

สารบัญ

บทที่	หน้า
1 บทนำ.....	1
ความเป็นมาของปัญหา.....	1
จุดมุ่งหมายของการวิจัย.....	2
ความสำคัญของการวิจัย.....	3
ขอบเขตของการวิจัย.....	3
นิยามศัพท์เฉพาะ.....	4
2 เอกสารและงานวิจัยที่เกี่ยวข้อง.....	7
พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. 2546.....	7
พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทาง อิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549.....	8
หลักเกณฑ์การประเมินการบริหารความเสี่ยง TRIS ประจำปีบัญชี 2550 และ 2551	9
การบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC 27001 2005.....	10
การประเมินความเสี่ยง (Risk Assessment) ตามมาตรฐาน NIST SP 800-30. งานวิจัยที่เกี่ยวข้อง	15
3 วิธีดำเนินการวิจัย.....	27
วิธีการศึกษาและพัฒนาระบบงาน.....	27
เครื่องมือที่ใช้ในการพัฒนาระบบสารสนเทศ.....	32

สารบัญ (ต่อ)

บทที่	หน้า
4 ผลการวิจัย.....	35
การกำหนดเกณฑ์การประเมินความเสี่ยงสารสนเทศ.....	35
การวิเคราะห์ ออกแบบ และพัฒนาระบบสารสนเทศเพื่อสนับสนุนการประเมิน ความเสี่ยงสารสนเทศหน่วยงานรัฐวิสาหกิจ.....	44
การออกแบบหน้าจอระบบ.....	75
ผลการพัฒนาระบบสารสนเทศเพื่อสนับสนุนการประเมินความเสี่ยงสารสนเทศ หน่วยงานรัฐวิสาหกิจ.....	73
การประเมินงบประมาณการพัฒนาระบบสารสนเทศ.....	83
ความเป็นไปได้ทางเศรษฐศาสตร์ (Economic).....	87
5 บทสรุป.....	91
สรุปผลการวิจัย.....	91
อภิปรายผลการวิจัย.....	92
ข้อเสนอแนะ.....	94
บรรณานุกรม.....	96
ประวัติผู้ศึกษาค้นคว้า.....	98

สารบัญตาราง

ตาราง		หน้า
1	แสดงด้านบุคคลที่ได้รับผลกระทบ.....	๑
2	แสดงด้านความปลอดภัยในชีวิตและสุขภาพของผู้ใช้งาน.....	10
3	แสดงด้านมูลค่าความเสียหายโดยตรงของผู้ใช้บริการ.....	10
4	แสดงวัตถุประสงค์การควบคุม (Control Objectives).....	12
5	แสดงนิยามของระดับความเป็นไปได้ (Likelihood Definitions).....	13
6	แสดงนิยามของระดับของความรุนแรง (Impact Definitions).....	13
7	แสดงเมตริกซ์ระดับความเสี่ยง 3x3.....	20
8	แสดงนิยามของระดับของความเสียหายและสิ่งที่ต้องปฏิบัติ (Risk Scale and Necessary Actions).....	21
9	แสดงการกำหนดสถานะแวดล้อม.....	22
10	แสดงตัวอย่างการหาสาเหตุที่มาของความเสี่ยง.....	23
11	แสดงตัวอย่างการกำหนดกลุ่มและคำอธิบายความเสี่ยงเพื่อสร้างตารางใช้ วิเคราะห์.....	24
12	แสดงตัวอย่างการสร้างตาราง (Matrix).....	24
13	แสดงตัวอย่างขั้นตอนในการระบุและจัดลำดับความเสี่ยงที่เลือกไว้ และสร้าง ทะเบียน.....	25
14	แสดงขั้นตอนการควบคุมการรับมือกับความเสี่ยง.....	25
15	แสดงการจัดหมวดหมู่สินทรัพย์และตัวอย่าง.....	36
16	แสดงระดับผลกระทบต่อการรักษาความลับของข้อมูลสารสนเทศ (Confidentiality).....	37
17	แสดงระดับผลกระทบต่อความมั่นคงของข้อมูลสารสนเทศ (Integrity).....	38
18	แสดงระดับผลกระทบต่อความพร้อมใช้ของข้อมูลสารสนเทศ (Availability).....	38
19	แสดงผลรวมค่าน้ำหนักของผลกระทบ.....	39
20	แสดงระดับมูลค่าสินทรัพย์.....	39
21	แสดงผลกระทบด้านมูลค่าความสูญเสีย.....	40
22	แสดงผลกระทบด้านผู้ให้บริการ.....	40

