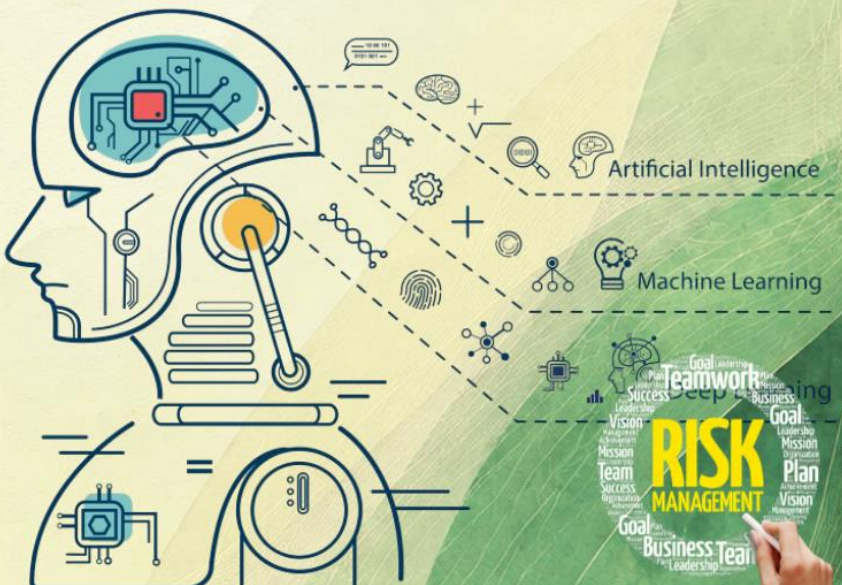
คู่มือการบริหารความเสี่ยง

มหาวิทยาลัยแม่โจ้

ENTERPRISE RISK MANAGEMENT

ฉบับปรับปรุง พ.ศ. 2570



MAEJO UNIVERSITY
ENTERPRISE RISK MANAGEMENT MANUAL
REVISED EDITION 2027

คำนำ

มหาวิทยาลัยแม่โจ้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM) ในฐานะกลไกสำคัญที่สนับสนุนให้สภามหาวิทยาลัยและฝ่ายบริหารสามารถกำกับดูแล ตัดสินใจ และขับเคลื่อนยุทธศาสตร์ภายใต้สภาวะความไม่แน่นอนได้อย่างเหมาะสม มีประสิทธิผล และทันต่อการเปลี่ยนแปลง

การบริหารความเสี่ยงมิใช่เพียงการป้องกันความสูญเสียหรือการจัดทำรายงานให้เป็นไปตามข้อกำหนดเท่านั้น แต่เป็นกระบวนการที่บูรณาการเข้ากับการกำหนดกลยุทธ์ การบริหารผลการดำเนินงาน การจัดสรรทรัพยากร การควบคุมภายใน และการเสริมสร้างความยืดหยุ่นขององค์กร เพื่อสนับสนุนการสร้าง รักษา และเพิ่มคุณค่าให้แก่มหาวิทยาลัยและผู้มีส่วนได้ส่วนเสียอย่างยั่งยืน

คู่มือฉบับนี้จัดทำขึ้นโดยประยุกต์ใช้มาตรฐานและกรอบแนวทางที่เกี่ยวข้อง ได้แก่ ISO 31000:2018, COSO Enterprise Risk Management—Integrating with Strategy and Performance (2017) และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 ตลอดจนแนวทางด้านการควบคุมภายใน การตรวจสอบภายใน และการพัฒนาองค์กรสู่ความเป็นเลิศ เพื่อใช้เป็นกรอบกลางในการบริหารความเสี่ยงของส่วนงานและบุคลากรทุกระดับของมหาวิทยาลัยแม่โจ้ให้เป็นไปในทิศทางและมาตรฐานเดียวกัน

มหาวิทยาลัยมุ่งส่งเสริมให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการบริหารงานและเป็นความรับผิดชอบร่วมกันของบุคลากรทุกระดับ โดยผู้บริหารและเจ้าของความเสี่ยงรับผิดชอบต่อการระบุ ประเมิน จัดการ และติดตามความเสี่ยงในงานที่ตนกำกับ หน่วยงานด้านการบริหารความเสี่ยงทำหน้าที่กำหนดกรอบและมาตรฐาน สนับสนุนเครื่องมือ ข้อมูล และคำปรึกษา ตลอดจนติดตามและรวบรวมภาพรวมความเสี่ยงของมหาวิทยาลัย ขณะที่กองตรวจสอบภายในทำหน้าที่ให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระต่อความเพียงพอและประสิทธิผลของการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายใน

บุคลากรทุกคนมีหน้าที่ตระหนักถึงความเสี่ยง ปฏิบัติตามมาตรการควบคุม รายงานเหตุการณ์หรือสัญญาณเตือนที่สำคัญ และร่วมพัฒนาระบบบริหารความเสี่ยงอย่างต่อเนื่อง เพื่อให้มหาวิทยาลัยสามารถบรรลุวัตถุประสงค์และยุทธศาสตร์ได้อย่างมั่นคง โปร่งใส มีธรรมาภิบาล และยืดหยุ่นต่อการเปลี่ยนแปลง

คณะกรรมการบริหารจัดการความสี่ยง และการควบคุมภายใน
มหาวิทยาลัยแม่โจ้
พ.ศ 2570

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญภาพ

สารบัญตาราง

สารบัญตาราง (ต่อ)

