

สารบัญตาราง

ตารางที่		หน้า
2.1	ระดับของโอกาสในการเกิด.....	49
2.2	ระดับของผลกระทบที่เกิดขึ้น	50
2.3	ค่าความเสี่ยง.....	51
2.4	คะแนนตามระดับความเสี่ยง	51
2.5	ระดับของผลกระทบที่เกิดขึ้น	52
2.6	หลักการในการประเมินความเสี่ยง	56
2.7	หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์.....	61
2.8	บทกำหนดโทษ.....	62
2.9	ความตื่นตัวของภาคธุรกิจ ในการจัดทำ Privacy Policy.....	66
4.1	ร้อยละของกลุ่มตัวอย่าง จำแนกตามเพศของผู้ตอบแบบสอบถาม.....	82
4.2	ร้อยละของกลุ่มตัวอย่าง จำแนกตามอายุของผู้ตอบแบบสอบถาม.....	83
4.3	ร้อยละของกลุ่มตัวอย่าง จำแนกตามวุฒิการศึกษาของผู้ตอบแบบสอบถาม..	84
4.4	ร้อยละของกลุ่มตัวอย่าง จำแนกตามประสบการณ์ทำงานของผู้ตอบ	85
	แบบสอบถาม.....	
4.5	ร้อยละของกลุ่มตัวอย่าง จำแนกตามประสบการณ์ทำงานองค์กรในปัจจุบัน	
	ของผู้ตอบแบบสอบถาม.....	86
4.6	ร้อยละของกลุ่มตัวอย่าง จำแนกตามตำแหน่งงานในองค์กรของผู้ตอบ.....	
	แบบสอบถาม.....	87
4.7	ร้อยละของกลุ่มตัวอย่าง จำแนกตามหน่วยงานที่สังกัดของผู้ตอบ	
	แบบสอบถาม.....	88
4.8	ผลการสำรวจ หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัย	
	(Security Policy).....	89
4.9	ผลการสำรวจ หมวดที่ 2 : โครงสร้างทางด้านความมั่นคงปลอดภัย	
	สำหรับองค์กร (Organization of information security)	93
4.10	ผลการสำรวจ หมวดที่ 3 ด้านการบริหารจัดการทรัพย์สินขององค์กร	
	(Asset management)	95

4.11	ผลการสำรวจ หมวดที่ 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร	
	(Human resources security)	98
4.12	ผลการสำรวจ หมวดที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพ	
	และสิ่งแวดล้อม (Physical and environmental security)	103
4.13	ผลการสำรวจ หมวดที่ 6 การบริหารจัดการด้านการสื่อสารและ.....	
	การดำเนินงานของเครือข่ายสารสนเทศ (Communications and.....	
	operations management).....	112
4.14	ผลการสำรวจ หมวดที่ 7 การควบคุมการเข้าถึง (Access control)	119
4.15	ผลการสำรวจ หมวดที่ 8 การจัดหา การพัฒนา และการบำรุงรักษา.....	
	ระบบสารสนเทศ (Information systems acquisition, development	
	and maintenance).....	126
4.16	ผลการสำรวจ หมวดที่ 9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้อง.....	
	กับความมั่นคงปลอดภัยขององค์กร (Information security incident	
	management)	130
4.17	ผลการสำรวจ หมวดที่ 10 การบริหารความต่อเนื่องในการดำเนินงานของ....	
	องค์กร (Business continuity management).....	132
4.18	ผลการสำรวจ หมวดที่ 11 การปฏิบัติตามข้อกำหนด (Compliance)	135
4.19	ผลการสำรวจความคิดเห็นของพนักงาน หมวดที่ 1 ด้านนโยบาย	
	ความมั่นคงปลอดภัยสำหรับสารสนเทศ	137
4.20	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 2 ด้านโครงสร้าง	
	ทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal Organization)	
	และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties).....	138
4.21	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 3 ด้านหน้าที่.....	
	ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets)	
	และการจัดหมวดหมู่สารสนเทศ (Information classification)	139
4.22	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 4 ด้านการสร้าง.....	
	ความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment.....	
	และในระหว่างการ จ้างงาน (During employment)	140

4.23	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 5 ด้านการสร้าง..... ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security).....	142
4.24	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 6 ด้านการบริหาร จัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ ขององค์กร (Communication and Operations Management).....	143
4.25	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 7 ด้าน การควบคุม การเข้าถึง (Access Control)	145
4.26	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 8 ด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition , Development and Maintenance).....	147
4.27	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 9 ด้านการบริหาร จัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management).....	149
4.28	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 10 ด้านการบริหาร ความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)	151
4.29	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 11 ด้านการปฏิบัติ..... ตามข้อกำหนด (Compliance)	152
4.30	เมตริกซ์ระดับความเสี่ยง 5 x 5	154
4.31	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง ความเสี่ยงด้าน Confidentiality	155
4.32	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง ความเสี่ยงด้าน Availability (เฉพาะพนักงาน IT).....	157
4.33	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง ความเสี่ยงด้าน Confidentiality (เฉพาะพนักงาน IT).....	164
4.34	ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง ความเสี่ยงด้าน Integrity (เฉพาะพนักงาน IT).....	167
4.35	ตารางแสดงความสัมพันธ์ระหว่างความเสี่ยง กับมาตรฐาน ISO/IEC27001..	174

5.1	สรุปผลสำรวจการปฏิบัติตามกรอบ ISO/IEC 27001 ขององค์กรฯ ในปัจจุบัน	180
5.2	สรุปผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง ที่มีต่อการดำเนินงาน ตามกรอบ ISO/IEC27001 ขององค์กรในปัจจุบัน	182
5.3	ลำดับเหตุการณ์ความเสี่ยงทั้ง 3 ด้านทั้งหมดขององค์กร โดยเรียงลำดับจาก..... ระดับความเสี่ยงสูงไปหาความเสี่ยงน้อย.....	184
5.4	มาตรการในการลดความเสี่ยงในระดับสูง	187
5.5	มาตรการในการลดความเสี่ยงในระดับปานกลาง	193
5.6	มาตรการในการลดความเสี่ยงในระดับต่ำ.....	195