สารบัญตาราง (ต่อ)

ตาราง		หน้า
23	แสดงผลกระทบด้านบริการ.....	41
24	แสดงผลกระทบด้านทางกฎหมาย.....	41
25	แสดงการจัดระดับผลกระทบต่อธุรกิจ.....	42
26	แสดงประเมินความเป็นไปได้ที่จะเกิดภัยคุกคาม (Vulnerability).....	42
27	แสดงระดับความเสี่ยง.....	44
28	แสดงคำอธิบายแผนภาพกระแสข้อมูลในระดับ Context.....	45
29	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 1 กำหนดสิทธิ์ผู้ใช้งาน ระบบ.....	45
30	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 2 บันทึกข้อมูล.....	47
31	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 3 ประมวลผลเพื่อประเมิน ความเสี่ยง.....	43
32	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 4 จัดทำรายงาน.....	43
33	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 1.1 ลงทะเบียนผู้ใช้งาน ระบบ.....	51
34	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 1.2 จัดทำรายงานผู้ใช้งาน ระบบ.....	51
35	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 1.3 ตรวจสอบสิทธิ์การใ้ งานระบบ.....	52
36	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 3.1 ตรวจสอบโอกาสการ เกิดภัยคุกคาม.....	53
37	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 3.2 วิเคราะห์ผลกระทบ.....	53
38	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 3.3 คำนวณระดับความ เสี่ยง.....	54
39	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 3.4 เลือกรูปวิธีการควบคุม.....	54
40	แสดงคำอธิบายการประมวลผลของกระบวนการงานที่ 4.1 จัดทำรายงานวิธีการ ควบคุมความเสี่ยงต่อสินทรัพย์.....	57

สารบัญตาราง (ต่อ)

ตาราง		หน้า
41	แสดงคำอธิบายการประมวลผลของกระบวนการที่ 4.2 จัดทำรายงานผลการประเมินความเสี่ยง.....	57
42	แสดงคำอธิบายการประมวลผลของกระบวนการที่ 4.3 จัดทำรายงานสินทรัพย์ภัยคุกคาม ช่องโหว่ แผนควบคุม และระดับความสำคัญของสินทรัพย์....	58
43	แสดงสรุป Entity และคำอธิบาย.....	60
44	แสดงการออกแบบฐานข้อมูล.....	67
45	แสดงฐานข้อมูล SecurityConcern	68
46	แสดงฐานข้อมูล SecurityTerm.....	68
47	แสดงฐานข้อมูล AssetTpye	68
48	แสดงฐานข้อมูล Asset	68
49	แสดงฐานข้อมูล People.....	69
50	แสดงฐานข้อมูล Department	70
51	แสดงฐานข้อมูล Position.....	70
52	แสดงฐานข้อมูล PeopleRole.....	70
53	แสดงฐานข้อมูล Asset_Concern.....	70
54	แสดงฐานข้อมูล AssetValue	71
55	แสดงฐานข้อมูล Threat	71
56	แสดงฐานข้อมูล Vulner	72
57	แสดงฐานข้อมูล ThreatVulner	72
58	แสดงฐานข้อมูล Likelihood	72
59	แสดงฐานข้อมูล ImpactConcern	72
60	แสดงฐานข้อมูล ImpactTerm	73
61	แสดงฐานข้อมูล AssetsImpact	73
62	แสดงฐานข้อมูล AssetsImpValue	73
63	แสดงฐานข้อมูล RiskLevel	74
64	แสดงฐานข้อมูล AnnexA.....	74

สารบัญตาราง (ต่อ)

ตาราง		หน้า
65	แสดงฐานข้อมูล RiskAssessment	74
66	แสดงตารางแสดงการประเมินงบประมาณการพัฒนาระบบสารสนเทศ.....	83
67	แสดงรายการวิเคราะห์หาค่า Total Unadjusted Function Points (TUFPP).....	84
68	แสดงรายการวิเคราะห์หาค่า Project Complexity (PC).....	85
69	แสดงค่าใช้จ่ายสำหรับอุปกรณ์.....	87

