

นโยบายการบริหารความเสี่ยง สมาคมส่งเสริมสถาบันกรรมการบริษัทไทย

1. บทนำ

สมาคมส่งเสริมสถาบันกรรมการบริษัทไทย (ต่อไปนี้จะเรียกว่า สมาคมฯ) มุ่งมั่นในการบริหารความเสี่ยงควบคู่ไปกับการจัดการเชิงกลยุทธ์ โดยเชื่อว่าการบริหารความเสี่ยงอย่างมีประสิทธิภาพเป็นสิ่งสำคัญอย่างยิ่งต่อความยั่งยืนขององค์กร ซึ่งส่งผลโดยตรงต่อการบรรลุเป้าหมายที่กำหนดไว้ ภายใต้การเปลี่ยนแปลงของสภาพแวดล้อมในการดำเนินธุรกิจที่มีอย่างต่อเนื่อง การตอบสนองต่อความต้องการของผู้มีส่วนได้เสียทุกกลุ่มอย่างเหมาะสม และการป้องกันความสูญเสียที่อาจเกิดขึ้นจากความไม่แน่นอนต่าง ๆ พร้อมทั้งยังช่วยในการแสวงหาโอกาสในการเพิ่มมูลค่าทางธุรกิจ

2. วัตถุประสงค์

นโยบายการบริหารความเสี่ยง (“นโยบายฉบับนี้”) มีวัตถุประสงค์เพื่อ

- 1) กำหนดกรอบการปฏิบัติงานในกระบวนการบริหารความเสี่ยงของสมาคมฯ เพื่อนำไปปฏิบัติทั่วทั้งองค์กร และเพื่อให้มั่นใจว่ามีการกำหนดหน้าที่ความรับผิดชอบในการควบคุมความเสี่ยงที่ได้รับรู้อย่างเหมาะสม ทั้งในระดับกรรมการ ผู้บริหาร และพนักงานของสมาคมฯ
- 2) เพื่อบูรณาการการบริหารความเสี่ยงเข้าสู่กระบวนการตัดสินใจขององค์กรในทุกระดับ (Integrating Risk Management into Decision Making) กระบวนการตัดสินใจสำคัญเริ่มตั้งแต่การกำหนดนโยบายและกลยุทธ์ การวางแผนงาน การจัดทำงบประมาณ การลงทุน การบริหารโครงการ กระบวนการปฏิบัติงาน การบริหารผลการปฏิบัติงาน และงานสนับสนุนองค์กรในทุกด้าน

3. ขอบเขต

นโยบายฉบับนี้ให้มีผลบังคับใช้กับทุกการดำเนินงานภายในสมาคมฯ รวมถึงบุคลากรทุกระดับของสมาคมฯ อันประกอบด้วย กรรมการ ผู้บริหาร และพนักงานของสมาคมฯ

4. นิยามของความเสี่ยง

“ความเสี่ยง” หมายถึง ความเป็นไปได้ที่เหตุการณ์บางอย่างจะเกิดขึ้นและส่งผลกระทบต่อบรรลุยุทธศาสตร์และวัตถุประสงค์ทางธุรกิจของสมาคมฯ โดยเหตุการณ์ดังกล่าวอาจมีผลทั้งทางบวกและทางลบ และอาจเกิดจากปัจจัยภายในหรือภายนอกองค์กร ซึ่งจำเป็นต้องมีการประเมิน ควบคุม และบริหารจัดการอย่างเหมาะสมเพื่อสนับสนุนการดำเนินงานให้เป็นไปตามเป้าหมายอย่างยั่งยืน

