บริษัท อี-คัสตอม เซอร์วิส จำกัด

ระเบียบการปฏิบัติงาน การบริหารความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศ

Information Security Risk Management Procedure

เอกสารเลขที่	ECS-QP-02	**เวอร์ชัน**	1.0
วันที่บังคับใช้	9		
ชั้นข้อมูล	เอกสารภายใน		
เจ้าของเอกสาร			

ผู้จัดทำ	**ผู้ตรวจสอบ**	**ผู้อนุมัติ**
ลงชื่อ (.....) ตำแหน่ง..... วันที่	ลงชื่อ (.....) ตำแหน่ง..... วันที่	ลงชื่อ (.....) ตำแหน่ง..... วันที่ .....

ประวัติการแก้ไขเอกสาร

เวอร์ชัน	วันที่บังคับใช้	รายละเอียดการแก้ไข
1.0		เอกสารสร้างใหม่

สารบัญ

1 วัตถุประสงค์

ระเบียบการปฏิบัติงาน การบริหารความเสี่ยงด้านความมั่นปลอดภัยสารสนเทศฉบับนี้ จัดทำขึ้นเพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน เพื่อลดความเสียหายที่อาจเกิดแกระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศดำเนินงานได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขได้อย่างทันท่วงที เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ เพื่อพิสูจน์หาปัจจัยที่ก่อให้เกิดความเสี่ยง และผลจากการประเมินความเสี่ยงจะถูกนำมาเข้ากระบวนการจัดการความเสี่ยง และเพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหาร และผู้ปฏิบัติในการดูรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของบริษัท อี-คัสตอม เซอร์วิส จำกัด

2 ขอบเขต

ระเบียบการปฏิบัติงาน การบริหารความเสี่ยงด้านความมั่นปลอดภัยสารสนเทศและความต่อเนื่องทางธุรกิจฉบับนี้ จัดทำขึ้นสำหรับการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่อยู่ภายใต้ขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของบริษัท อี-คัสตอม เซอร์วิส จำกัด

3 คำจำกัดความและอักษรย่อ

คำกำจัดความ อักษรย่อ	คำอธิบาย
เหตุการณ์ความเสี่ยง (Risk Scenario)	■ เหตุการณ์ที่เกิดขึ้นแล้ว มีผลกระทบด้านความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ ข้อมูลสารสนเทศ รวมไปถึงทรัพย์สินสารสนเทศ/ทรัพยากรอื่นๆ ของบริษัท อี-คัสตอม เซอร์วิส จำกัดส่งผลให้กระบวนการดำเนินธุรกิจของบริษัท อี-คัสตอม เซอร์วิส จำกัดล่าช้าหรือหยุดชะงัก
การบริหารความเสี่ยง (Risk Management)	■ เป็นการบริหารปัจจัย และควบคุมกิจกรม หรือกระบวนการต่าง ๆ เพื่อลดโอกาสที่จะทำให้เกิดความเสียหาย หรือล้มเหลว ดังนั้นเพื่อควบคุมให้ระดับความเสียหาย และผลกระทบที่อาจจะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถรับได้ ประเมินได้ ควบคุมได้ และสามารถตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามภารกิจหลักตามกฎหมายจัดตั้งส่วนราชการ

คำกำจัดความ อักษรย่อ	คำอธิบาย
การประเมินความเสี่ยง (Risk Assessment)	■ การคาดคะเน หรือคำนวณโอกาสที่จะเป็นเหตุให้เกิดความเสียหายและหรือความเสียหายที่จะส่งผลกระทบต่อการทำงานที่ไม่บรรลุเป้าหมายที่วางไว้ เพื่อให้ทราบความสำคัญของความเสี่ยงที่แตกต่างกัน และใช้การพิจารณาในการกำหนดจุดควบคุมความเสี่ยงที่มีนัยสำคัญ
ผลกระทบ (Impact)	■ การเปลี่ยนแปลงในทางลบ มีผลต่อระดับของการบรรลุวัตถุประสงค์การดำเนินการทางธุรกิจหรือในการปฏิบัติงาน
โอกาสเกิดขึ้นของเหตุการณ์ (Likelihood)	■ โอกาสหรือความเป็นไปได้ที่จะเกิดเหตุการณ์/สถานการณ์ โดยอ้างอิงจากข้อมูลทางสถิติของเหตุการณ์/สถานการณ์ที่เกิดขึ้น
มาตรการควบคุม (Control)	■ มาตรการที่ใช้สำหรับจัดการ หรือเปลี่ยนแปลงความเสี่ยง โดยรวมถึงกระบวนการ นโยบาย การปฏิบัติ หรือการกระทำใด ๆ ที่เปลี่ยนแปลงความเสี่ยง ซึ่งอาจเป็นรูปแบบการจัดการด้านเทคนิค ด้านการดำเนินการ ด้านบริหารจัดการ หรือด้านกฎหมาย
แผนจัดการความเสี่ยง (Risk Treatment Plan: RTP)	■ แผนดำเนินการเพื่อบริหารความเสี่ยงโดยการควบคุม จัดการแก้ไข หรือปรับลดความเสี่ยง สำหรับรายการความเสี่ยงที่อยู่ในระดับที่ต้องควบคุมเพื่อจัดการความเสี่ยงนั้น
ความเสี่ยงคงเหลือ (Residual Risk)	■ ความเสี่ยงที่ยังคงเหลืออยู่ ภายในบริษัท อี-คัสตอม เซอร์วิส จำกัดหลังจากการจัดการความเสี่ยงไปแล้ว โดยรวมถึงการประเมินคาดการณ์ความเสี่ยงคงเหลือภายหลังจากการจัดทำแผนจัดการความเสี่ยง
เจ้าของความเสี่ยง (Risk Owner)	■ เจ้าของความเสี่ยงเป็นบุคคลหรือหน่วยงานผู้มีภาระความรับผิดชอบและอำนาจในการบริหารจัดการความเสี่ยง ซึ่งรับผิดชอบต่อผลกระทบที่เกิดขึ้นจากรายการความเสี่ยง