สารบัญภาพ

ภาพ		หน้า
1	หลักการ Plan-Do-Check-Act (PDCA Model).....	12
2	กิจกรรมการประเมินความเสี่ยงตามมาตรฐาน NIST SP 800-30.....	31
3	ลำดับขั้นตอนของแผนงาน (Gantt Chart).....	33
4	การหาค่าระดับผลกระทบต่อธุรกิจ.....	42
5	แผนภาพกระแสข้อมูลระดับ Context (Data Flow Diagram: Context Level)..	46
6	แผนภาพกระแสข้อมูลระดับ Level 0 (Data Flow Diagram: Level 0).....	50
7	แผนภาพกระแสข้อมูลในระดับ Level 1 ของกระบวนการที่ 1 (Data Flow Diagram: Level 1 Process 1).....	52
8	แผนภาพกระแสข้อมูลในระดับ Level 1 ของกระบวนการที่ 3 (Data Flow Diagram: Level 1 Process 3).....	53
9	แผนภาพกระแสข้อมูลในระดับ Level 1 ของกระบวนการที่ 4 (Data Flow Diagram: Level 1 Process 4).....	53
10	ความสัมพันธ์ระหว่างสินทรัพย์กับประเภทสินทรัพย์.....	61
11	ความสัมพันธ์ระหว่างประเภทความสำคัญของสินทรัพย์กับค่าความสำคัญของ สินทรัพย์.....	61
12	ความสัมพันธ์ระหว่างสินทรัพย์กับประเภทความสำคัญของสินทรัพย์.....	61
13	ความสัมพันธ์ระหว่างบุคคลกับแผนก.....	62
14	ความสัมพันธ์ระหว่างบุคคลกับตำแหน่ง.....	62
15	ความสัมพันธ์ระหว่างบุคคลกับสิทธิ์การใช้งาน.....	62
16	ความสัมพันธ์ระหว่างสินทรัพย์กับความเป็นไปได้ที่จะเกิดภัยคุกคาม.....	63
17	ความสัมพันธ์ระหว่างผลกระทบกับประเภทของผลกระทบ.....	63
18	ความสัมพันธ์ระหว่างช่องโหว่กับภัยคุกคามต่อเหตุการณ์ความเสี่ยง.....	64
19	ความสัมพันธ์ระหว่างสินทรัพย์กับเหตุการณ์ความเสี่ยง.....	64
20	ความสัมพันธ์ระหว่างสินทรัพย์กับระดับความเสี่ยง.....	64
21	ความสัมพันธ์ระหว่างสินทรัพย์กับการประเมินความเสี่ยง.....	65
22	ความสัมพันธ์ระหว่างการประเมินความเสี่ยงกับมาตรฐานควบคุม.....	65

สารบัญภาพ (ต่อ)

ภาพ		หน้า
23	แผนภาพความสัมพันธ์ระหว่างข้อมูล (Entity Relationship Diagram) ระบบสารสนเทศเพื่อสนับสนุนการประเมินความเสี่ยงสารสนเทศ หน่วยงานรัฐวิสาหกิจ.....	66
24	หน้าจอลำสำหรับการเข้าสู่ระบบ.....	75
25	หน้าจอหลักสำหรับการใช้งาน.....	76
26	หน้าจอลำสำหรับการลงทะเบียนสิทธิ์.....	76
27	หน้าจอลำสำหรับการลงทะเบียนผู้ใช้งาน.....	77
28	ตัวอย่างรายงานสรุปข้อมูลรายการสิทธิ์.....	77
29	หน้าจอลำสำหรับการเข้าสู่ระบบ.....	78
30	หน้าจอหลักสำหรับการใช้งาน.....	78
31	หน้าจอลำสำหรับการลงทะเบียนสิทธิ์.....	79
32	หน้าจอลำสำหรับการลงทะเบียนผู้ใช้งาน.....	79
33	หน้าจอลำสำหรับการประเมินความเสี่ยงของสิทธิ์.....	80
34	หน้าจอลำสำหรับการอนุมัติผลการประเมินความเสี่ยง.....	80
35	หน้าจอลำสำหรับการออกรายงาน.....	81
36	หน้าจอรายงานบัญชีสิทธิ์.....	81
37	หน้าจอรายงานบัญชีสิทธิ์แยกตามประเภท.....	82
38	หน้าจอรายงานผลการประเมินความเสี่ยงสารสนเทศ.....	82
39	การวิเคราะห์ความเป็นไปได้ในทางเศรษฐศาสตร์.....	89