5. นโยบายการบริหารความเสี่ยง

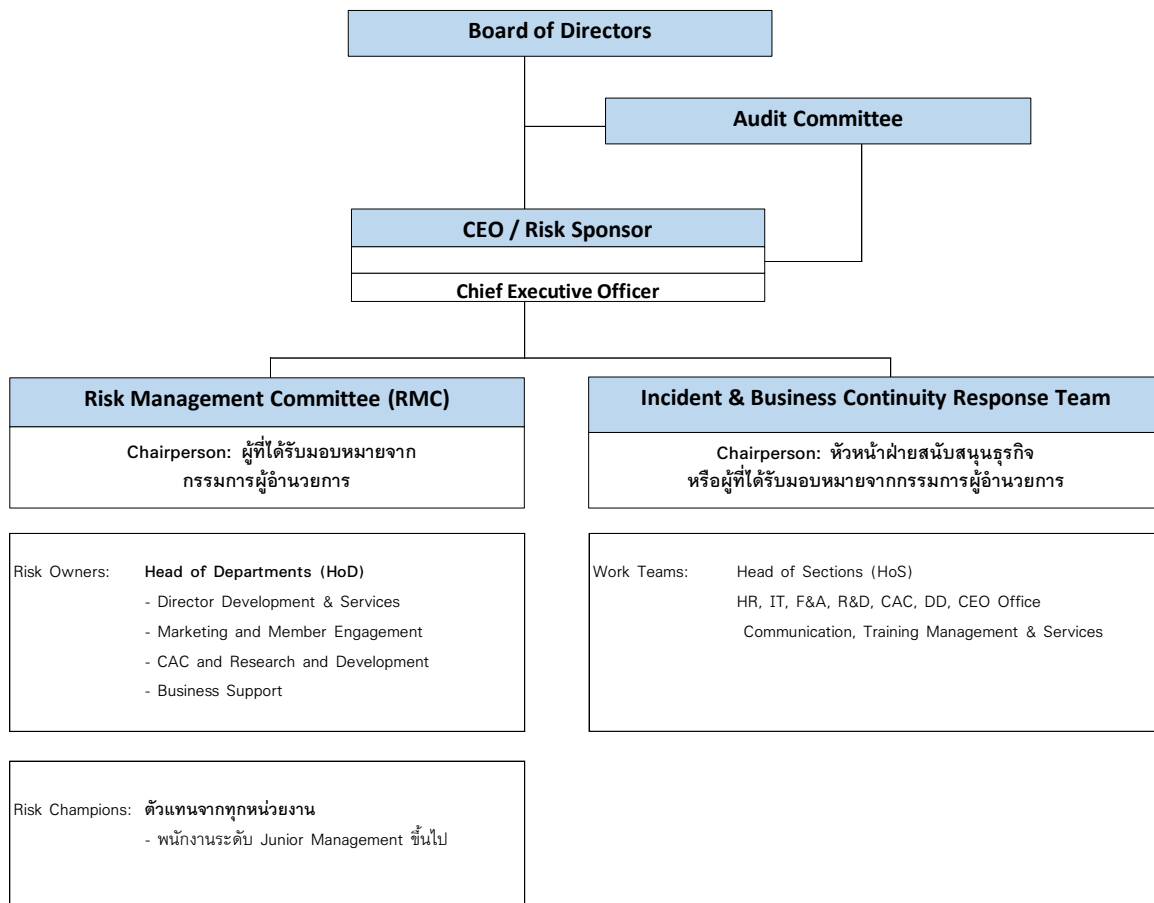
สมาคมฯ มีการกำหนดนโยบายการบริหารความเสี่ยง ดังต่อไปนี้

- 5.1 สมาคมฯ จะดำเนินธุรกิจภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) เพื่อให้บรรลุวัตถุประสงค์ของสมาคมฯ และตอบสนองต่อความคาดหวังของผู้มีส่วนได้เสีย โดยกำหนดให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการวางแผนกลยุทธ์ การดำเนินงาน และการตัดสินใจในระดับองค์กรอย่างเป็นระบบ
- 5.2 สมาคมฯ กำหนดกรอบและกระบวนการบริหารความเสี่ยงที่สอดคล้องกับมาตรฐานสากลและเชื่อมโยงกันทั้งในระดับองค์กรและหน่วยงาน โดยอ้างอิงกรอบ COSO Enterprise Risk Management (ERM) ซึ่งครอบคลุมความเสี่ยงสำคัญ 7 ด้าน ได้แก่
 1. ความเสี่ยงเชิงกลยุทธ์ (Strategic Risk)
 2. ความเสี่ยงด้านการดำเนินงาน (Operational Risk)
 3. ความเสี่ยงด้านการเงิน (Financial Risk)
 4. ความเสี่ยงด้านกฎหมายและการกำกับดูแล (Legal & Compliance Risk)
 5. ความเสี่ยงด้านชื่อเสียง (Reputational Risk)
 6. ความเสี่ยงด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG Risk)
 7. ความเสี่ยงเกิดใหม่ (Emerging Risk)

