



การไฟฟ้าส่วนภูมิภาคจังหวัดศรีสะเกษ

รายงานผลการประเมินความเสี่ยง
(Risk Assessment Report)

จัดทำโดย

คณะกรรมการ BCM การไฟฟ้าส่วนภูมิภาคจังหวัดศรีสะเกษ



รายละเอียดเอกสาร

ชื่อโครงการ	การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM)
ชื่อเอกสาร	รายงานผลการประเมินความเสี่ยง (Risk Assessment Report)
จัดทำโดย	คณะทำงาน BCM การไฟฟ้าส่วนภูมิภาคจังหวัดศรีสะเกษ

ประวัติการปรับปรุงเอกสาร

ครั้งที่	ผู้ดำเนินการ	วันที่มีผลบังคับใช้	รายละเอียด
1	คณะทำงาน BCM กฟจ.ศก.	27 มิ.ย. 2559	ออกเอกสารครั้งแรก
2	คณะทำงาน BCM กฟจ.ศก.	22 มิ.ย. 2560	ทบทวนปรับปรุงแผนประจำปี 2560
3	คณะทำงาน BCM กฟจ.ศก.	15 มิ.ย. 2561	ทบทวนปรับปรุงแผนประจำปี 2561
4	คณะทำงาน BCM กฟจ.ศก.	12 มิ.ย. 2562	ทบทวนปรับปรุงแผนประจำปี 2562

หมายเหตุ: หากเอกสารฉบับนี้ไม่ได้รับการทบทวนและปรับปรุงเป็นระยะเวลานานกว่า 12 เดือน เอกสารฉบับนี้อาจไม่สามารถนำไปใช้ได้อย่างมีประสิทธิภาพ



สารบัญ

หน้า

บทนำ.....	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
วัตถุประสงค์	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
ขอบเขต	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
วิธีการประเมินความเสี่ยง	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
การระบุภัยคุกคาม	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
การประเมินและจัดลำดับความเสี่ยง.....	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
หลักเกณฑ์การประเมินความเสี่ยง	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
ผลกระทบ (Impact)	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
โอกาสที่จะเกิด (Likelihood).....	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
คำจำกัดความของภัยคุกคาม	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
สรุปผลการประเมินความเสี่ยง.....	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า
ภัยคุกคามที่จัดทำแผนตอบโต้ภาวะฉุกเฉิน	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า4
ภัยคุกคามที่ต้องจัดทำมาตรการควบคุมเพิ่มเติม	14
การควบคุมที่มีอยู่ในปัจจุบัน	ผิดพลาด! ไม่ได้กำหนดที่คั่นหน้า



บทนำ

ตามแนวคิด วิธีการ และแผนการทำงานสำหรับโครงการพัฒนาระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) กำหนดให้ดำเนินการศึกษาและทำความเข้าใจองค์กร รวมถึงการประเมินความเสี่ยง (Risk Assessment) เพื่อระบุและประเมินภัยคุกคามที่อาจส่งผลกระทบต่อ การดำเนินธุรกิจอย่างต่อเนื่อง ตลอดจนการจัดทำข้อเสนอแนะเพื่อลดโอกาสที่จะเกิดและผลกระทบจากภัยคุกคาม และพิจารณาเลือกภัยคุกคามที่สำคัญอันเป็นผลจากการวิเคราะห์และจัดลำดับความเสี่ยงเพื่อจัดทำแผนตอบสนองอุบัติการณ์

การประเมินความเสี่ยง (Risk Assessment) ซึ่งอ้างอิงมาตรฐาน ISO 22301: 2012 และคู่มือการบริหารความเสี่ยงฉบับปรับปรุง 2560 ของการไฟฟ้าส่วนภูมิภาคเป็นแนวทาง โดยดำเนินการเป็นไปในลักษณะของการประชุมเชิงปฏิบัติการ (Workshop) ผู้รับผิดชอบของสำนักงานการไฟฟ้าส่วนภูมิภาคจตุรรวมงาน ได้สรุปผลการประเมินความเสี่ยงและรวบรวมข้อเสนอแนะเพื่อเป็นแนวทางในการลดโอกาสที่จะเกิดและผลกระทบจากภัยคุกคามไว้ในรายงานฉบับนี้



วัตถุประสงค์

- เพื่อระบุและประเมินภัยคุกคามที่อาจส่งผลกระทบต่อการดำเนินธุรกิจอย่างต่อเนื่องของ การไฟฟ้าจุฬารวมงาน
- เพื่อเป็นแนวทางในการลดโอกาสที่จะเกิดและผลกระทบจากภัยคุกคาม
- เพื่อพิจารณาเลือกภัยคุกคามที่สำคัญเพื่อจัดทำแผนตอบสนองอุบัติการณ์