4 บทบาท หน้าที่และความรับผิดชอบ

บทบาท	หน้าที่และความรับผิดชอบ
คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee)	■ พิจารณาอนุมัติขั้นตอนการดำเนินงานสำหรับบริหารความเสี่ยงและเกณฑ์การประเมินความเสี่ยง ■ พิจารณาอนุมัติรายงานผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง ■ พิจารณาอนุมัติผลการจัดการความเสี่ยง
ผู้จัดการระบบบริหารจัดการความมั่นคงปลอดภัย (ISMR)	■ ติดตามความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง ■ รวบรวมรายงานความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง
คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Team)	■ จัดทำขั้นตอนการดำเนินงานสำหรับบริหารความเสี่ยงและเกณฑ์การประเมินความเสี่ยง ■ กำหนดสถานการณ์ความเสี่ยง ■ ดำเนินการประเมินความเสี่ยง ■ จัดทำรายงานผลการประเมินความเสี่ยง ■ จัดทำแผนปฏิบัติตามแผนจัดการความเสี่ยง ■ ติดตามความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง ■ นำเสนอความคืบหน้าของแผนจัดการความเสี่ยงในการประชุม
เจ้าของความเสี่ยง	■ พิจารณาความถูกต้องเหมาะสมของผลการประเมินความเสี่ยงและแผนการจัดการความเสี่ยง
ผู้รับผิดชอบแผนจัดการความเสี่ยง	■ สรุปและจัดทำรายงานความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง ■ ตรวจสอบความถูกต้องเหมาะสมของแผนจัดการความเสี่ยง

5 ขั้นตอนการดำเนินการ

บริษัท อี-คัสตอม เซอร์วิส จำกัดได้นำเทคโนโลยีสารสนเทศมาใช้งานเพื่อช่วยประสิทธิภาพการดำเนินงานและให้บริการประชาชนได้รับความสะดวก รวดเร็ว ขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือปัจจัยทั้งภายในและภายนอก ส่งผลกระทบต่อการดำเนินงานขององค์กร ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่งคงปลอดภัย ซึ่งมีขั้นตอนการดำเนินการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ ดังนี้

5.1 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ กระบวนการทำงานที่ช่วยให้ฝ่ายเทคโนโลยีสารสนเทศสามารถประเมินความเสี่ยงและโอกาสของเหตุการณ์ต่าง ๆ เพื่อนำขอมูลของการประเมินความเสี่ยงที่ได้มีวิเคราะห์และจัดระดับความสำคัญ เพื่อวางแผนป้องกันความเสี่ยงหรือสร้างโอกาส และนำไปสร้างมาตรการเพื่อให้ฝ่ายเทคโนโลยีสารสนเทศสามารถบรรลุผลสำเร็จของพันธกิจที่ตั้งไว้

5.2 การระบุเหตุการณ์ความเสี่ยง

การระบุเหตุการณ์ความเสี่ยง (Risk Scenario) คือ เป็นการค้นหาและระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กร ทั้งภายในและภายนอก ทั้งเหตุการณ์ที่เคยเกิดขึ้นมาแล้วในอดีต และการคาดการณ์ในอนาคต ส่งผลให้การดำเนินงานไม่บรรลุผลสำเร็จตามวัตถุประสงค์ที่กำหนดไว้ โดยระบุเหตุการณ์ความเสี่ยงที่คาดว่าจะส่งผลทำให้สารสนเทศสูญเสียความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้ (Availability) เพื่อให้สามารถกำหนดแผนจัดการความเสี่ยงได้ตรงตามสาเหตุและสามารถลดความเสี่ยงลงได้อย่างมีประสิทธิผล