โดยทั้งนโยบาย กรอบ และกระบวนการบริหารความเสี่ยงจะต้องได้รับการทบทวนเป็นระยะ ๆ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

- 5.3 การบริหารความเสี่ยงเป็นองค์ประกอบหนึ่งที่สำคัญของทุกกระบวนการในการดำเนินงานของสมาคมฯ จึงถือเป็นความรับผิดชอบของบุคลากรทุกระดับภายในสมาคมฯ โดยทุกหน่วยงานมีหน้าที่ในการระบุ ประเมิน และ จัดการความเสี่ยงอย่างเหมาะสม พร้อมทั้งดำเนินกิจกรรมควบคุมความเสี่ยงให้สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ อันจะส่งผลให้การดำเนินงานบรรลุและเป็นไปตามเป้าหมายที่กำหนดไว้ อีกทั้งยังรักษาผลประโยชน์ของผู้มีส่วนได้เสีย คำนึงถึงประโยชน์สูงสุดขององค์กร และเป็นการแสวงหาโอกาสในการสร้างมูลค่าเพิ่มให้กับองค์กร
- 5.4 สมาคมฯ ให้ความสำคัญกับการส่งเสริมวัฒนธรรมในการบริหารความเสี่ยงที่มีประสิทธิภาพ (Risk Culture) มุ่งเน้นให้มีการจัดสรรทรัพยากรและให้การสนับสนุนในด้านต่าง ๆ อย่างเหมาะสม รวมถึงการฝึกอบรม และการสื่อสารอย่างต่อเนื่อง เพื่อสร้างความตระหนักรู้ และปลูกฝังจิตสำนึกด้านความเสี่ยงให้แก่บุคลากรทุกระดับ
- 5.5 ผู้บริหารและพนักงานทุกคนมีหน้าที่ปฏิบัติตามนโยบายการบริหารความเสี่ยง กรอบกระบวนการบริหารความเสี่ยงตามที่สมาคมฯ กำหนด โดยคณะกรรมการบริหารความเสี่ยง (Risk Management Committee หรือ RMC) มีหน้าที่กำกับ ติดตาม และรายงานผลการดำเนินการ รวมถึงทบทวนประสิทธิผลของระบบบริหารความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง และเสนอแนวทางการปรับปรุงต่อฝ่ายบริหารและคณะกรรมการที่เกี่ยวข้อง

6. โครงสร้างองค์กรในกระบวนการบริหารความเสี่ยง (Risk Management)



7. หน้าที่ความรับผิดชอบ

- 7.1 คณะกรรมการสมาคมฯ (Board of Directors) มีหน้าที่ความรับผิดชอบโดยรวมในการกำกับดูแลการบริหารความเสี่ยงภายในสมาคมฯ
- 7.2 คณะกรรมการตรวจสอบ (Audit Committee) สนับสนุนคณะกรรมการสมาคมฯ ในการปฏิบัติหน้าที่ด้านการบริหารความเสี่ยงโดยสอบทานให้มั่นใจว่าระบบการบริหารความเสี่ยงและการควบคุมภายในมีความเหมาะสม เพียงพอ และมีประสิทธิผล
- 7.3 ฝ่ายจัดการ (Management) มีหน้าที่ความรับผิดชอบในการดำเนินการตามนโยบายฉบับนี้และกำกับดูแลให้มีการปฏิบัติตามอย่างต่อเนื่อง โดยพิจารณาและสอบทานการบริหารความเสี่ยงและระบบควบคุมภายในของสมาคมฯ
- 7.4 คณะทำงานบริหารความเสี่ยง (Risk Management Committee – RMC) ซึ่งแต่งตั้งโดยกรรมการผู้อำนวยการ มีหน้าที่ทำให้เชื่อมั่นได้ว่าความเสี่ยงทางธุรกิจที่สำคัญ ได้รับการระบุและประเมินอย่างสม่ำเสมอ รวมทั้งได้มีการกำหนดมาตรการจัดการความเสี่ยงที่มีประสิทธิผลไว้ โดยรับผิดชอบในเรื่องต่าง ๆ ดังนี้