ขอบเขต

ขอบเขตของการประเมินความเสี่ยงครอบคลุมกระบวนการหลักของ การไฟฟ้าจุฬารวมงาน ดังต่อไปนี้

ลำดับ	กระบวนการ	MTPD	RTO	RPO	MAL
1	งานแก้ไขการจ่ายกระแสไฟฟ้าขัดข้อง	4 ชั่วโมง	3 ชั่วโมง	24 ชั่วโมง	50%
2	งานควบคุมการจ่ายกระแสไฟฟ้า	4 ชั่วโมง	3 ชั่วโมง	24 ชั่วโมง	100%
3	งานรับชำระค่าไฟ (รายย่อย-รายใหญ่)	24 ชั่วโมง	24 ชั่วโมง	4 ชั่วโมง	100%
4	งานจดหน่วยและแจ้งหนี้ค่าไฟ (รายย่อย)	24 ชั่วโมง	24 ชั่วโมง	24 ชั่วโมง	100%
5	งานจดหน่วยและแจ้งหนี้ค่าไฟ (รายใหญ่)	24 ชั่วโมง	24 ชั่วโมง	24 ชั่วโมง	100%
6	งานรับเรื่องขอติดตั้งมิเตอร์ใหม่	48 ชั่วโมง	24 ชั่วโมง	24 ชั่วโมง	100%
7	งานติดตั้งมิเตอร์	48 ชั่วโมง	24 ชั่วโมง	24 ชั่วโมง	100%



วิธีการประเมินความเสี่ยง

การประเมินความเสี่ยง (Risk Assessment) ซึ่งมีวัตถุประสงค์เฉพาะสำหรับโครงการบริหารธุรกิจให้เกิดความต่อเนื่อง (BCM) โดยอ้างอิงตามมาตรฐาน ISO 22301: 2012 และคู่มือการบริหารความเสี่ยงฉบับปรับปรุง 2560 ของ กฟภ. บางส่วน มีวิธีการดังต่อไปนี้

การระบุภัยคุกคาม

การระบุภัยคุกคามที่สำคัญที่เกิดขึ้นในปัจจุบันและอาจจะเกิดขึ้นในอนาคต หมายถึง ความเสียหายหรือเหตุการณ์ใดๆ ที่ส่งผลกระทบต่อการทำงานของธุรกิจอย่างต่อเนื่อง โดยภัยคุกคามที่ถูกระบุ จะขึ้นอยู่กับลักษณะของกระบวนการหลัก โดยอาจคำนึงถึงความเสี่ยงโดยทั่วไปด้านความต่อเนื่องทางธุรกิจที่รวบรวมโดยสถาบันอันเป็นที่ยอมรับในระดับสากล เช่น Business Continuity Institute (BCI) เป็นต้น

ผู้รับผิดชอบจะต้องร่วมกับการระบุภัยคุกคาม โดยพิจารณาปัจจัยทั้งจากภายในองค์กร เช่น วัฒนธรรม โครงสร้างองค์กร บุคลากร เป็นต้น และจากภายนอกองค์กร เช่น การเมือง สภาวะเศรษฐกิจ และระบบเทคโนโลยีสารสนเทศ เป็นต้น

การประเมินและจัดลำดับความเสี่ยง

การประเมินและวัดระดับความเสี่ยงเป็นขั้นตอนที่ช่วยในการจัดลำดับความเสี่ยง โดยเรียงลำดับความเสี่ยงสูงสุดไปจนถึงความเสี่ยงต่ำสุด การประเมินระดับความเสี่ยงจะอาศัยพื้นฐานในการพิจารณาความสัมพันธ์ของผลกระทบ (Impact) และโอกาสที่จะเกิด (Likelihood) ตามหลักเกณฑ์การประเมินความเสี่ยงที่ได้ตกลงร่วมกัน และสามารถคำนวณได้จาก ระดับความเสี่ยง = โอกาสที่จะเกิด x ผลกระทบ

การจัดลำดับความเสี่ยงควรกำหนดเงื่อนไขที่ใช้ในการจัดลำดับความเสี่ยงและจัดลำดับความเสี่ยงจากมากไปหาน้อย เพื่อใช้ประโยชน์ในการจัดทำข้อเสนอแนะเพื่อลดโอกาสที่จะเกิดและผลกระทบจากภัยคุกคาม และพิจารณาเลือกภัยคุกคามที่สำคัญเพื่อจัดทำแผนตอบสนองอุบัติการณ์