ส่วนที่ 1
บทนำและความสำคัญของการบริหารความเสี่ยง

Introduction and Significance of Risk Management

1.1 ความเป็นมาและความสำคัญ

สภาพแวดล้อมการดำเนินงานของสถาบันอุดมศึกษามีการเปลี่ยนแปลงอย่างรวดเร็ว มีความเชื่อมโยงซับซ้อน และมีความไม่แน่นอนเพิ่มขึ้น ทั้งจากการเปลี่ยนแปลงโครงสร้างประชากรและจำนวนผู้เรียนที่ลดลง ความต้องการของผู้เรียนและตลาดแรงงานที่เปลี่ยนแปลง การแข่งขันด้านการศึกษา การวิจัยและนวัตกรรม ความก้าวหน้าของปัญญาประดิษฐ์และเทคโนโลยีดิจิทัล ความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงและความยั่งยืนทางการเงิน การเปลี่ยนแปลงสภาพภูมิอากาศ ความคาดหวังด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (Environmental, Social and Governance: ESG) ความปลอดภัย ตลอดจนกฎหมาย นโยบาย และมาตรฐานการกำกับดูแลที่มีความซับซ้อนมากขึ้น ปัจจัยดังกล่าวอาจก่อให้เกิดทั้งความเสี่ยงและโอกาสต่อการบรรลุพันธกิจ เป้าประสงค์ และความยั่งยืนในระยะยาวของมหาวิทยาลัย

มหาวิทยาลัยแม่โจ้ได้ประกาศใช้นโยบายการบริหารความเสี่ยงเมื่อวันที่ 23 เมษายน พ.ศ. 2565 เพื่อให้ทุกส่วนงานมีระบบบริหารความเสี่ยงที่เป็นมาตรฐานเดียวกัน อย่างไรก็ตาม บริบท ยุทธศาสตร์ รูปแบบการดำเนินงาน และความคาดหวังของผู้มีส่วนได้ส่วนเสียได้เปลี่ยนแปลงอย่างมีนัยสำคัญ มหาวิทยาลัยจึงทบทวนและยกระดับนโยบาย รวมทั้งปรับปรุงคู่มือการบริหารความเสี่ยง พ.ศ. 2570 จากระบบที่มุ่งเน้นการควบคุมความเสียหายและการจัดทำรายงานตามรอบเวลา ไปสู่กลไกสนับสนุนการกำกับดูแล การบริหาร และการตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเชิงประจักษ์

มหาวิทยาลัยให้ความสำคัญกับการบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM) ในฐานะกลไกที่สนับสนุนให้สภามหาวิทยาลัยและฝ่ายบริหารสามารถกำกับดูแล กำหนดยุทธศาสตร์ พิจารณานโยบายและโครงการ จัดลำดับความสำคัญ จัดสรรทรัพยากร และติดตามผลการดำเนินงานภายใต้ความไม่แน่นอนได้อย่างเหมาะสม โดยพิจารณาความเชื่อมโยง ผลกระทบร่วม และการกระจุกตัวของความเสี่ยงในภาพรวมทั้งมหาวิทยาลัย การบริหารความเสี่ยงตามคู่มือฉบับนี้มิได้มุ่งเพียงหลีกเลี่ยงหรือลดความสูญเสีย แต่ครอบคลุมถึงการบริหารโอกาส การสร้าง รักษา และเพิ่มคุณค่า ตลอดจนการคุ้มครองชื่อเสียง ความเชื่อมั่น ความปลอดภัย และความยั่งยืนของมหาวิทยาลัย การตัดสินใจจึงต้องอาศัยข้อมูลที่ถูกต้อง ครบถ้วน ทันเวลา และเหมาะสมกับระดับการตัดสินใจ หรือการตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเป็นฐาน (Risk-informed and Data-driven Decision-making) พร้อมทั้งติดตามความเสี่ยงเกิดใหม่ ปัจจัยขับเคลื่อนความเสี่ยง และแนวโน้มการเปลี่ยนแปลงอย่างต่อเนื่อง

ระบบบริหารความเสี่ยงต้องเชื่อมโยงระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้ (Risk Appetite: RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) เข้ากับตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators: KRIs) สัญญาณเตือนล่วงหน้า (Early Warning Signals: EWS) เกณฑ์การยกระดับรายงานและการตอบสนอง

(Escalation and Response) ตลอดจนการตัดสินใจของผู้บริหาร (Executive Decision) เพื่อให้มหาวิทยาลัยสามารถเตรียมการและดำเนินมาตรการได้ก่อนที่ความเสี่ยงจะส่งผลกระทบต่อเป้าหมายอย่างมีนัยสำคัญ

มหาวิทยาลัยบูรณาการการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ (Governance, Risk and Compliance: GRC) เข้ากับการควบคุมภายใน การตรวจสอบภายใน การบริหารความต่อเนื่องขององค์กร (Business Continuity Management: BCM) แผนความต่อเนื่องในการดำเนินงาน (Business Continuity Plan: BCP) และการเสริมสร้างความยืดหยุ่นขององค์กร (Organizational Resilience) ตามหลัก Three Lines เพื่อให้บทบาท ความรับผิดชอบ การประสานงาน และการให้ความเชื่อมั่นมีความชัดเจน เชื่อมโยงกัน และไม่ซ้ำซ้อน ตั้งแต่ปีงบประมาณ พ.ศ. 2570 มหาวิทยาลัยปรับประเภทความเสี่ยงหลักจาก 6 ประเภท เป็น 4 ประเภท ได้แก่ ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการดำเนินงาน ความเสี่ยงด้านการเงิน และความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล พร้อมกำหนดให้ชื่อเสียงและความเชื่อมั่น ความปลอดภัย สิ่งแวดล้อมและ ESG ตลอดจนผลกระทบต่อการวิจัยและวิชาการ เป็นมิติผลกระทบร่วม (Cross-cutting Impacts) การจำแนกประเภทดังกล่าวมีวัตถุประสงค์เพื่อสร้างมาตรฐาน ความครอบคลุม และความชัดเจนในการกำหนดเจ้าของความเสี่ยงและสายการรายงาน มิใช่เพื่อแยกการบริหารความเสี่ยงเป็นรายด้านหรือแบบไซโล