1. จัดทำนโยบายการบริหารความเสี่ยง กลยุทธ์ และหลักเกณฑ์ในการบริหารความเสี่ยง เพื่อเสนอให้คณะกรรมการสมาคมฯ พิจารณาและอนุมัติ
2. พิจารณาสอบทานความเสี่ยงและแนวทางการจัดการความเสี่ยงของสมาคมฯ ตามที่หน่วยงานเจ้าของความเสี่ยงได้ประเมินไว้ รวมทั้งให้ข้อเสนอแนะเพื่อปรับปรุงแก้ไข
3. พัฒนาตัวชี้วัดความเสี่ยงหลัก (Key Risk Indicator: KRI) กำหนดค่ามาตรฐานผลการดำเนินงานความเสี่ยง (Key Performance Parameter: KPP) เป็น 3 ระดับ คือ ระดับที่ยอมรับได้ (Acceptable) ระดับเตือนภัย (Trigger) และ ระดับเสี่ยงภัย (Risky)
4. จัดทำคู่มือการบริหารความเสี่ยง (Risk Management Manual) ทบทวน และปรับปรุงให้เหมาะสมกับปัจจุบันอยู่เสมอ
5. กำกับดูแลความมีประสิทธิภาพของกระบวนการบริหารความเสี่ยงของสมาคมฯ โดยการติดตามและสอบทานอย่างต่อเนื่อง
6. รายงานผลการบริหารความเสี่ยงให้ฝ่ายจัดการ คณะกรรมการตรวจสอบ และคณะกรรมการสมาคมฯ พิจารณา
7. สอบทานนโยบาย กรอบ และกระบวนการบริหารความเสี่ยงเป็นประจำทุกปี

7.5 คณะทำงานด้านเหตุฉุกเฉินและการดำเนินธุรกิจต่อเนื่อง (Incident & Business Continuity Response Team)

คณะทำงานชุดนี้ทำหน้าที่ในการตอบสนองต่อเหตุการณ์ฉุกเฉิน วิกฤต และภาวะหยุดชะงักของการดำเนินงาน โดยมีหน้าที่ความรับผิดชอบดังต่อไปนี้

1. ประเมินสถานการณ์และระดับความรุนแรงของเหตุการณ์ฉุกเฉินหรือวิกฤตที่เกิดขึ้น
2. จัดทำและดำเนินการตามแผนการบริหารเหตุฉุกเฉิน (Incident & Emergency Management Plan) และแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan หรือ BCP)
3. ประสานงานระหว่างฝ่ายต่าง ๆ เพื่อฟื้นฟูกิจกรรมหลักของสมาคมฯ ให้กลับคืนสู่สภาวะปกติ
4. ปรับปรุงแผน BCP และแผนสื่อสารภาวะวิกฤต (Crisis Communication Plan) ให้สอดคล้องกับสถานการณ์
5. จัดประชุม War Room กรณีเกิดเหตุการณ์ระดับร้ายแรง พร้อมดำเนินการตอบสนองภายในกรอบเวลาที่เหมาะสม
6. รายงานผลการดำเนินการและบทเรียนหลังเหตุการณ์ให้คณะกรรมการบริหารความเสี่ยง กรรมการผู้อำนวยการ และฝ่ายจัดการ

7.6 ผู้แทนความเสี่ยงประจำฝ่ายงาน (Risk Champions)

Risk Champions ทำหน้าที่เป็นตัวแทนของแต่ละฝ่าย/แผนกในด้านการบริหารความเสี่ยง มีบทบาทสำคัญในการเชื่อมโยงระหว่างหน่วยงานปฏิบัติการกับคณะกรรมการบริหารความเสี่ยง โดยมีหน้าที่ความรับผิดชอบดังนี้