การประเมินระดับความเสี่ยงแบ่งออกเป็น 3 ระดับ ดังนี้

ระดับความเสี่ยง	คำอธิบาย	การจัดการความเสี่ยง
สีเขียว (ต่ำ)	ความเสี่ยงอยู่ในระดับต่ำ (Score 1-4)	สามารถยอมรับความเสี่ยงได้ แต่ต้องมีมาตรการควบคุมที่เหมาะสม และดำเนินการตามมาตรการควบคุมนั้นอย่างสม่ำเสมอ
สีเหลือง (ปานกลาง)	ความเสี่ยงอยู่ในระดับปานกลาง (Score 5-12)	องค์กรต้องจัดทำแผนการตอบโต้ภาวะฉุกเฉิน และต้องหามาตรการควบคุมเพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (ระดับต่ำ) ในกรณีโอกาสต่ำมากและผลกระทบสูงมาก ซึ่งไม่สามารถลดผลกระทบได้แล้ว ให้ไปดำเนินการ ตามมาตรการควบคุมนั้นอย่างสม่ำเสมอ



ระดับความเสี่ยง	คำอธิบาย	การจัดการความเสี่ยง
สีแดง (สูงมาก)	ความเสี่ยงอยู่ในระดับสูงมาก (Score 13-25)	องค์กรต้องจัดทำแผนการตอบโต้ภาวะฉุกเฉินและต้องหามาตรการควบคุมเพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (ระดับต่ำ) อย่างเร่งด่วนทันที

ระดับความเสี่ยง (Risk Matrix)

เกณฑ์การจัดการความเสี่ยง						
ผลกระทบ	5	ปานกลาง (5)	ปานกลาง (10)	สูงมาก (15)	สูงมาก (20)	สูงมาก (25)
	4	ต่ำ (4)	ปานกลาง (8)	ปานกลาง (12)	สูงมาก (16)	สูงมาก (20)
	3	ต่ำ (3)	ปานกลาง (6)	ปานกลาง (9)	ปานกลาง (12)	สูงมาก (15)
	2	ต่ำ (2)	ต่ำ (4)	ปานกลาง (6)	ปานกลาง (8)	ปานกลาง (10)
	1	ต่ำ (1)	ต่ำ (2)	ต่ำ (3)	ต่ำ (4)	ปานกลาง (5)
		1	2	3	4	5
		โอกาส				

หลักเกณฑ์การประเมินความเสี่ยง

หลักเกณฑ์ที่ใช้สำหรับการประเมินความเสี่ยง ซึ่งอาศัยพื้นฐานในการพิจารณาความสัมพันธ์ของผลกระทบ (Impact) และโอกาสที่จะเกิด (Likelihood) โดยตกลงร่วมกันดังนี้

ผลกระทบ (Impact)

คะแนน	ผลกระทบ	ความหมาย
1	ต่ำมาก	การดำเนินงานหยุดชะงักเป็นเวลาน้อยกว่า 1 ชั่วโมง
2	ต่ำ	การดำเนินงานหยุดชะงักเป็นเวลามากกว่า 1 แต่ไม่เกิน 2 ชั่วโมง
3	ปานกลาง	การดำเนินงานหยุดชะงักเป็นเวลามากกว่า 2 แต่ไม่เกิน 4 ชั่วโมง
4	สูง	การดำเนินงานหยุดชะงักเป็นเวลามากกว่า 4 แต่ไม่เกิน 8 ชั่วโมง
5	สูงมาก	การดำเนินงานหยุดชะงักเป็นเวลามากกว่า 8 ชั่วโมง



โอกาสที่จะเกิด (Likelihood)

คะแนน	โอกาสที่จะเกิด	ความหมาย
1	ต่ำมาก	1 - 20% ทางสถิติ หรือ ความถี่ 0 ครั้ง/ปี
2	ต่ำ	21 - 40% ทางสถิติ หรือ ความถี่ 1 ครั้ง/ปี
3	ปานกลาง	41 - 60% ทางสถิติ หรือ ความถี่ 2 - 3 ครั้ง/ปี
4	สูง	61 - 80% ทางสถิติ หรือ ความถี่ 4 - 5 ครั้ง/ปี
5	สูงมาก	81 - 100% ทางสถิติ หรือ ความถี่มากกว่า 5 ครั้ง/ปี



ผลการประเมินความเสี่ยง

จากการประชุมเชิงปฏิบัติการ (Workshop) และการประเมินความเสี่ยงโดยใช้วิธีการลงความเห็นของผู้ร่วมประเมินความเสี่ยงซึ่งเป็นเจ้าของกระบวนการที่ได้รับผลกระทบจากภัยคุกคาม สามารถสรุปผลการประเมินความเสี่ยงได้ดังต่อไปนี้