5.3 การระบุมาตรการควบคุมปัจจุบัน

มาตรการควบคุมปัจจุบัน (Existing Control) เป็นมาตรการที่ใช้หรือมีการดำเนินการอยู่เพื่อจัดการความกับความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามที่อาศัยประโยชน์จากช่องโหว่มาสร้างความเสียหายต่อทรัพย์สินสารสนเทศที่มีอยู่ โดยที่มาตรการควบคุมปัจจุบันอาจเป็นได้ทั้ง วิธีการควบคุม การจ้างบริการ การใช้อุปกรณ์มาควบคุม เป็นต้น

5.4 การประเมินผลกระทบ

ผลกระทบ (Impact) คือ ผลลัพธ์ของเหตุการณ์ที่เกิดขึ้นจากภัยคุกคาม ซึ่งมีผลกระทบกับระบบสารสนเทศหรือต่อธุรกิจ อาจสร้างความเสียหายกับระบบสารสนเทศ ทรัพย์สินสารสนเทศ ทรัพยากรหรือองค์กรในด้านต่าง ๆ โดยต้องพิจารณามาตรการควบคุมที่มีปัจจุบันประกอบ ว่ามาตรการดังกล่าวสามารถลดผลกระทบที่เกิดขึ้นได้หรือไม่ และระบุระดับผลกระทบของบริษัท อี-คัสตอม เซอร์วิส จำกัด ได้ให้ความสำคัญต่อผลกระทบ 5 ด้าน โดยกำหนดระดับของผลกระทบแต่ละด้าน ดังต่อไปนี้

1) ผลกระทบด้านการเงิน (Finance Impact)

ผลกระทบด้านการเงิน (F: Financial)		
ระดับ		**หลักเกณฑ์การวัด**
5	สูงมาก	มากกว่า 4,000,000 บาท
4	สูง	ตั้งแต่ 3,000,001 - 4,000,000 บาท
3	ปานกลาง	ตั้งแต่ 2,000,001 - 3,000,000 บาท
2	น้อย	ตั้งแต่ 1,000,001 – 2,000,000 บาท
1	น้อยมาก	ไม่เกิน 1,000,000 บาท

2) ผลกระทบด้านกระบวนการ (Operation Impact)

ผลกระทบด้านการดำเนินการ (O: Operation)		
ระดับ		**หลักเกณฑ์การวัด**
5	สูงมาก	ระบบหยุดชะงักมากกว่า 4 ชั่วโมง
4	สูง	ระบบหยุดชะงักระหว่าง 3 – 4 ชั่วโมง
3	ปานกลาง	ระบบหยุดชะงักระหว่าง 1 – 3 ชั่วโมง
2	น้อย	ระบบหยุดชะงักระหว่าง 30 - 60 นาที
1	น้อยมาก	ระบบหยุดชะงักน้อยกว่า 30 นาที

3) ผลกระทบด้านชื่อเสียงองค์กร (Reputation Impact)

ผลกระทบด้านชื่อเสียงองค์กร (R: Reputation)		
ระดับ		**หลักเกณฑ์การวัด**
5	สูงมาก	ส่งผลต่อความน่าเชื่อถือและมีการเสนอข่าวในหนังสือพิมพ์/วิทยุ/โทรทัศน์/Internet ในเชิงลบ มากกว่า 1 วัน
4	สูง	ส่งผลต่อความน่าเชื่อถือและมีการเสนอข่าวในหนังสือพิมพ์/วิทยุ/โทรทัศน์/Internet ในเชิงลบ ตลอดวันแต่ไม่เกิน 1 วัน
3	ปานกลาง	ส่งผลต่อความน่าเชื่อถือและมีการเสนอข่าวในหนังสือพิมพ์/วิทยุ/โทรทัศน์/Internet ในเชิงลบ ในช่วงใดช่วงหนึ่งของวัน
2	น้อย	เป็นข่าวภายในองค์กรหรือส่งผลต่อความน่าเชื่อถือแต่ไม่เป็นข่าวในสื่อต่าง ๆ
1	น้อยมาก	ไม่ส่งผลต่อความน่าเชื่อถือของบริษัท อี-คัสตอม เซอร์วิส จำกัด

4) ผลกระทบด้านกฎหมายและข้อบังคับ (Law and regulatory)

ผลกระทบด้านกฎหมายและข้อบังคับ (L : Law and regulatory)		
ระดับ		**หลักเกณฑ์การวัด**
5	สูงมาก	ขัดต่อกฎระเบียบของหน่วยงานภายนอกที่กำกับดูแลบริษัท อี-คัสตอม เซอร์วิส จำกัด หรือที่กฎหมายกำหนดให้ต้องปฏิบัติตาม หากไม่ปฏิบัติตามจะมีผลทางกฎหมาย
4	สูง	ขัดต่อกฎระเบียบของหน่วยงานภายนอกที่กำกับดูแลบริษัท อี-คัสตอม เซอร์วิส จำกัด หรือที่กฎหมายกำหนดให้ต้องปฏิบัติตาม
3	ปานกลาง	ขัดต่อนโยบายหรือกฎระเบียบข้อบังคับของบริษัท อี-คัสตอม เซอร์วิส จำกัด โดยส่งผลต่อการดำเนินธุรกิจหรือการให้บริการของระบบ
2	น้อย	ขัดต่อนโยบายหรือกฎระเบียบข้อบังคับของบริษัท อี-คัสตอม เซอร์วิส จำกัด โดยละเมิดเพียงวงจำกัดและไม่ส่งผลต่อการดำเนินธุรกิจหรือการให้บริการของระบบ