1. ระบุ ประเมิน และรายงานความเสี่ยงภายในฝ่ายของตนต่อคณะกรรมการบริหารความเสี่ยง
2. สนับสนุนการจัดทำและปรับปรุงข้อมูลใน Risk Register ขององค์กร
3. ส่งเสริมความเข้าใจเกี่ยวกับนโยบายและกระบวนการบริหารความเสี่ยงในหน่วยงานของตน
4. ประสานงานการดำเนินกิจกรรมควบคุมความเสี่ยงภายในฝ่าย และติดตามผลการดำเนินการ
5. มีส่วนร่วมในการวิเคราะห์เหตุการณ์ความเสี่ยง (Incident Review) และการพัฒนาแนวทางป้องกันในอนาคต
6. ทำหน้าที่เป็นจุดติดต่อหลักของฝ่ายงานในการสื่อสารกับคณะทำงานบริหารความเสี่ยง

7.7 พนักงาน

พนักงานทุกคนถือเป็นส่วนสำคัญของกระบวนการบริหารความเสี่ยง โดยมีหน้าที่ความรับผิดชอบดังต่อไปนี้

1. ปฏิบัติงานโดยคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินงานในหน้าที่ความรับผิดชอบของตน
2. ปฏิบัติตามนโยบายและแนวทางการบริหารความเสี่ยงของสมาคมฯ อย่างเคร่งครัด
3. แจ้งเตือนหรือรายงานเหตุการณ์หรือพฤติกรรมที่อาจก่อให้เกิดความเสี่ยงหรือผลกระทบต่อสมาคมฯ ผ่านช่องทางที่กำหนด
4. สนับสนุนกิจกรรมด้านการบริหารความเสี่ยง เช่น การฝึกอบรม การประเมินความเสี่ยง และการดำเนินแผนควบคุมความเสี่ยง
5. ร่วมมือกับ Risk Champions หรือผู้แทนฝ่ายในกรณีที่ต้องมีการรวบรวมข้อมูล ประเมินหรือปรับปรุงการควบคุมความเสี่ยง
6. มีส่วนร่วมในการสร้างวัฒนธรรมแห่งความตระหนักรู้เรื่องความเสี่ยง (Risk Awareness) ในที่ทำงาน

7.8 ผู้ตรวจสอบภายใน (Internal Audit) มีหน้าที่ความรับผิดชอบในการสอบทานประสิทธิภาพของการควบคุมภายในผ่านการตรวจสอบภายในประจำปี ซึ่งเป็นการตรวจสอบกระบวนการทางธุรกิจที่สำคัญตามปัจจัยเสี่ยง รวมทั้งติดตามการปรับปรุงแก้ไขข้อบกพร่องที่ตรวจพบโดยรายงานผลให้คณะกรรมการตรวจสอบได้รับทราบ

นโยบายการบริหารความเสี่ยงฉบับนี้ได้รับการอนุมัติจากคณะกรรมการสมาคมฯ ในการประชุมครั้งที่ 4/2568 เมื่อวันที่ 5 สิงหาคม 2568 และมีผลบังคับใช้ตั้งแต่วันที่ 6 สิงหาคม 2568 เป็นต้นไป และให้ยกเลิกนโยบายการบริหารความเสี่ยง ฉบับลงวันที่ 15 ธันวาคม 2563

(นายรพี สุจริตกุล)
ประธานกรรมการ
สมาคมส่งเสริมสถาบันกรรมการบริษัทไทย

เอกสารแนบท้ายนโยบายบริหารความเสี่ยง 1

กระบวนการบริหารความเสี่ยง (Risk Management Process)