คำจำกัดความของภัยคุกคาม

ลำดับ	ภัยคุกคาม	ความหมาย
1.1	ไฟไหม้ระบบจำหน่าย	เกิดไฟไหม้ระบบจำหน่าย
1.2	ไฟไหม้ระบบสายส่ง	เกิดไฟไหม้ระบบสายส่ง
1.3	ไฟไหม้สำนักงาน	เกิดไฟไหม้สำนักงาน
1.4	ไฟไหม้คลังพัสดุและมิเตอร์	เกิดไฟไหม้คลังพัสดุและมิเตอร์
1.5	ไฟไหม้สถานีไฟฟ้า	เกิดไฟไหม้สถานีไฟฟ้า
2.1	น้ำท่วมระบบจำหน่าย	เกิดน้ำท่วมซึ่งบริเวณระบบจำหน่าย (ระดับน้ำและระยะเวลาท่วมเทียบเท่ามหาอุทกภัยปี พ.ศ. 2554)
2.2	น้ำท่วมระบบสายส่ง	เกิดน้ำท่วมซึ่งบริเวณระบบสายส่ง (ระดับน้ำและระยะเวลาท่วมเทียบเท่ามหาอุทกภัยปี พ.ศ. 2554)
2.3	น้ำท่วมสำนักงาน	เกิดน้ำท่วมซึ่งบริเวณสำนักงาน (ระดับน้ำและระยะเวลาท่วมเทียบเท่ามหาอุทกภัยปี พ.ศ. 2554)
2.4	น้ำท่วมคลังพัสดุและมิเตอร์	เกิดน้ำท่วมซึ่งบริเวณคลังพัสดุและมิเตอร์ (ระดับน้ำและระยะเวลาท่วมเทียบเท่ามหาอุทกภัยปี พ.ศ. 2554)
2.5	น้ำท่วมสถานีไฟฟ้า	เกิดน้ำท่วมซึ่งบริเวณสถานีไฟฟ้า (ระดับน้ำและระยะเวลาท่วมเทียบเท่ามหาอุทกภัยปี พ.ศ. 2554)
3.1	เกิดพายุที่ระบบจำหน่าย	เกิดพายุรุนแรงส่งผลกระทบต่อระบบจำหน่าย
3.2	เกิดพายุที่ระบบสายส่ง	เกิดพายุรุนแรงส่งผลกระทบต่อระบบสายส่ง
3.3	เกิดพายุที่สำนักงาน	เกิดพายุรุนแรงส่งผลกระทบต่อสำนักงาน
3.4	เกิดพายุที่คลังพัสดุและมิเตอร์	เกิดพายุรุนแรงส่งผลกระทบต่อคลังพัสดุและมิเตอร์
3.5	เกิดพายุที่สถานีไฟฟ้า	เกิดพายุรุนแรงส่งผลกระทบต่อสถานีไฟฟ้า
4	ระบบไฟฟ้าขัดข้อง	ระบบไฟฟ้าที่จ่ายกระแสไฟให้สำนักงานเกิดขัดข้องทำให้ไม่มีไฟฟ้าใช้
5.1	เกิดเหตุวินาศกรรมที่ระบบจำหน่าย	เกิดเหตุวินาศกรรมส่งผลกระทบต่อระบบจำหน่าย
5.2	เกิดเหตุวินาศกรรมที่ระบบสายส่ง	เกิดเหตุวินาศกรรมส่งผลกระทบต่อระบบสายส่ง
5.3	เกิดเหตุวินาศกรรมที่สำนักงาน	เกิดเหตุวินาศกรรมส่งผลกระทบต่อสำนักงาน



ลำดับ	ภัยคุกคาม	ความหมาย
5.4	เกิดเหตุวินาศกรรมที่คลังพัสดุและมิเตอร์	เกิดเหตุวินาศกรรมส่งผลกระทบต่อคลังพัสดุและมิเตอร์
5.5	เกิดเหตุวินาศกรรมที่สถานีไฟฟ้า	เกิดเหตุวินาศกรรมส่งผลกระทบต่อสถานีไฟฟ้า
6	เกิดเหตุจลาจลหรือชุมนุม	เกิดเหตุจลาจลหรือชุมนุม หน่วยงานรัฐและเอกชนไม่สามารถเปิดทำการได้ตามปกติ
7	โรคระบาด	เกิดโรคระบาดในพื้นที่ใกล้เคียงซึ่งครอบคลุมสำนักงาน และมีบุคลากรของ กฟภ. ติดเชื้อไม่สามารถมาปฏิบัติงานได้
8	ผู้รับจ้างไม่สามารถให้บริการได้	ผู้รับจ้างไม่สามารถให้บริการได้
9	ระบบไอทีล้มเหลว	เกิดความล้มเหลวของระบบคอมพิวเตอร์ของสำนักงาน ไม่สามารถใช้งานได้
10	ระบบเครือข่ายล้มเหลว	เกิดความล้มเหลวของระบบเครือข่ายและการสื่อสารของสำนักงาน ไม่สามารถใช้งานได้
11	ไวรัสคอมพิวเตอร์	ไวรัสคอมพิวเตอร์ระบาดในระบบงาน ซึ่งสร้างความเสียหายต่อระบบงานและข้อมูลที่สำคัญ
12	ถูกโจมตีระบบคอมพิวเตอร์	ระบบงานและระบบฐานข้อมูลที่สำคัญถูกผู้ไม่ประสงค์ดีโจมตี
13	สารพิษรั่วไหล	สารเคมีอันตรายต่อชีวิตมนุษย์เกิดการรั่วไหลบริเวณสำนักงาน