ผลกระทบด้านกฎหมายและข้อบังคับ (L : Law and regulatory)		
ระดับ		**หลักเกณฑ์การวัด**
1	น้อยมาก	ไม่ขัดต่อนโยบายหรือกฎระเบียบข้อบังคับของบริษัท อี-คัสตอม เซอร์วิส จำกัด

5) ผลกระทบด้านลูกค้า

ผลกระทบด้านลูกค้า (C : Customer)		
ระดับ		**หลักเกณฑ์การวัด**
5	สูงมาก	ลูกค้าปัจจุบันขอยกเลิกสัญญาการให้บริการทันทีและลูกค้ารายใหม่ลดลง
4	สูง	ลูกค้าปัจจุบันไม่ต่อสัญญาในรอบสัญญาถัดไป และ/หรือ ลูกค้ารายใหม่ลดลง
3	ปานกลาง	ลูกค้าปัจจุบันไม่พอใจการให้บริการ และ/หรือ ลูกค้ารายใหม่ลดลง
2	น้อย	ลูกค้าปัจจุบันไม่พอใจการให้บริการแต่ไม่กระทบลูกค้ารายใหม่
1	น้อยมาก	ไม่ส่งผลกระทบต่อลูกค้า

5.5 การประเมินโอกาสเกิดของเหตุการณ์

โอกาสเกิดของเหตุการณ์ (Likelihood) คือ โอกาสหรือความถี่ของการเกิดเหตุการณ์ที่ก่อให้เกิดความสูญเสีย โดยอาจจำแนกเป็นระดับต่ำ ปานกลาง สูง หรือร้อยละของโอกาสที่จะเกิดขึ้นได้ อย่างไรก็ตามการประเมินความสูญเสียที่ไม่เคยเกิดขึ้นในอดีตอาจเป็นเรื่องยาก ดังนั้น จึงไม่ควรใช้ข้อมูลในอดีตอ้างอิงเพียงอย่างเดียว แต่ควรใช้การวิเคราะห์ปัจจัยเสี่ยงขององค์กรด้วยการวิเคราะห์ความเสี่ยงภายใต้สถานการณ์ที่เป็นไปได้ทั้งหมด การศึกษาข้อมูลเพิ่มเติมจากองค์กรอื่นๆ หรือผู้เชี่ยวชาญด้านการบริหารความเสี่ยงอื่น ซึ่งจะช่วยให้การประเมินความเสี่ยงสมเหตุสมผลมากขึ้น ในการระบุระดับโอกาสเกิดของเหตุการณ์มีเกณฑ์ดังนี้

ระดับโอกาสเกิด (L: Likelihood)		
ระดับ		**หลักเกณฑ์การวัด**
5	สูงมาก	มีโอกาสเกิด 1 ครั้ง ต่อเดือน (ปีละ 12 ครั้ง)
4	สูง	มีโอกาสเกิด 1 ครั้ง ต่อไตรมาส (ปีละ 4 ครั้ง)

ระดับโอกาสเกิด (L: Likelihood)		
ระดับ		หลักเกณฑ์การวัด
3	ปานกลาง	มีโอกาสเกิด 1 ครั้ง ในรอบ 1 ปี
2	น้อย	มีโอกาสเกิด 1 ครั้ง ในรอบ 3 ปี
1	น้อยมาก	มีโอกาสเกิด 1 ครั้ง ในรอบ 5 ปี

5.6 การจัดระดับความเสี่ยง

ระดับความเสี่ยง (Risk Level) เกิดจากคำนวณโดยนำเอาระดับผลกระทบที่สูงที่สุดมาคำนวณกับระดับของโอกาสเกิดเหตุการณ์ความเสี่ยง

ระดับความเสี่ยง = ค่าผลกระทบสูงสุด × ระดับโอกาสเกิดของเหตุการณ์

นำระดับความเสี่ยง (Risk Level) ที่คำนวณได้มาเปรียบเทียบตารางการจัดระดับความเสี่ยงเพื่อจัดระดับความสำคัญ สำหรับจัดการความเสี่ยงที่ประเมินได้ โดยพิจารณาจากตารางการจัดระดับความเสี่ยง ดังนี้

Risk Value		Likelihood Level				
		1 Yearly	2 Half-Yearly	3 Quarterly	4 Monthly	5 Weekly
Impact Level	Very High 5	L5	M10	H15	E20	E25
	High 4	L4	M8	H12	H16	E20
	Medium 3	L3	M6	M9	H12	H15
	Low 2	L2	L4	M6	M8	M10
	Very Low 1	L1	L2	L3	L4	L5