คู่มือฉบับปรับปรุง พ.ศ. 2570 จึงเป็นกรอบกลางสำหรับเชื่อมโยงการบริหารความเสี่ยงกับการกำกับดูแล ยุทธศาสตร์ ผลการดำเนินงาน การควบคุมภายใน และการให้ความเชื่อมั่น เพื่อให้ทุกส่วนงานสามารถบริหารความเสี่ยงและโอกาสในทิศทางเดียวกัน สนับสนุนการตัดสินใจได้อย่างทันเวลา และช่วยให้มหาวิทยาลัยดำเนินพันธกิจได้อย่างต่อเนื่อง มั่นคง และยั่งยืน

1.2 วัตถุประสงค์ของคู่มือและการบริหารความเสี่ยง

คู่มือฉบับนี้จัดทำขึ้นเพื่อให้การบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้เป็นระบบ เชื่อมโยงกับการกำกับดูแลและการบริหารมหาวิทยาลัย และสามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรม โดยมีวัตถุประสงค์ดังต่อไปนี้

1. กำหนดมาตรฐานร่วมของมหาวิทยาลัย: เพื่อกำหนดกรอบ หลักการ กระบวนการ เกณฑ์ เครื่องมือ แบบรายงาน และคำศัพท์ด้านการบริหารความเสี่ยงให้มีความชัดเจนและเป็นมาตรฐานเดียวกันทั่วทั้งมหาวิทยาลัย

2. เชื่อมโยงความเสี่ยงกับยุทธศาสตร์และการสร้างคุณค่า: เพื่อบูรณาการความเสี่ยงและโอกาสเข้ากับวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ เป้าประสงค์ ตัวชี้วัด การลงทุน โครงการสำคัญ การจัดสรรทรัพยากร และผลการดำเนินงานของมหาวิทยาลัย

3. สนับสนุนการตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเป็นฐาน: เพื่อให้สภามหาวิทยาลัยและฝ่ายบริหารได้รับข้อมูลความเสี่ยงและโอกาสที่ถูกต้อง ครบถ้วน เชื่อถือได้ ทันเวลา และเหมาะสมกับระดับการตัดสินใจสำหรับใช้ประกอบการกำหนดนโยบาย การอนุมัติโครงการ การจัดลำดับความสำคัญ และการจัดสรรทรัพยากร

4. กำหนดกรอบการยอมรับความเสี่ยงและอำนาจตัดสินใจ: เพื่อกำหนดระดับความเสี่ยงสูงสุดที่มหาวิทยาลัยสามารถรองรับได้ (Risk Capacity) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) รวมทั้งเกณฑ์การยกระดับรายงาน การตอบสนอง และอำนาจตัดสินใจเมื่อความเสี่ยงเข้าใกล้หรือเกินเกณฑ์ที่กำหนด

5. พัฒนาการบริหารความเสี่ยงเชิงรุก: เพื่อให้ทุกส่วนงานสามารถระบุ วิเคราะห์ ประเมิน ตอบสนอง ติดตาม ทบทวน และรายงานความเสี่ยงอย่างเป็นระบบ โดยใช้ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators: KRIs) สัญญาณเตือนล่วงหน้า (Early Warning Signals: EWS) การวิเคราะห์ข้อมูล และการติดตามความเสี่ยงเกิดใหม่

6. กำหนดบทบาทและความรับผิดชอบให้ชัดเจน: เพื่อกำหนดบทบาท หน้าที่ ความเป็นเจ้าของความเสี่ยง อำนาจตัดสินใจ และเส้นทางการรายงานของสภามหาวิทยาลัย ฝ่ายบริหาร คณะกรรมการ ส่วนงาน เจ้าของความเสี่ยง และบุคลากรทุกระดับให้สอดคล้องกับหลัก Three Lines

7. บูรณาการความเสี่ยง การควบคุม และการให้ความเชื่อมั่น: เพื่อเชื่อมโยงการบริหารความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ และการตรวจสอบภายในให้สนับสนุนกันอย่างเป็นระบบ ลดช่องว่างและความซ้ำซ้อน และเพิ่มประสิทธิผลของการกำกับดูแลตามแนวคิด Risk-Control-Assurance

8. เสริมสร้างความพร้อมและความยืดหยุ่นขององค์กร: เพื่อเพิ่มขีดความสามารถในการเตรียมพร้อม รับมือ ตอบสนอง และฟื้นตัวจากเหตุฉุกเฉิน ภาวะวิกฤต เหตุหยุดชะงัก ความเสี่ยงเกิดใหม่ และการเปลี่ยนแปลงที่สำคัญ โดยเชื่อมโยงการบริหารความต่อเนื่องขององค์กรและแผนความต่อเนื่องในการดำเนินงาน (BCM/BCP) รวมทั้งคำนึงถึงมิติ ESG ความปลอดภัย และชื่อเสียง

9. ส่งเสริมวัฒนธรรมความเสี่ยงและการพัฒนาอย่างต่อเนื่อง: เพื่อสร้างความตระหนัก ความโปร่งใส ความรับผิดชอบ และการมีส่วนร่วมของบุคลากรทุกระดับ พร้อมทั้งพัฒนาความรู้และความสามารถ ประเมินระดับการพัฒนาของระบบ และนำผลการประเมินกับบทเรียนที่ได้รับมาปรับปรุงการบริหารความเสี่ยงอย่างต่อเนื่อง

10. เพิ่มความคุ้มค่า ความเชื่อมั่น และความยั่งยืน: เพื่อสนับสนุนการใช้ทรัพยากรอย่างคุ้มค่า การใช้ประโยชน์จากโอกาส การสร้าง รักษา และเพิ่มคุณค่า การคุ้มครองผู้มีส่วนได้ส่วนเสีย ตลอดจนการดำเนินพันธกิจของมหาวิทยาลัยอย่างต่อเนื่องภายใต้ระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้