สรุปผลการประเมินความเสี่ยง

ลำดับ	ภัยคุกคาม	กระบวนการที่ได้รับผลกระทบ*							การควบคุม	ประเมินความเสี่ยง			มาตรการจัดการความเสี่ยง
		1	2	3	4	5	6	7		โอกาสที่จะเกิด	ผลกระทบ	ระดับความเสี่ยง	
1.1	ไฟไหม้ระบบจำหน่าย	√	√	-	-	-	-	-	C01	ต่ำมาก (1)	ปานกลาง (3)	ต่ำ (3)	ยอมรับความเสี่ยง
1.2	ไฟไหม้ระบบสายส่ง	√	√	-	-	-	-	-	C01	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
1.3	ไฟไหม้สำนักงาน	√	√	√	√	√	√	√	C01, C02, C03	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
1.4	ไฟไหม้คลังพัสดุและมิเตอร์	√	-	-	-	-	-	√	C01, C02	ต่ำมาก (1)	ปานกลาง (3)	ต่ำ(3)	ยอมรับความเสี่ยง
1.5	ไฟไหม้สถานีไฟฟ้า	√	√	-	-	-	-	-	C01, C02	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
2.1	น้ำท่วมระบบจำหน่าย	√	√	-	√	√	-	√	C01	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
2.2	น้ำท่วมระบบสายส่ง	√	√	-	-	-	-	-	C01	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
2.3	น้ำท่วมสำนักงาน	√	√	√	√	√	√	√	C01	ต่ำมาก (1)	ต่ำ (2)	ต่ำ (2)	ยอมรับความเสี่ยง
2.4	น้ำท่วมคลังพัสดุและมิเตอร์	-	-	-	-	-	-	√	C01	ต่ำมาก (1)	ปานกลาง (3)	ต่ำ (3)	ยอมรับความเสี่ยง
2.5	น้ำท่วมสถานีไฟฟ้า	√	√	-	-	-	-	-	C01	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
3.1	เกิดพายุที่ระบบจำหน่าย	√	√	-	-	-	-	-	C01, C04	ต่ำ(2)	สูงมาก(5)	ปานกลาง(10)	ทำแผน ERP และเพิ่มมาตรการ ควบคุม
3.2	เกิดพายุที่ระบบสายส่ง	√	√	-	-	-	-	-	C01, C04	ต่ำ(2)	สูงมาก(5)	ปานกลาง(10)	ทำแผน ERP และเพิ่มมาตรการ ควบคุม
3.3	เกิดพายุที่สำนักงาน	√	√	-	-	-	-	-	C01	ต่ำมาก (1)	ต่ำ (2)	ต่ำ (2)	ยอมรับความเสี่ยง
3.4	เกิดพายุที่คลังพัสดุและมิเตอร์	-	-	-	-	-	-	√	C01	ต่ำมาก (1)	ต่ำ (2)	ต่ำ (2)	ยอมรับความเสี่ยง
3.5	เกิดพายุที่สถานีไฟฟ้า	√	√	-	-	-	-	-	C01	ต่ำมาก (1)	ต่ำ (2)	ต่ำ (2)	ยอมรับความเสี่ยง
4	ระบบไฟฟ้าขัดข้อง	√	√	√	√	√	√	√	C05	ปานกลาง (3)	ต่ำมาก (1)	ต่ำ (3)	ยอมรับความเสี่ยง