ผู้รับผิดชอบ	กระบวนการ
คณะกรรมการสมาคมฯ และฝ่ายจัดการระดับสูง (CEO / Risk Sponsor)	1. กำหนดบริบทเชิงกลยุทธ์และ Risk Appetite - กำหนดกรอบการบริหารความเสี่ยงให้สอดคล้องกับเป้าหมาย วิสัยทัศน์ และพันธกิจของสมาคมฯ - อนุมัติระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) - สนับสนุนทรัพยากรและส่งเสริมวัฒนธรรมความเสี่ยงในองค์กร
คณะกรรมการบริหารความเสี่ยง (Risk Management Committee – RMC) ร่วมกับ Risk Champions	2. ระบุความเสี่ยง (Risk Identification) ระบุเหตุการณ์ ความไม่แน่นอน หรือโอกาสที่อาจส่งผลกระทบต่อวัตถุประสงค์ของสมาคมฯ ในทุกด้าน
	3. วิเคราะห์และประเมินความเสี่ยง (Risk Analysis & Assessment) - วิเคราะห์ความเป็นไปได้และผลกระทบของความเสี่ยง - จัดระดับความเสี่ยง และจัดทำ Risk Register ร่วมกับหน่วยงานเจ้าของความเสี่ยง (Risk Owners) - ประเมินความเพียงพอของมาตรการควบคุมที่มีอยู่
Risk Owners ร่วมกับ Work Teams	4. กำหนดแนวทางตอบสนองและจัดการความเสี่ยง (Risk Response & Mitigation) - เสนอแนวทางควบคุม/ลด/โอน/ยอมรับความเสี่ยง (ตามระดับความรุนแรง) - จัดทำ Action Plan / KRI (Key Risk Indicators)/ BCP / Contingency Plan ร่วมกับฝ่ายสนับสนุนที่เกี่ยวข้อง - ดำเนินมาตรการควบคุมตามแผนและมาตรการจัดการความเสี่ยง
Incident & Business Continuity Response Team (IBCRT)	5. บริหารความเสี่ยงภาวะวิกฤตและการบริหารความต่อเนื่องทางธุรกิจ (Crisis Risk Management & Business Continuity Management) - บูรณาการแผนตอบสนองเหตุการณ์ (Incident Management) และแผนความต่อเนื่องทางธุรกิจ (BCP) - ตอบสนองฉุกเฉิน ประเมินสถานการณ์ พื้นฟูระบบและสื่อสารภายใน-ภายนอก
ฝ่ายจัดการ / Risk Management Committee (RMC)	6. ติดตามและทบทวน (Monitoring & Review) - ติดตามผลการดำเนินแผนควบคุม - วิเคราะห์แนวโน้ม (Risk Trend) และปรับปรุง Risk Register - รายงานความเสี่ยงและผลการบริหารความเสี่ยงต่อกรรมการผู้อำนวยการ คณะกรรมการตรวจสอบ และ คณะกรรมการสมาคมฯ
ผู้ตรวจสอบภายใน / คณะกรรมการตรวจสอบ / คณะกรรมการสมาคมฯ	7. ตรวจสอบและประเมิน (Internal Audit & Oversight) - ตรวจสอบประสิทธิภาพของกระบวนการควบคุมความเสี่ยง - เสนอขอเสนอแนะเชิงระบบ - ตรวจสอบความสอดคล้องกับนโยบาย/กฎหมาย
พนักงานทุกคน	- ปฏิบัติตามแนวทางความเสี่ยงที่กำหนดในระดับปฏิบัติการ - รายงานความเสี่ยงหรือเหตุการณ์ผิดปกติที่พบเจอ - ร่วมสนับสนุนการสร้างวัฒนธรรมองค์กรด้านความเสี่ยง

เอกสารแนบท้ายนโยบายบริหารความเสี่ยง 2

เกณฑ์การประเมินผลกระทบ (IMPACT)

Impact หมายถึง ระดับของผลกระทบหรือความเสียหาย ที่อาจเกิดขึ้นกับองค์กร หากเหตุการณ์ ความเสี่ยงนั้นเกิดขึ้นจริง โดยผลกระทบอาจครอบคลุมทั้งด้าน Financial และ Non-Financial

เกณฑ์การประเมินผลกระทบที่อาจเกิดขึ้น (RISK IMPACT ASSESSMENT)