1.3 ขอบเขตการใช้คู่มือ

คู่มือฉบับนี้ใช้เป็นกรอบกลางสำหรับการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้ ครอบคลุมสภามหาวิทยาลัย คณะกรรมการที่เกี่ยวข้อง ผู้บริหาร ส่วนงาน หน่วยงาน และบุคลากรทุกระดับ ตามโครงสร้าง อำนาจหน้าที่ และความรับผิดชอบที่มีผลใช้บังคับ รวมทั้งใช้เป็นแนวทางในการกำกับความเสี่ยงที่เกิดจากผู้รับจ้าง ผู้ให้บริการ พันธมิตร และบุคคลภายนอกที่เกี่ยวข้องกับการดำเนินพันธกิจของมหาวิทยาลัย ผ่านข้อกำหนดในสัญญาข้อตกลง หรือกลไกการกำกับดูแลที่เหมาะสม

ขอบเขตการใช้คู่มือครอบคลุมหน่วยงานดังต่อไปนี้

- สำนักงานสภามหาวิทยาลัย
- สำนักงานมหาวิทยาลัย
- คณะและวิทยาลัย
- สำนักหรือส่วนงานที่มีฐานะเทียบเท่า
- หน่วยงานวิสาหกิจและหน่วยงานสนับสนุนอื่นตามโครงสร้างของมหาวิทยาลัย

การนำคู่มือไปใช้ให้ยึดหลักความเหมาะสมตามสัดส่วน (Proportionality) โดยคำนึงถึงลักษณะภารกิจ ขนาด ความซับซ้อน บริบท ผู้มีส่วนได้ส่วนเสีย และระดับความเสี่ยงของแต่ละส่วนงาน ทั้งนี้ การประยุกต์ใช้ตามความเหมาะสมต้องไม่ลดทอนหลักการ ข้อกำหนดขั้นต่ำ หรือหน้าที่ความรับผิดชอบตามกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง และนโยบายที่เกี่ยวข้อง

หากข้อความในคู่มือขัดหรือแย้งกับกฎหมาย ระเบียบ หรือข้อบังคับที่มีผลใช้บังคับ ให้ยึดถือกฎหมาย ระเบียบ หรือข้อบังคับนั้นเป็นสำคัญ และให้หน่วยงานผู้รับผิดชอบเสนอทบทวนหรือปรับปรุงคู่มือให้สอดคล้องโดยเร็ว

1.4 ความหมายและองค์ประกอบที่ใช้ในการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง ผลกระทบของความไม่แน่นอนต่อวัตถุประสงค์ ซึ่งอาจทำให้ผลการดำเนินงานเบี่ยงเบนจากผลลัพธ์ที่คาดหวังทั้งในด้านลบและด้านบวก ดังนั้น ความเสี่ยงทุกรายการต้องเชื่อมโยงกับวัตถุประสงค์ ยุทธศาสตร์ เป้าประสงค์ หรือผลลัพธ์ที่ต้องการบรรลุอย่างชัดเจน และไม่ควรระบุเป็นเพียงปัญหาที่เกิดขึ้นแล้ว ผลกระทบปลายทาง หรือข้อความทั่วไปที่ไม่สามารถประเมิน มอบหมายผู้รับผิดชอบ และกำหนดแนวทางจัดการได้ การเขียนข้อความความเสี่ยง (Risk Statement) ควรแสดงความสัมพันธ์ระหว่างสาเหตุ เหตุการณ์ และผลกระทบ โดยใช้โครงสร้างดังนี้

“เนื่องจาก [สาเหตุหรือปัจจัยขับเคลื่อนความเสี่ยง] อาจทำให้เกิด [เหตุการณ์หรือความไม่แน่นอน] ส่งผลให้ [วัตถุประสงค์ ยุทธศาสตร์ หรือผู้มีส่วนได้ส่วนเสียได้รับผลกระทบอย่างไร]”

องค์ประกอบสำคัญที่ใช้ในการระบุและวิเคราะห์ความเสี่ยง ประกอบด้วย

1. **วัตถุประสงค์ (Objective):** ผลลัพธ์ที่มหาวิทยาลัยหรือส่วนงานต้องการบรรลุ ซึ่งใช้เป็นจุดอ้างอิงในการระบุและประเมินความเสี่ยง
2. **สาเหตุหรือปัจจัยขับเคลื่อนความเสี่ยง (Cause/Risk Driver):** ปัจจัย เงื่อนไข หรือการเปลี่ยนแปลงทั้งภายในและภายนอกที่อาจทำให้ความเสี่ยงมีโอกาสเกิดขึ้นหรือมีความรุนแรงเพิ่มขึ้น
3. **เหตุการณ์ความเสี่ยง (Risk Event):** เหตุการณ์ สถานการณ์ หรือความไม่แน่นอนที่อาจเกิดขึ้นและส่งผลต่อการบรรลุวัตถุประสงค์
4. **ผลกระทบหรือผลสืบเนื่อง (Impact/Consequence):** ผลที่อาจเกิดขึ้นต่อวัตถุประสงค์ ยุทธศาสตร์ การเงิน การดำเนินงาน การปฏิบัติตามกฎหมาย ชื่อเสียง ความปลอดภัย สิ่งแวดล้อม ผู้มีส่วนได้ส่วนเสีย หรือความต่อเนื่องของพันธกิจ
5. **โอกาสเกิด (Likelihood):** ความน่าจะเป็นหรือความถี่ที่เหตุการณ์ความเสี่ยงอาจเกิดขึ้นภายในช่วงเวลาที่กำหนด
6. **การควบคุมที่มีอยู่ (Existing Controls):** นโยบาย กระบวนการ ระบบ หรือกิจกรรมที่ได้ออกแบบและนำไปปฏิบัติ เพื่อลดโอกาสเกิด ลดผลกระทบ ตรวจจับเหตุการณ์ หรือเพิ่มความพร้อมในการตอบสนองต่อความเสี่ยง
7. **เจ้าของความเสี่ยง (Risk Owner):** ผู้มีอำนาจและความรับผิดชอบในการตัดสินใจ บริหาร ติดตาม และรายงานความเสี่ยงที่ได้รับมอบหมาย