ลำดับ	ภัยคุกคาม	กระบวนการที่ได้รับผลกระทบ*							การควบคุม	ประเมินความเสี่ยง			มาตรการจัดการ ความเสี่ยง
		1	2	3	4	5	6	7		โอกาสที่จะเกิด	ผลกระทบ	ระดับความเสี่ยง	
5.1	เกิดเหตุวินาศกรรมที่ระบบจำหน่าย	√	√	-	-	-	-	-	C01	ต่ำมาก (1)	สูง (4)	ต่ำ (4)	ยอมรับความเสี่ยง
5.2	เกิดเหตุวินาศกรรมที่ระบบสายส่ง	√	√	-	-	-	-	-	C01	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
5.3	เกิดเหตุวินาศกรรมที่สำนักงาน	√	√	√	√	√	√	√	C01, C06	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
5.4	เกิดเหตุวินาศกรรมที่คลังพัสดุและ มิเตอร์	√	-	-	-	-	-	√	C01	ต่ำมาก (1)	สูง (4)	ต่ำ(4)	ยอมรับความเสี่ยง
5.5	เกิดเหตุวินาศกรรมที่สถานีไฟฟ้า	√	√	-	-	-	-	-	C01, C06	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
6	เกิดเหตุจลาจลหรือชุมนุม	√	√	√	√	√	√	√	C01, C06	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
7	โรคระบาด	√	√	√	√	√	√	√	C01, C07	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP
8	ผู้รับจ้างไม่สามารถให้บริการได้	√	-	-	√	√	-	√	C08	ต่ำมาก (1)	สูง (4)	ต่ำ (4)	ยอมรับความเสี่ยง
9	ระบบไอทีล้มเหลว	√	√	√	√	√	√	√	C09	ต่ำ (2)	ต่ำ (2)	ต่ำ(4)	ยอมรับความเสี่ยง
10	ระบบเครือข่ายล้มเหลว	√	√	√	√	√	√	√	C09	ต่ำ (2)	ต่ำ (2)	ต่ำ(4)	ยอมรับความเสี่ยง
11	ไวรัสคอมพิวเตอร์	√	√	√	√	√	√	√	C10, C12	ต่ำมาก (1)	ต่ำ (2)	ต่ำ(2)	ยอมรับความเสี่ยง
12	ถูกโจมตีระบบคอมพิวเตอร์	√	√	√	√	√	√	√	C11, C12	ต่ำมาก (1)	สูง (4)	ต่ำ(4)	ยอมรับความเสี่ยง
13	สารพิษรั่วไหล	√	√	√	√	√	√	√	C01, C07	ต่ำมาก (1)	สูงมาก (5)	ปานกลาง (5)	ทำแผน ERP

หมายเหตุ กระบวนการที่ได้รับผลกระทบ *

1 = งานแก้ไขการจ่ายกระแสไฟฟ้าขัดข้อง

3 = งานรับชำระค่าไฟ (รายย่อย-รายใหญ่)

4 = งานจดหน่วยและแจ้งหนี้ค่าไฟ (รายย่อย)

6 = งานรับเรื่องขอติดตั้งมิเตอร์ใหม่

2 = งานควบคุมการจ่ายกระแสไฟฟ้า

5 = งานจดหน่วยและแจ้งหนี้ค่าไฟ (รายใหญ่)

7 = งานติดตั้งมิเตอร์



จากผลการประเมินความเสี่ยง สามารถจัดลำดับภัยคุกคามตามระดับความเสี่ยงได้ ดังนี้

ระดับความเสี่ยง	ภัยคุกคาม
สูงมาก	-
ปานกลาง	ไฟไหม้ระบบสายส่งไฟไหม้สำนักงานไฟไหม้สถานีไฟฟ้า น้ำท่วมระบบจำหน่ายน้ำท่วมระบบ สายส่ง น้ำท่วมสำนักงานน้ำท่วมสถานีไฟฟ้าเกิดแผ่นดินไหวที่ระบบจำหน่ายเกิดแผ่นดินไหวที่ระบบ สายส่ง เกิดแผ่นดินไหวที่สำนักงาน เกิดแผ่นดินไหวที่สถานีไฟฟ้าเกิดแผ่นดินไหวที่ค้ำส่งพัสดุและมิเตอร์ เกิดพายุที่ระบบจำหน่ายเกิดพายุที่ระบบสายส่ง เกิดสึนามิที่ระบบจำหน่ายเกิด สึนามิที่ระบบสายส่ง เกิด สึนามิที่สำนักงาน เกิด สึนามิที่สถานีไฟฟ้าเกิด สึนามิที่ค้ำส่งพัสดุและมิเตอร์เกิดเหตุวินาศกรรมที่ระบบสายส่งเกิดเหตุวินาศกรรมที่สำนักงานเกิดเหตุวินาศกรรมที่สถานีไฟฟ้าเกิดเหตุจลาจลหรือชุมนุมโรคระบาดสารพิษรั่วไหล
ต่ำ	ไฟไหม้ระบบจำหน่ายไฟไหม้ค้ำส่งพัสดุและมิเตอร์น้ำท่วมค้ำส่งพัสดุและมิเตอร์เกิดพายุที่สำนักงานเกิดพายุที่ค้ำส่งพัสดุและมิเตอร์เกิดพายุที่สถานีไฟฟ้าระบบไฟฟ้าขัดข้องเกิดเหตุวินาศกรรมที่ระบบจำหน่ายเกิดเหตุวินาศกรรมที่ค้ำส่งพัสดุและมิเตอร์ผู้รับจ้างไม่สามารถให้บริการได้ระบบไอทีล้มเหลวระบบเครือข่ายล้มเหลวไวรัสคอมพิวเตอร์ถูกโจมตีระบบคอมพิวเตอร์