Impact Level	Financial Loss	Reputation	Stakeholders / Members	Rules & Law / Compliance	Operation	Employee
5 Severe	> 500,000 บาท	สื่อสังคมออนไลน์ เผยแพร่ข่าวหรือข้อมูล ทางด้านลบ	ถูกบุคคลภายนอกหรือ สมาชิกฟ้องร้องหรือ กล่าวหาต่อความเสียหายที่เกิดขึ้น	ถูกยกเลิกสัญญา/ ใบอนุญาต กรรมการ และผู้บริหารระดับสูง ขององค์กรถูกกล่าวหา	กระบวนการหลัก หยุตชะงัก สูญเสีย ความสามารถในการ ให้บริการ	ขวัญกำลังใจลดลง รุนแรง เสี่ยงต่อการ ลาออกหมู่
4 Significant	ระหว่าง 250,001 - 500,000 บาท	ปรากฏข่าวลือที่อาจ พาดพิงองค์กรหรือ สมาชิก IOD	คณะกรรมการ วิทยากร หรือผู้บริหาร ขององค์กรต้องชี้แจง และอธิบายข้อเท็จจริง	ถูกหน่วยงานรัฐ ตรวจสอบและชี้แจง ความผิด	กระบวนการหลักล่าช้า/ ชัดข้องอย่างชัดเจน	พนักงานวิตกกังวล ต้องมีการชี้แจงเป็น ทางการ
3 Moderate	ระหว่าง 100,001 - 250,000 บาท	คณะกรรมการ IOD แสดงความเป็นห่วง เรื่องชื่อเสียง	บุคคลภายนอกหรือ สมาชิกตั้งคำถามต่อ คณะกรรมการหรือ ผู้บริหารขององค์กร	องค์กรอาจต้องส่ง หลักฐานและชี้แจงเป็น ทางการ	มีผลต่อแผนงานหรือ ประสิทธิภาพการ ให้บริการบางส่วน	มีข้อร้องเรียนภายใน/ ความเครียดเพิ่มขึ้น
2 Minor	ระหว่าง 10,001 - 100,000 บาท	มีข่าวลือภายใน	บุคคลภายนอกหรือ สมาชิกเริ่มมีความ สงสัยและสอบถาม ข้อมูล	เกิดการทำความผิด เล็กน้อยที่อาจถูกเตือน หรือปรับตามกฎหมาย แต่ไม่รุนแรง	เกิดความล่าช้าในระดับ ย่อย ไม่กระทบ เป้าหมายหลัก	รับรู้ผลกระทบบ้าง เล็กน้อย
1 Negligible	< 10,000 บาท	แทบจะไม่มี	แทบจะไม่มี	แทบจะไม่มี	ไม่มีผลกระทบต่อการ ดำเนินงาน	ไม่มีผลกระทบต่อ พนักงาน

เกณฑ์การประเมินโอกาสเกิด (LIKELIHOOD)

Likelihood คือ ความน่าจะเป็นที่เหตุการณ์ความเสี่ยงจะเกิดขึ้นภายในช่วงเวลาที่กำหนด โดยพิจารณา ทั้งจากประสบการณ์ในอดีต ความถี่ในการเกิด และลักษณะของการดำเนินงานที่เกี่ยวข้อง

เกณฑ์การประเมินโอกาสเกิด (RISK LIKELIHOOD ASSESSMENT)

Probability Level	คำอธิบาย (Possibility)	% โอกาสที่จะเกิดขึ้นในระยะเวลา 1 ปี
5 Almost Certain	เกิดขึ้นแทบแน่นอนหรือเป็นประจำเกือบทุกปี	> 90%
4 Likely	เป็นไปได้สูง น่าจะเกิดขึ้นในบางรอบปี หรือเกิดในหลายฝ่าย งาน	61% - 90%
3 Possible	น่าจะเป็นไปได้ อาจเกิดขึ้นในบางเงื่อนไข / เคยเกิดขึ้นบางครั้ง	31% - 60%
2 Unlikely	ไม่น่าจะเกิด แต่อาจเป็นไปได้ในบางสถานการณ์	10% - 30%
1 Rare	โอกาสเกิดน้อยมาก หรือไม่เคยเกิดมาก่อน	< 10%

เอกสารแนบท้ายนโยบายบริหารความเสี่ยง 3

การจัดลำดับความเสี่ยง (Degree of Risk)