8. **กรอบเวลา (Time Horizon):** ช่วงเวลาที่ความเสี่ยงอาจเกิดขึ้นหรือส่งผลกระทบ ซึ่งใช้ประกอบการประเมินความเร่งด่วนและกำหนดระยะเวลาตอบสนอง

ความเสี่ยงสามารถพิจารณาได้สองมุมมอง ได้แก่

- **ภัยคุกคามหรือความเสี่ยงเชิงลบ (Threat):** ความไม่แน่นอนที่อาจก่อให้เกิดความสูญเสีย ความเสียหาย การหยุดชะงัก หรือทำให้มหาวิทยาลัยไม่สามารถบรรลุวัตถุประสงค์ตามที่กำหนด
- **โอกาส (Opportunity):** ความไม่แน่นอนที่อาจนำไปสู่ผลลัพธ์ที่ดีกว่าคาด การพัฒนานวัตกรรม การเพิ่มประสิทธิภาพ หรือการสร้างคุณค่า ทั้งนี้ การแสวงหาและใช้ประโยชน์จากโอกาสต้องอยู่ภายใต้หลักธรรมาภิบาล ข้อจำกัดตามกฎหมาย และระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้

ตารางที่ 1-1 *ความแตกต่างระหว่างความเสี่ยง (**Risk**) และปัญหาหรือเหตุการณ์ (**Issue/Event**)*

ประเด็น	ความเสี่ยง (Risk)	ปัญหาหรือเหตุการณ์ (Issue/Event)
สถานะ	ยังมีความไม่แน่นอนว่าอาจเกิดขึ้น	เกิดขึ้นแล้วหรือกำลังเกิดขึ้น
แนวทางหลัก	ป้องกัน ลด เตรียมพร้อม หรือแสวงหาโอกาส	ระงับเหตุ แก้ไข ฟื้นฟู และลดผลกระทบ
การประเมิน	ประเมินโอกาสเกิดและผลกระทบ	ประเมินความรุนแรง ผลเสีย และความเร่งด่วน
ลักษณะการบริหาร	เชิงรุกและมองไปข้างหน้า	ตอบสนองเหตุการณ์และแก้ไขปัญหา
ความเชื่อมโยง	ความเสี่ยงที่จัดการไม่เพียงพออาจกลายเป็นปัญหา	ปัญหาที่เกิดขึ้นเป็นข้อมูลสำหรับทบทวนความเสี่ยงและการควบคุม

เมื่อเกิดปัญหาหรือเหตุการณ์แล้ว ส่วนงานต้องดำเนินการระงับเหตุ แก้ไข ฟื้นฟู และรายงานตามกระบวนการที่กำหนด พร้อมทั้งวิเคราะห์สาเหตุราก ทบทวนทะเบียนความเสี่ยง ระดับความเสี่ยง และประสิทธิผลของการควบคุม และบทเรียนที่ได้รับ เพื่อป้องกันการเกิดซ้ำและปรับปรุงระบบอย่างต่อเนื่อง

1.5 ความสำคัญและประโยชน์ของการบริหารความเสี่ยง

การบริหารความเสี่ยงที่มีประสิทธิผลและบูรณาการเป็นองค์ประกอบสำคัญของการกำกับดูแลและการบริหารมหาวิทยาลัย ช่วยให้มหาวิทยาลัยสามารถดำเนินพันธกิจภายใต้ความไม่แน่นอน ใช้ประโยชน์จากโอกาส และรักษาความต่อเนื่องของการดำเนินงาน โดยก่อให้เกิดประโยชน์สำคัญดังต่อไปนี้

1. สนับสนุนการบรรลุยุทธศาสตร์: ช่วยให้มหาวิทยาลัยเข้าใจปัจจัย ความไม่แน่นอน และเงื่อนไขที่อาจส่งผลต่อวิสัยทัศน์ พันธกิจ เป้าประสงค์ และตัวชี้วัดสำคัญ รวมทั้งสามารถพิจารณาทางเลือกและโอกาสเชิงยุทธศาสตร์ได้อย่างรอบด้าน

2. ยกระดับคุณภาพการตัดสินใจ: ช่วยให้สภามหาวิทยาลัยและฝ่ายบริหารสามารถเปรียบเทียบทางเลือก ผลได้ ผลเสีย สมมติฐาน ความไม่แน่นอน และระดับความเสี่ยง ก่อนกำหนดนโยบาย อนุมัติแผนงานหรือโครงการ และตัดสินใจลงทุน

3. เพิ่มประสิทธิภาพการจัดสรรทรัพยากร: ช่วยให้มหาวิทยาลัยจัดลำดับความสำคัญและจัดสรรงบประมาณ บุคลากร เทคโนโลยี และทรัพยากรอื่นให้เหมาะสมกับระดับความเสี่ยง ความเร่งด่วน และความสำคัญเชิงยุทธศาสตร์

4. เสริมสร้างธรรมาภิบาลและความรับผิดชอบ: ทำให้บทบาท หน้าที่ ความเป็นเจ้าของความเสี่ยง ระดับอำนาจในการยอมรับความเสี่ยง และเส้นทางการรายงานมีความชัดเจน โปร่งใส ตรวจสอบได้ และสอดคล้องกับหลัก Three Lines

5. พัฒนาการควบคุมภายในให้เหมาะสมกับความเสี่ยง: ช่วยให้มาตรการควบคุมตอบสนองต่อสาเหตุและระดับความเสี่ยงอย่างเหมาะสม ลดช่องว่างของการควบคุม ไม่สร้างภาระเกินความจำเป็น และสามารถประเมินประสิทธิผลได้จากหลักฐานเชิงประจักษ์

6. ลดความสูญเสียและผลกระทบจากการหยุดชะงัก: เพิ่มความพร้อมในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นตัวจากเหตุฉุกเฉิน ภาวะวิกฤต เหตุการณ์ไซเบอร์ ภัยพิบัติ และเหตุหยุดชะงักที่อาจกระทบต่อพันธกิจสำคัญของมหาวิทยาลัย