ภัยคุกคามที่จัดทำแผนตอบโต้ภาวะฉุกเฉิน

สำหรับภัยคุกคามที่จะนำมาจัดทำแผน ตอบโต้ภาวะฉุกเฉิน ซึ่งเป็นส่วนหนึ่งของแผน ตอบโต้ภาวะฉุกเฉิน (Emergency Response Plan) และแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ซึ่งพิจารณาจากภัยคุกคามที่ผลการประเมินความเสี่ยงมีระดับผลกระทบอยู่ใน ระดับปานกลางและสูงมาก มีจำนวนทั้งหมด 8 ภัยคุกคามดังต่อไปนี้

1. ไฟไหม้
2. น้ำท่วม
3. พายุ
4. เกิดเหตุวินาศกรรม
5. เกิดเหตุจลาจลหรือชุมนุม
6. โรคระบาด
7. ผู้รับจ้างไม่สามารถให้บริการได้
8. สารพิษรั่วไหล

ภัยคุกคามที่ต้องจัดทำมาตรการควบคุมเพิ่มเติม

สำหรับภัยคุกคามที่ต้องจัดทำมาตรการควบคุมเพิ่มเติมเพื่อลดโอกาสและผลกระทบผลให้อยู่ในระดับความเสี่ยงต่ำ ซึ่งเป็นระดับความเสี่ยงที่ กฟภ. ยอมรับได้ ประกอบด้วย

ภัยคุกคาม	มาตรการควบคุมเพิ่มเติมเพื่อลดโอกาส และ/หรือผลกระทบ ให้ความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้ (ระดับต่ำ)
เกิดพายุที่ระบบจำหน่าย	1. เพิ่มมาตรการเทคนิคกริดหุ้มโคนเสาไฟฟ้าให้มีความแข็งแรงมากขึ้น 2. เพิ่มสายยึดโยงเสาไฟฟ้าให้มีความแข็งแรงเพิ่มขึ้น 3. ปรับลดระยะห่างของเสาไฟฟ้าให้มีความแข็งแรงขึ้น (ปักเสาแชนไลน์)
เกิดพายุที่ระบบสายส่ง	

- หมายเหตุ 1. กรณีระดับความเสี่ยงปานกลางและสูงมาก ให้จัดทำแผน ERP และจัดทำมาตรการควบคุมเพิ่มเติม
2. กรณีระดับความเสี่ยงปานกลาง (โอกาสเกิดเป็น 1 และผลกระทบเป็น 5)ให้จัดทำแผน ERP เพียงอย่างเดียว



การควบคุมที่มีอยู่ในปัจจุบัน

เลขที่	หมายเลขภัยคุกคามที่เกี่ยวข้อง	รายละเอียด
C01	1.1-1.5, 2.1-2.5, 3.1-3.5, 4.1-4.5, 5.1-5.5, 7.1-7.5, 8, 9, 15	ในกรณีเกิดสถานการณ์ฉุกเฉิน จะมีการตั้ง War Room เพื่อประชุมและวิเคราะห์แนวทางการแก้ไขสถานการณ์ ดำเนินการแก้ไข และติดตามสถานการณ์อย่างใกล้ชิดจนกว่าสถานการณ์จะคลี่คลาย และมีการเตรียมพร้อมของชุดซ่อมแซมฉุกเฉิน ทั้งบุคลากร อุปกรณ์ และยานพาหนะ เพื่อเข้าแก้ไขสถานการณ์ฉุกเฉิน
C02	1.3, 1.4, 1.5	มีการติดตั้งอุปกรณ์ดับเพลิงเพื่อใช้ในกรณีเกิดเหตุไฟไหม้
C03	1.3	มีการซักซ้อมการหนีไฟปีละ 1 ครั้ง
C04	4.1, 4.2	มีการประสานงานกับองค์การบริหารส่วนตำบล เทศบาล และหน่วยงานต่างๆ ให้ตรวจสอบการตั้งป้ายโฆษณา และต้นไม้ใหญ่ ตลอดจนการจัดทำหนังสือแจ้งเตือน และประชาสัมพันธ์ผ่านสื่อต่างๆ เพื่อให้ระมัดระวังหรือดำเนินการรื้อถอนป้ายโฆษณาและต้นไม้ใหญ่ เพื่อป้องกันเหตุร้ายแรงที่อาจเกิดขึ้นในกรณีเกิดพายุ
C05	6	มีการติดตั้งอุปกรณ์สำรองไฟ (UPS) และสามารถสลับแหล่งจ่ายไฟ (Source) ในกรณีระบบไฟฟ้าขัดข้องได้
C06	7.3, 7.5, 8	มีเจ้าหน้าที่รักษาความปลอดภัยคอยดูแล และติดตั้งกล้องวงจรปิด (CCTV) บริเวณสำนักงานและสถานีไฟฟ้า
C07	9, 15	มีการฉีดวัคซีนป้องกันโรคระบาดประจำปีหรือในกรณีที่เกิดโรคระบาดโดยกองสถานพยาบาล รวมถึงการดูแลในด้านอาชีวอนามัยอย่างสม่ำเสมอโดยเจ้าหน้าที่ความปลอดภัยของ กฟภ.
C08	10	กำหนดให้บุคลากรของ กฟภ. ปฏิบัติงานทดแทนในกรณีที่ผู้รับจ้างไม่สามารถปฏิบัติงานได้
C09	11, 12	มีการดูแลรักษาระบบงานและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ และได้รับการสนับสนุนในการแก้ปัญหาหรือปรับปรุงประสิทธิภาพจากผู้รับจ้าง (Vendor)
C10	13	มีการติดตั้งซอฟต์แวร์ Antivirus สำหรับคอมพิวเตอร์ทุกเครื่องที่ใช้งานของ กฟภ.
C11	14	มีการติดตั้ง IPS (Intrusion Prevention System) IDS (Intrusion Detection System) และ Firewall
C12	13, 14	มีหน่วยงานรับผิดชอบในการดูแลความมั่นคงปลอดภัยของ กฟภ. โดยรับผิดชอบในการเฝ้าระวังภัยคุกคาม เช่น การทดสอบความมั่นคงปลอดภัย ด้วยวิธีเจาะระบบ เป็นต้น และบริหารจัดการความมั่นคงปลอดภัยของระบบงานและเครือข่าย