5.7 พิจารณาระดับความเสี่ยงกับเกณฑ์การยอมรับความเสี่ยง

เมื่อได้ค่าของระดับความเสี่ยงแล้ว ผู้มีอำนาจตัดสินใจจะต้องพิจารณาระดับความเสี่ยงที่ยอมรับได้ เพื่อหาแนวทางในการตอบสนองความเสี่ยงโดยมีทางเลือกสำหรับตอบสนองความเสี่ยงดังต่อไปนี้

ระดับความเสี่ยง	เกณฑ์การยอมรับความเสี่ยง
สูงมาก **E20,E25**	**ระดับความเสี่ยงที่ต้องมีการดำเนินการควบคุม** – ยังไม่มีมาตรการรองรับความเสี่ยงที่เกิดขึ้น
สูง **H12,H15,H16**	**ระดับความเสี่ยงที่ต้องมีการดำเนินการควบคุม** – มีมาตรการรองรับแล้ว แต่ไม่เพียงพอต่อระดับโอกาสที่จะเกิด หรือผลกระทบของความเสี่ยงที่เกิดขึ้นจำเป็นต้องมีมาตรการใหม่มารองรับ
ปานกลาง **M6,M8,M9,M10**	**ระดับความเสี่ยงที่ยอมรับได้** – มีมาตรการรองรับดี แต่และมีกระบวนการปฏิบัติอย่างจริงจัง
ต่ำ **L1,L2,L3,L4,L5**	**ระดับความเสี่ยงที่ยอมรับได้** – มีมาตรการรองรับดี ผลที่เกิดขึ้นดีโดยยอมรับระดับโอกาสที่จะเกิด และผลกระทบของความเสี่ยงที่เกิดขึ้น

ระดับความเสี่ยง	การตอบสนองความเสี่ยง (Risk Response)				ผู้มีอำนาจตัดสินใจ (Decision Maker)
สูงมาก	Accept and Monitor	Control	Transfer	Avoid	ISMS Committee
สูง	Accept and Monitor	Control	Transfer		ISMS Committee, ISMR,
ปานกลาง	Accept				Manager
ต่ำ	Accept				Manager

5.8 การเลือกแนวทางการตอบสนองความเสี่ยง

การเลือกแนวทางตอบสนองความเสี่ยงเป็นพิจารณาว่าความเสี่ยงที่วิเคราะห์ได้อยู่ในระดับที่ยอมรับได้หรือไม่ และหากยอมรับไม่ได้ก็ต้องเลือกแนวทางในการตอบสนองความเสี่ยง โดยแนวทางการตอบสนองต่อความเสี่ยงแบ่งเป็น 4 แนวทาง และสัมพันธ์กับระดับความเสี่ยง คือ

การยอมรับความเสี่ยง (Accept) หมายความว่า เป็นความเสี่ยงที่ยอมรับให้เกิดขึ้น และไม่ต้องดำเนินการกิจกรรมใด ๆ แต่ต้องเฝ้าระวังติดตามไม่ให้ความเสี่ยงเลื่อนระดับสูงขึ้น

การควบคุมความเสี่ยง (Control) หมายความว่า เป็นความเสี่ยงที่ต้องทำการควบคุม และทำแผนการลดความเสี่ยง (Treatment Plan) ควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

การถ่ายโอนความเสี่ยง (Transfer) หมายความว่า เป็นความเสี่ยงที่อาจต้องถ่ายโอนให้หน่วยงานอื่นรับความเสี่ยงนั้นไป หรือร่วมรับความเสี่ยงกับหน่วยงานอื่น

การหลีกเลี่ยงความเสี่ยง (Avoid) หมายความว่า เป็นความเสี่ยงที่จะต้องหลีกเลี่ยง ไม่ให้มีการกระทำหรือการปฏิบัติที่จะนำไปสู่ความเสี่ยง

5.9 การกำหนดเจ้าของความเสี่ยง

ความเสี่ยงในแต่ละระดับจะต้องได้รับการกำหนดให้ผู้ที่เป็นเจ้าของความเสี่ยง (Risk Owner) เป็นผู้รับผิดชอบในการดำเนินการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ แสดงให้เห็นถึงระดับความเสี่ยงและเจ้าของความเสี่ยงแต่ละระดับ

5.10 กำหนดแผนจัดการความเสี่ยง

สำหรับระดับความเสี่ยงที่ได้กำหนดให้มีการควบคุมความเสี่ยง (Control) ให้กำหนดแผนจัดการความเสี่ยง (Risk Treatment Plan) โดยมีรายละเอียดที่สำคัญประกอบไปด้วย กิจกรรมหรือวิธีในการดำเนินจัดการความเสี่ยง ทรัพยากรที่ต้องใช้ ระยะเวลาที่คาดว่าจะใช้ในการดำเนินการจัดการตามแผนลดความเสี่ยงและผู้รับผิดชอบในแต่ละกิจกรรม