7. ส่งเสริมวัฒนธรรมความเสี่ยงและการเรียนรู้: สนับสนุนให้บุคลากรตระหนักถึงความเสี่ยง กล้ารายงานสัญญาณเตือน เหตุการณ์ และข้อผิดพลาดโดยสุจริต มีความรับผิดชอบต่อความเสี่ยงในขอบเขตงานของตน และนำบทเรียนมาใช้ป้องกันการเกิดซ้ำ

8. เพิ่มความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย: แสดงให้เห็นว่ามหาวิทยาลัยมีระบบบริหารจัดการที่มีประสิทธิภาพ โปร่งใส รับผิดชอบ และสามารถรับมือกับความไม่แน่นอนได้อย่างเหมาะสม อันช่วยเสริมสร้างความเชื่อมั่นของนักศึกษา บุคลากร หน่วยงานกำกับดูแล คู่ความร่วมมือ และสังคม

9. สนับสนุนคุณภาพและความเป็นเลิศขององค์กร: เชื่อมโยงข้อมูลความเสี่ยงกับการประกันคุณภาพ เกณฑ์คุณภาพการศึกษาเพื่อการดำเนินการที่เป็นเลิศ (EdPEx) การควบคุมภายใน การตรวจสอบภายใน และการปรับปรุงผลการดำเนินงานอย่างต่อเนื่อง

10. สร้างคุณค่า ความยืดหยุ่น และความยั่งยืน: ช่วยให้มหาวิทยาลัยสามารถปรับตัวต่อการเปลี่ยนแปลง รักษาพันธกิจสำคัญ ใช้ประโยชน์จากโอกาส สร้างและปกป้องคุณค่า ตลอดจนดำเนินงานโดยคำนึงถึงสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG) เพื่อความยั่งยืนในระยะยาว

1.6 หลักการบริหารความเสี่ยงตาม ISO 31000:2018

มหาวิทยาลัยแม่โจ้ประยุกต์ใช้หลักการบริหารความเสี่ยงตามมาตรฐาน ISO 31000:2018 เพื่อให้ระบบบริหารความเสี่ยงสามารถสร้างและคุ้มครองคุณค่า สนับสนุนการตัดสินใจ และช่วยให้มหาวิทยาลัยบรรลุวัตถุประสงค์ภายใต้ความไม่แน่นอน โดยประกอบด้วยหลักการสำคัญ 8 ประการ ดังต่อไปนี้

1. บูรณาการ (Integrated): การบริหารความเสี่ยงเป็นส่วนหนึ่งของการกำกับดูแล การกำหนดยุทธศาสตร์ การวางแผน การบริหารผลการดำเนินงาน การบริหารโครงการ การจัดสรรทรัพยากร และการตัดสินใจในทุกระดับ มิใช่กระบวนการที่ดำเนินการแยกจากงานประจำ

2. มีโครงสร้างและครอบคลุม (Structured and Comprehensive): การบริหารความเสี่ยงต้องดำเนินการอย่างเป็นระบบ มีโครงสร้างและแนวทางที่สม่ำเสมอ ครอบคลุมความเสี่ยงที่สำคัญ และทำให้ผลการประเมินสามารถเปรียบเทียบ ติดตาม และรายงานได้อย่างเหมาะสม

3. เหมาะสมกับบริบท (Customized): กรอบและกระบวนการบริหารความเสี่ยงต้องออกแบบให้เหมาะสมและได้สัดส่วนกับบริบทภายในและภายนอก วัตถุประสงค์ โครงสร้าง ภารกิจ วัฒนธรรม และระดับความซับซ้อนของมหาวิทยาลัยและแต่ละส่วนงาน

4. มีส่วนร่วม (Inclusive): ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องควรได้รับโอกาสให้มีส่วนร่วมอย่างเหมาะสมและทันเวลา เพื่อให้ข้อมูล ความรู้ ประสบการณ์ และมุมมองที่หลากหลายได้รับการพิจารณา ส่งผลให้การระบุและประเมินความเสี่ยงมีความรอบด้านและเป็นที่ยอมรับร่วมกัน

5. มีพลวัต (Dynamic): การบริหารความเสี่ยงต้องสามารถคาดการณ์ ตรวจจับ รับรู้ และตอบสนองต่อการเปลี่ยนแปลงของบริบทได้อย่างทันท่วงที เนื่องจากความเสี่ยงอาจเกิดขึ้นใหม่ เปลี่ยนแปลง เพิ่มขึ้น ลดลง หรือหมดความสำคัญไปตามสถานการณ์

6. ใช้สารสนเทศที่ดีที่สุดเท่าที่มี (Best Available Information): การตัดสินใจด้านความเสี่ยงควรใช้ข้อมูลในอดีต ข้อมูลปัจจุบัน การคาดการณ์ และความเห็นจากผู้เชี่ยวชาญเท่าที่มีอยู่ โดยต้องพิจารณาคุณภาพ ความทันเวลา ความน่าเชื่อถือ ข้อจำกัด ความไม่แน่นอน และสมมติฐานของข้อมูลอย่างโปร่งใส

7. คำนึงถึงปัจจัยมนุษย์และวัฒนธรรม (Human and Cultural Factors): การบริหารความเสี่ยงต้องคำนึงถึงค่านิยม ทัศนคติ พฤติกรรม ความรู้ ความสามารถ แรงจูงใจ อคติ และวัฒนธรรมองค์กร เนื่องจากปัจจัยเหล่านี้มีอิทธิพลต่อการรับรู้ การตัดสินใจ และการจัดการความเสี่ยงในทุกระดับ

8. ปรับปรุงอย่างต่อเนื่อง (Continual Improvement): มหาวิทยาลัยต้องทบทวนและพัฒนากรอบ กระบวนการ เครื่องมือ ข้อมูล ความสามารถของบุคลากร และวัฒนธรรมความเสี่ยงอย่างต่อเนื่อง โดยใช้ผลการติดตาม เหตุการณ์ที่เกิดขึ้น ข้อสังเกตจากการตรวจสอบ การเปลี่ยนแปลงของบริบท และบทเรียนที่ได้รับเป็นข้อมูลประกอบการปรับปรุง

