน การควบคุมการเข้าถึง (Access control)	54
4.1.2.8	ผลสำรวจด้าน การจัดหา การพัฒนา และการบำรุงรักษา ระบบสารสนเทศ (Information systems acquisition, development and maintenance)	56
4.1.2.9	ผลสำรวจด้าน การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยขององค์กร (Information security incident management).....	58
4.1.2.10	ผลสำรวจด้าน การบริหารความต่อเนื่องในการดำเนินงาน ขององค์กร (Business continuity management)	59
4.1.2.11	ผลสำรวจด้าน การปฏิบัติตามข้อกำหนด (Compliance)	60
4.1.3	ผลสำรวจความคิดเห็น ด้านการวิเคราะห์ความเสี่ยงของการรักษา ความปลอดภัยระบบสารสนเทศ.....	62
4.1.3.1	ความเสี่ยงด้าน การรักษาความลับและสิทธิในการเข้าถึง ข้อมูล.....	63
4.1.3.2	ความเสี่ยงด้าน ความถูกต้องและความครบถ้วนของ ข้อมูล.....	67
4.1.3.3	ความเสี่ยงด้าน การเข้าถึงข้อมูลต่างๆได้เมื่อต้องการใช้ งาน	70
4.2	ผลการทดสอบสมมุติฐาน	76
4.2.1	สมมุติฐานข้อที่ 1	76
4.2.1.1	ผลสำรวจด้าน นโยบายความมั่นคงปลอดภัยสำหรับ สารสนเทศ (Information security policy)	76
4.2.1.2	ผลสำรวจด้าน โครงสร้างทางด้านความมั่นคงปลอดภัย ภายในองค์กร (Internal organization) และที่เกี่ยวข้อง กับลูกค้าหรือหน่วยงานภายนอก (External parties)	79
4.2.1.3	ผลสำรวจด้าน หน้าที่ความรับผิดชอบต่อทรัพย์สินของ องค์กร (Responsibility for assets) และการจัด หมวดหมู่สารสนเทศ (Information classification)	83

4.2.1.4	ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการจ้างงาน (During employment)	85
4.2.1.5	ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)	89
4.2.1.6	ผลสำรวจด้าน การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)	93
4.2.1.7	ผลสำรวจด้าน การควบคุมการเข้าถึง (Access control)	100
4.2.1.8	ผลสำรวจด้าน การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)	108
4.2.1.9	ผลสำรวจด้าน การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)	110
4.2.1.10	ผลสำรวจด้าน การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)	113
4.2.1.11	ผลสำรวจด้าน การปฏิบัติตามข้อกำหนด (Compliance)	115
4.2.2	สมมติฐานข้อที่ 2	118
4.2.2.1	ผลสำรวจด้าน นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)	118
4.2.2.2	ผลสำรวจด้าน โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization) และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)	121
4.2.2.3	ผลสำรวจด้าน หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) และการจัดหมวดหมู่สารสนเทศ (Information classification)	123

4.2.2.4	ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการจ้างงาน (During employment)	125
4.2.2.5	ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)	128
4.2.2.6	ผลสำรวจด้าน การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)	131
4.2.2.7	ผลสำรวจด้าน การควบคุมการเข้าถึง (Access control)	137
4.2.2.8	ผลสำรวจด้าน การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)	143
4.2.2.9	ผลสำรวจด้าน การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)	145
4.2.2.10	ผลสำรวจด้าน การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)	147
4.2.2.11	ผลสำรวจด้าน การปฏิบัติตามข้อกำหนด (Compliance)	149
4.3	การวิเคราะห์ความเสี่ยง.....	152
4.3.1	การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด	152
4.3.2	การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้	153
4.3.3	การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล	154
4.3.4	การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม	155
4.3.5	ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้ ..	156
4.3.6	Router / Firewall เสียทำให้ไม่สามารถใช้งานได้	157
4.3.7	ฐานข้อมูล (database) ถูกขัดจังหวะการทำงาน (corrupt) เนื่องจากฮาร์ดแวร์และซอฟต์แวร์ทำงานผิดพลาด	158

4.4 การวิเคราะห์แนวทางปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยด้าน	
สารสนเทศ ISO/IEC 17799:2005	160
4.4.1 การควบคุมการเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด	161
4.4.2 การควบคุมการสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้	163
4.4.3 การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล	165
4.4.4 การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม	167
4.4.5 ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้ ..	170
4.4.6 Router / Firewall เสียทำให้ไม่สามารถใช้งานได้	173
4.4.7 ฐานข้อมูล (database) ถูกขัดจังหวะการทำงาน (corrupt)	175
เนื่องจากฮาร์ดแวร์และซอฟต์แวร์ทำงานผิดพลาด	175
5. สรุปผลการวิจัยและข้อเสนอแนะ	177
5.1 สรุปผลการวิจัย	177
5.2 ข้อเสนอแนะเกี่ยวกับงานวิจัย	184
ภาคผนวก	
ก. ตัวอย่างแบบประเมินองค์กรเบื้องต้นตาม มาตรฐาน ISO17799	187
ข. ตัวอย่างแบบสอบถาม	192
บรรณานุกรม	200
ประวัติการศึกษา	201