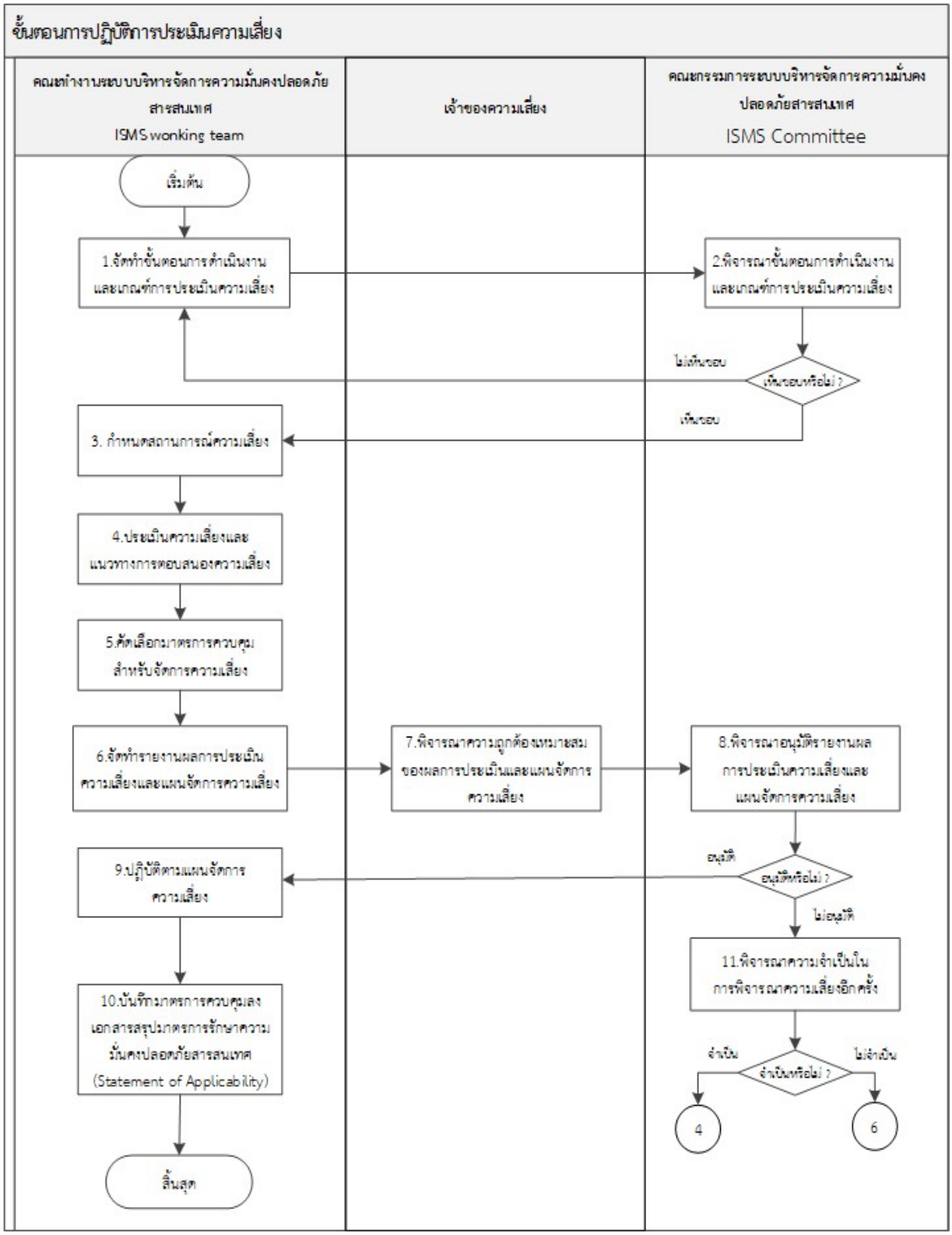
ทั้งนี้ สำหรับระดับความเสี่ยงใดที่ไม่ได้กำหนดให้ต้องมีการควบคุม ไม่จำเป็นต้องกำหนดแผนการควบคุมความเสี่ยงและไม่ต้องวัดระดับความเสี่ยงที่หลงเหลือ

5.11 วัดระดับความเสี่ยงคงเหลือ

กรณีที่มีการจัดการความเสี่ยงด้วยการควบคุม (Control) ภายหลังจากการกำหนดแผนการจัดการความเสี่ยง และดำเนินการตามแผนดังกล่าวเสร็จสิ้น ให้ทำการประเมินความเสี่ยงอีกครั้ง เพื่อหาค่าความเสี่ยงคงเหลือ (Residual Risk) โดยพิจารณาจากเงื่อนไขที่ต้องนำมาพิจารณาในการประเมินความเสี่ยงดังนี้ มาตรการควบคุมที่เพิ่มขึ้นเพื่อควบคุมความเสี่ยง (New Control) ระดับผลกระทบ (Impact) หลังและโอกาสเกิดของเหตุการณ์ (Likelihood) หลังเพิ่มมาตรการควบคุมความเสี่ยง