หลักการทั้ง 8 ประการเป็นคุณลักษณะพื้นฐานของการบริหารความเสี่ยงที่มีประสิทธิผล มีเป้าหมายเพื่อสนับสนุนการสร้างและคุ้มครองคุณค่าของมหาวิทยาลัย มิใช่ขั้นตอนของกระบวนการที่ต้องดำเนินการตามลำดับ ทั้งนี้ มหาวิทยาลัยและส่วนงานต้องนำหลักการดังกล่าวไปประยุกต์ใช้ร่วมกันตลอดกระบวนการบริหารความเสี่ยงและการตัดสินใจทุกระดับ

1.7 ความเชื่อมโยงระหว่างธรรมาภิบาล การบริหารความเสี่ยง การควบคุมภายใน และการให้ความเชื่อมั่น

ธรรมาภิบาล การบริหารความเสี่ยง การควบคุมภายใน และการให้ความเชื่อมั่นเป็นองค์ประกอบของระบบกำกับดูแลที่ต้องออกแบบและดำเนินการให้เชื่อมโยงกัน เพื่อสนับสนุนการบรรลุวัตถุประสงค์ของมหาวิทยาลัย ลดช่องว่างและความซ้ำซ้อนของการดำเนินงาน และทำให้ผู้กำกับดูแลได้รับข้อมูลที่เพียงพอสำหรับการตัดสินใจ โดยมีสาระสำคัญดังนี้

- **ธรรมาภิบาล (Governance):** ระบบและกระบวนการที่ใช้กำหนดทิศทาง กำกับดูแล มอบหมายความรับผิดชอบ กำหนดอำนาจตัดสินใจ ติดตามผล และดูแลให้มหาวิทยาลัยดำเนินงานอย่างโปร่งใส รับผิดชอบ และคำนึงถึงผู้มีส่วนได้ส่วนเสีย
- **การบริหารความเสี่ยง (Risk Management):** กระบวนการระบุ วิเคราะห์ ประเมิน ตอบสนอง ติดตาม ทบทวน และสื่อสารความเสี่ยงและโอกาสที่อาจส่งผลต่อการบรรลุวัตถุประสงค์
- **การควบคุมภายใน (Internal Control):** นโยบาย กระบวนการ ระบบ และกิจกรรมที่ออกแบบและดำเนินการเพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลต่อการบรรลุวัตถุประสงค์ด้านการดำเนินงาน การรายงาน และการปฏิบัติตามกฎหมายและข้อกำหนด
- **การให้ความเชื่อมั่น (Assurance):** การประเมินอย่างเป็นระบบต่อความเพียงพอและประสิทธิผลของธรรมาภิบาล การบริหารความเสี่ยง และการควบคุมภายใน โดยต้องระบุแหล่งที่มา ขอบเขต วิธีการ และระดับความเป็นอิสระของผู้ให้ความเชื่อมั่นอย่างชัดเจน

ความเชื่อมโยงดังกล่าวให้พิจารณาตามลำดับจาก **วัตถุประสงค์ ⟶ ความเสี่ยง ⟶ การควบคุม ⟶ การให้ความเชื่อมั่น ⟶ การรายงานต่อผู้กำกับดูแล** เพื่อให้สามารถตรวจสอบได้ว่าความเสี่ยงสำคัญมีการควบคุมที่เหมาะสม การควบคุมทำงานได้ตามที่ออกแบบ และผู้กำกับดูแลได้รับความเชื่อมั่นที่เพียงพอ

มหาวิทยาลัยกำหนดสายการกำกับดูแล การบริหาร การปฏิบัติ และการให้ความเชื่อมั่นตามหลัก Three Lines ดังนี้

1. **สภามหาวิทยาลัยและคณะกรรมการที่เกี่ยวข้อง (Governing Body):** กำหนดทิศทางและความคาดหวังด้านธรรมาภิบาล อนุมัตินโยบายและระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้ กำกับและติดตามการดำเนินงานของฝ่ายบริหาร รวมทั้งรับข้อมูลด้านความเสี่ยง การควบคุม และการให้ความเชื่อมั่นที่เพียงพอ ทันเวลา และเหมาะสมต่อการกำกับดูแล ตลอดจนสนับสนุนความเป็นอิสระของการตรวจสอบภายใน
2. **บทบาทสายงานที่หนึ่ง (First Line Roles):** ฝ่ายบริหาร ผู้บริหารส่วนงาน เจ้าของวัตถุประสงค์ เจ้าของกระบวนการ และเจ้าของความเสี่ยง รับผิดชอบต่อการดำเนินงานและผลลัพธ์ในงานที่ตนกำกับ รวมทั้งระบุ ประเมิน ตอบสนอง ติดตาม และรายงานความเสี่ยง ตลอดจนออกแบบ นำไปปฏิบัติ และประเมินการควบคุมภายในที่เกี่ยวข้อง
3. **บทบาทสายงานที่สอง (Second Line Roles):** หน่วยงานหรือผู้รับผิดชอบด้านการบริหารความเสี่ยง การควบคุมภายใน กฎหมายและการปฏิบัติตามกฎเกณฑ์ ความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล ความปลอดภัย BCM/BCP และหน้าที่กำกับเฉพาะด้าน ทำหน้าที่กำหนดกรอบ มาตรฐาน และเครื่องมือ ให้คำปรึกษา สนับสนุนข้อมูล ติดตาม วิเคราะห์ภาพรวม และท้าทายการตัดสินใจอย่างสร้างสรรค์ โดยไม่รับผิดชอบหรือบริหารความเสี่ยงแทนเจ้าของความเสี่ยง