ข้อเสนอแนะ

จากการประชุมเชิงปฏิบัติการ (Workshop) พบว่า การไฟฟ้าจตุรรมงาน อาจลดโอกาสที่จะเกิดและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคาม โดยการจัดทำแผนบริหารความเสี่ยงและเพิ่มมาตรการควบคุมที่มีอยู่เดิมและดังต่อไปนี้

ลำดับ	ข้อเสนอแนะ
1	ในกรณีที่เกิดสถานการณ์ฉุกเฉิน ควรมีการมอบอำนาจให้ผู้บังคับบัญชาของแต่ละหน่วยงานย่อยชั่วคราว เพื่อให้ตัดสินใจแก้ไขสถานการณ์ได้อย่างทันเวลา ตลอดจนการอนุมัติและการเบิกค่าใช้จ่ายล่วงหน้า ซึ่งจะช่วยลดระยะเวลาและความเสียหายที่อาจเกิดขึ้นจากภัยพิบัติต่อ การไฟฟ้าจตุรรมงาน และผู้ใช้บริการ
2	ควรมีการเก็บรวบรวมเอกสารสำคัญที่มีผลทางกฎหมาย เช่น สัญญาขายไฟและหนังสือค้ำประกันของธนาคาร เป็นต้น ในรูปแบบเอกสารอิเล็กทรอนิกส์เป็นเอกสารสำรองเพื่อลดผลกระทบในกรณีเกิดภัยคุกคามที่อาจส่งผลกระทบให้เอกสารดังกล่าวเกิดความเสียหาย
3	ในกรณีเกิดเหตุระบบไอทีและเครือข่ายล้มเหลว เป็นเหตุให้ระบบงานต่างๆ ไม่สามารถใช้งานได้ โดยเฉพาะระบบงาน BPM ซึ่งใช้ในการปฏิบัติงานรับชำระค่าไฟ (ผู้ใช้บริการรายย่อยและรายใหญ่) หากผู้รับผิดชอบสามารถกู้คืนระบบงาน BPM ให้สามารถกลับมาใช้งานได้ภายในระยะเวลา 15 นาที อาจเพิ่มความพึงพอใจให้แก่ผู้ใช้บริการของ การไฟฟ้าจตุรรมงาน ได้
4	สำหรับภัยคุกคามที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ได้แก่ ระบบเครือข่ายล้มเหลวไวรัสคอมพิวเตอร์ และการถูกโจมตีระบบคอมพิวเตอร์ หน่วยงานที่รับผิดชอบของการไฟฟ้าจตุรรมงาน อาจพิจารณาเพิ่มเติมมาตรการควบคุมเพื่อลดความเสี่ยงของภัยคุกคามดังกล่าว เช่น การควบคุมการใช้สื่อบันทึกข้อมูลชนิดพกพา และการทดสอบความมั่นคงปลอดภัย ด้วยวิธีการเจาะระบบ อย่างสม่ำเสมอ เป็นต้น