ระดับความเสี่ยง (Degree of Risk) หมายถึง ค่าความเสี่ยงที่ได้จากการประเมินร่วมกันระหว่าง “โอกาสที่เหตุการณ์จะเกิดขึ้น (Likelihood)” และ “ผลกระทบหากเหตุการณ์นั้นเกิดขึ้น (Impact)” โดยค่าดังกล่าวมักคำนวณจากการนำระดับของ $\text{Impact} \times \text{Likelihood}$ และใช้แสดงออกเป็นระดับของความรุนแรงของความเสี่ยง

เกณฑ์การจัดลำดับความเสี่ยง (Degree of Risk)

ระดับความเสี่ยงโดยรวม	ระดับคะแนน	ความหมาย
Low	1 - 4	ยอมรับได้หรือควบคุมด้วยมาตรการพื้นฐาน แต่ต้องไม่ละเลยจนความเสี่ยงลุกลามหรือเพิ่มระดับขึ้น
Medium	5 - 14	ต้องมีแผนควบคุมอย่างต่อเนื่อง เพื่อให้ระดับความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้
High	15 - 25	ไม่สามารถยอมรับได้ ต้องดำเนินการควบคุมอย่างเร่งด่วน จัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ในทันที

ตารางการจัดลำดับความเสี่ยง (Degree of Risk Matrix)

Likelihood \ Impact					
	1 - Rare	2 - Unlikely	3 - Possible	4 - Likely	5 - Almost Certain
5 - Severe	5	10	15	20	25
4 - Significant	4	8	12	16	20
3 - Moderate	3	6	9	12	15
2 - Minor	2	4	6	8	10
1 - Negligible	1	2	3	4	5

เอกสารแนบท้ายนโยบายบริหารความ

เสี่ยง 4

Key Performance Parameter (KPP)

เกณฑ์วัดผลที่กำหนดเป็นระดับ เพื่อใช้ในการประเมินสถานะของความเสี่ยงในเชิงปฏิบัติ โดยมีเป้าหมายเพื่อแจ้งเตือนล่วงหน้า (Early Warning) และดำเนินการแก้ไขก่อนที่ความเสี่ยงจะส่งผลกระทบต่อระบบ

เมื่อสมาคมฯ อยู่ในสถานการณ์ที่ต้องติดตามความเสี่ยงอย่างต่อเนื่อง หรือความเสี่ยงที่สำคัญระดับองค์กร เช่น ความเสี่ยงที่มี KRIs ชัดเจน (เช่น Turnover Rate, System Downtime, Financial Ratio) ความเสี่ยงที่มีแนวโน้มพัฒนาเร็ว (Operational, Compliance, Reputation) ความเสี่ยงที่อยู่ในแผน BCP หรือ Crisis Plan หรือเป็นความเสี่ยงระดับ High หรือ Medium ที่ต้องมีการติดตามใกล้ชิด และความเสี่ยงที่ต้องรายงานคณะกรรมการ สมาคมฯ กำหนดให้มีการติดตามความเสี่ยงอย่างเป็นระบบ โดยเริ่มการติดตามและจัดการตั้งแต่ความเสี่ยงยังอยู่ในระดับยอมรับได้

ระดับ	ชื่อระดับ	ความหมาย	แนวทางการดำเนินการ
1. Acceptable	ความเสี่ยงอยู่ในระดับยอมรับได้	สถานการณ์อยู่ภายใต้การควบคุม ไม่มีสัญญาณเตือน	ติดตามตามรอบปกติ
2. Trigger	เริ่มมีสัญญาณเตือน	ตัวชี้วัดเริ่มเข้าใกล้ขีดจำกัด/แนวโน้มเสี่ยง	ตรวจสอบต้นเหตุ, แจ้งเตือนผู้เกี่ยวข้อง, เตรียมแผนรองรับ
3. Risky	เกินระดับความเสี่ยงที่ยอมรับได้	ตัวชี้วัดแสดงให้เห็นว่าเกิดความเสี่ยงที่อาจส่งผลกระทบต่อ	ดำเนินการตามแผนฉุกเฉิน / รายงานระดับผู้บริหารทันที