หากภายหลังการควบคุมความเสี่ยงแล้ว ให้เจ้าของความเสี่ยงพิจารณาระดับความเสี่ยงเหลืออยู่เพื่อพิจารณาการดำเนินการดูแลความเสี่ยงนั้น ๆ ผลการประเมินความเสี่ยงจะเสนอคณะผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อพิจารณาและรับทราบต่อไป

5.12 ขั้นตอนปฏิบัติการดำเนินการประเมินความเสี่ยง



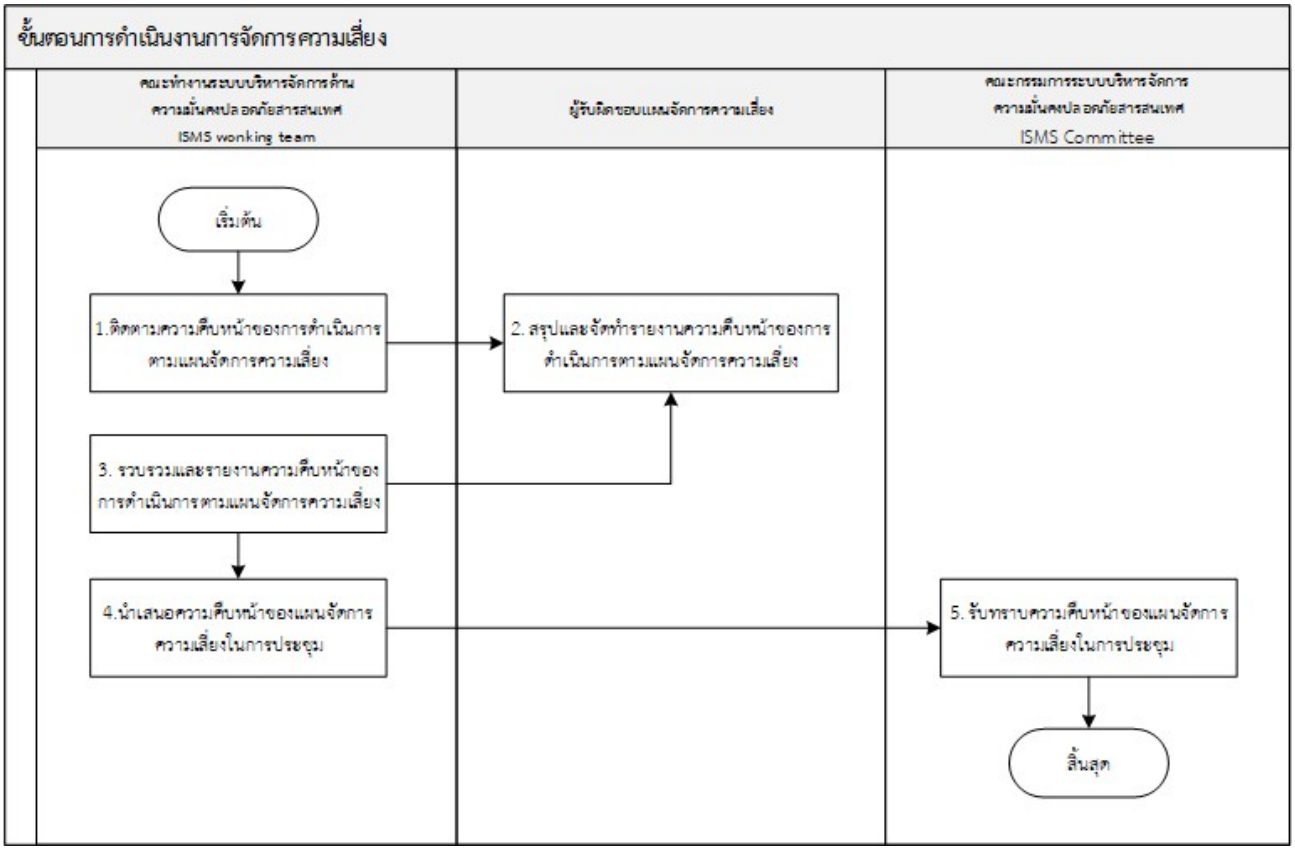
5.13 คำอธิบายขั้นตอนปฏิบัติการประเมินความเสี่ยง

ลำดับ	กระบวนการ	คำอธิบาย
1.	จัดทำขั้นตอนการดำเนินงานและเกณฑ์การประเมินความเสี่ยง	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการดังนี้ 1) จัดทำขั้นตอนการดำเนินงานสำหรับการบริหารความเสี่ยง 2) กำหนดเกณฑ์การประเมินความเสี่ยง 3) กำหนดรอบการประเมินความเสี่ยง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
2.	พิจารณาขั้นตอนการดำเนินงานสำหรับบริหารความเสี่ยงและเกณฑ์การประเมินความเสี่ยง	คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดำเนินการพิจารณาอนุมัติขั้นตอนการดำเนินงานสำหรับบริหารความเสี่ยงและเกณฑ์การประเมินความเสี่ยง ■ เห็นชอบ ให้ดำเนินการตามขั้นตอนที่ 3 ■ ไม่เห็นชอบ ให้ดำเนินการตามขั้นตอนลำดับที่ 1
3.	กำหนดสถานการณ์ความเสี่ยง	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการรวบรวมทรัพย์สินสารสนเทศ และกำหนดสถานการณ์ความเสี่ยงที่มีผลกระทบต่อองค์กร ทั้งภายในและภายนอก ทั้งเหตุการณ์ที่เคยเกิดขึ้นมาแล้วในอดีต และการคาดการณ์ในอนาคต
4.	ประเมินความเสี่ยงและแนวทางการตอบสนองความเสี่ยง	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการประเมินความเสี่ยงดังนี้ 1) ประเมินระดับผลกระทบแต่ละด้าน โดยจะนำค่าสูงสุดของผลกระทบทั้งหมดมาใช้วัดผล 2) ประเมินโอกาสเกิด (Likelihood) เพื่อหาค่าระดับความเสี่ยง (Risk Level) 3) จัดลำดับความเสี่ยง

ลำดับ	กระบวนการ	คำอธิบาย
		4) พิจารณาระดับความเสี่ยงกับเกณฑ์การยอมรับความเสี่ยง
5.	คัดเลือกมาตรการควบคุมสำหรับจัดการความเสี่ยง	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการคัดเลือกมาตรการควบคุมสำหรับจัดการความเสี่ยง จาก Annex A ของมาตรฐาน ISO27001 และ/หรือจากแหล่งอื่นๆ
6.	จัดทำรายงานผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการจัดทำรายงานผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง
7.	พิจารณาความถูกต้องเหมาะสมของผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง	เจ้าของความเสี่ยง ดำเนินการพิจารณาความถูกต้องเหมาะสมของผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง
8.	พิจารณารายงานผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง	คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พิจารณาอนุมัติรายงานผลการประเมินความเสี่ยง และแผนจัดการความเสี่ยง โดยแบ่งเป็น ■ อนุมัติ ให้ดำเนินการตามขั้นตอนลำดับที่ 9 ■ ไม่อนุมัติ ให้ดำเนินการตามขั้นตอนลำดับที่ 10
9.	ปฏิบัติตามแผนจัดการความเสี่ยง	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการปฏิบัติตามแผนจัดการความเสี่ยงที่ได้รับอนุมัติจากผู้มีอำนาจตัดสินใจ
10.	บันทึกมาตรการควบคุมลงเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability)	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการบันทึกมาตรการควบคุมลงเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability)
11.	จำเป็นต้องประเมินความเสี่ยงใหม่หรือไม่	คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดำเนินการพิจารณาความจำเป็นในการพิจารณาความเสี่ยงอีกครั้ง

ลำดับ	กระบวนการ	คำอธิบาย
		■ จำเป็น ต้องประเมินความเสี่ยงใหม่ ให้ดำเนินการตามขั้นตอนลำดับที่ 4 ■ ไม่จำเป็น ต้องประเมินความเสี่ยงใหม่ ให้ดำเนินการตามขั้นตอนลำดับที่ 6

5.14 ขั้นตอนการดำเนินการจัดการความเสี่ยง



5.15 คำอธิบายขั้นตอนการดำเนินการจัดการความเสี่ยง

ลำดับ	กระบวนการ	คำอธิบาย
1.	ติดตามความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ติดตามความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง

ลำดับ	กระบวนการ	คำอธิบาย
2.	สรุปและจัดทำรายงานความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง	ผู้รับผิดชอบแผนจัดการความเสี่ยง ดำเนินการสรุปและจัดทำรายงานความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง
3.	รวบรวมและรายงานความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการรวบรวมและรายงานความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยงในการประชุม
4.	นำเสนอความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยงในการประชุม	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการนำเสนอความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยงในการประชุม
5.	รับทราบความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง	คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ รับทราบความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง

6 เอกสารที่เกี่ยวข้อง

รหัสเอกสาร	ชื่อเอกสาร
ECS-QM-xx	รายการมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability)
ECS-QP-xx	กระบวนการปฏิบัติงาน การบริหารจัดการทรัพย์สินสารสนเทศ (Information Assets Management Procedure)

7 เอกสารสำหรับบันทึก

รหัสเอกสาร	ชื่อเอกสาร
ECS-EF-xx	ทะเบียนการวิเคราะห์ความเสี่ยง (Risk Assessment)
ECS-EF-xx	ทะเบียนรายการแผนดูแลความเสี่ยง (Risk Treatment)