4. **บทบาทสายงานที่สาม (Third Line Roles):** กองตรวจสอบภายในให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรมต่อความเพียงพอและประสิทธิผลของธรรมาภิบาล การบริหารความเสี่ยง และการควบคุมภายใน โดยรายงานผลต่อสภามหาวิทยาลัยหรือคณะกรรมการตรวจสอบตามโครงสร้างที่มหาวิทยาลัยกำหนด

5. **ผู้ให้ความเชื่อมั่นอื่น (Other Assurance Providers):** ผู้สอบบัญชี ผู้ประเมินภายนอก หน่วยรับรอง หน่วยงานกำกับดูแล และผู้เชี่ยวชาญอิสระ ให้ความเชื่อมั่นตามขอบเขต อำนาจหน้าที่ และระดับความเป็นอิสระของแต่ละหน่วยงาน ทั้งนี้ ผู้ให้ความเชื่อมั่นอื่นมิใช่ส่วนหนึ่งของ Three Lines แต่ควรประสานแผน ขอบเขต และผลการประเมินกับมหาวิทยาลัย เพื่อเพิ่มความครอบคลุม ลดความซ้ำซ้อน และป้องกันช่องว่างของการให้ความเชื่อมั่น

การจัดวางบทบาทตามหลัก Three Lines มิได้มีวัตถุประสงค์เพื่อแยกการทำงานเป็นไซโล แต่เพื่อให้ทุกฝ่ายประสานงานและแลกเปลี่ยนข้อมูลอย่างเหมาะสม โดยยังคงรักษาความรับผิดชอบ อำนาจหน้าที่ และระดับความเป็นอิสระของแต่ละบทบาท

กองตรวจสอบภายในต้องไม่รับผิดชอบบริหารความเสี่ยงแทนฝ่ายบริหาร และไม่ควรเป็นผู้กำหนด RA/RT เป็นเจ้าของทะเบียนความเสี่ยง เลือกหรือนำมาตรการควบคุมไปปฏิบัติ หรือรับผิดชอบต่อผลการบริหารความเสี่ยง หากได้รับมอบหมายภารกิจที่อาจกระทบต่อความเป็นอิสระหรือความเที่ยงธรรม ต้องเปิดเผยลักษณะของภารกิจ ขออนุมัติจากผู้กำกับดูแล กำหนดขอบเขตและระยะเวลาให้ชัดเจน และจัดให้มีมาตรการคุ้มครองหรือการให้ความเชื่อมั่นจากผู้ที่มีความเป็นอิสระอย่างเหมาะสม

1.8 กฎหมาย หลักเกณฑ์ และมาตรฐานอ้างอิง

คู่มือฉบับนี้จัดทำขึ้นภายใต้กฎหมาย หลักเกณฑ์ นโยบาย และข้อกำหนดที่เกี่ยวข้อง พร้อมทั้งประยุกต์ใช้มาตรฐานและกรอบแนวปฏิบัติที่เป็นที่ยอมรับ โดยจำแนกเอกสารอ้างอิงตามสถานะและวัตถุประสงค์ ดังนี้

1.8.1 กฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

1. พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 และที่แก้ไขเพิ่มเติม
2. พระราชบัญญัติมหาวิทยาลัยแม่โจ้ พ.ศ. 2560 และที่แก้ไขเพิ่มเติม
3. พระราชบัญญัติการอุดมศึกษา พ.ศ. 2562 และที่แก้ไขเพิ่มเติม
4. หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 และที่แก้ไขเพิ่มเติม ตามหนังสือกระทรวงการคลัง ที่ กค 0409.4/ว 23 ลงวันที่ 19 มีนาคม 2562 กรมบัญชีกลาง
5. แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กร ของกระทรวงการคลังหรือกรมบัญชีกลาง ฉบับที่มีผลใช้บังคับ
6. หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 และที่แก้ไขเพิ่มเติม

7. หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 และที่แก้ไขเพิ่มเติม ซึ่งปัจจุบันรวมถึงฉบับที่ 4 พ.ศ. 2566 กรมบัญชีกลาง

8. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และที่แก้ไขเพิ่มเติม

9. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และที่แก้ไขเพิ่มเติม

10. พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 รวมทั้งระเบียบและประกาศที่เกี่ยวข้อง

11. พระราชบัญญัติมาตรฐานทางจริยธรรม พ.ศ. 2562 ตลอดจนกฎหมายและข้อกำหนดด้านการป้องกันการทุจริตและประพฤติมิชอบที่เกี่ยวข้อง

12. กฎหมาย กฎกระทรวง ประกาศ และแนวปฏิบัติด้านมาตรฐานการอุดมศึกษา ธรรมาภิบาลของสถาบันอุดมศึกษา การวิจัยและจริยธรรมการวิจัยที่เกี่ยวข้อง

13. กฎหมายและข้อกำหนดด้านความปลอดภัย อาชีวอนามัย สิ่งแวดล้อม การสาธารณสุข การป้องกันและบรรเทาสาธารณภัย และการจัดการภาวะฉุกเฉินที่เกี่ยวข้อง

14. ข้อบังคับ ระเบียบ นโยบาย ประกาศ คำสั่ง และมติของสภามหาวิทยาลัยหรือมหาวิทยาลัยแม่โจ้ที่เกี่ยวข้อง

1.8.2 มาตรฐานและกรอบแนวปฏิบัติที่นำมาประยุกต์ใช้

15. ISO 31000:2018, *Risk Management—Guidelines* และฉบับที่มีผลใช้บังคับ

16. COSO, *Enterprise Risk Management—Integrating with Strategy and Performance* (2017)

17. COSO, *Internal Control—Integrated Framework* (2013)

18. ISO 22301:2019, *Security and Resilience—Business Continuity Management Systems—Requirements* รวมทั้งฉบับแก้ไขเพิ่มเติมที่มีผลใช้บังคับ เพื่อสนับสนุนการบริหารความต่อเนื่องขององค์กรและแผนความต่อเนื่องในการดำเนินงาน (BCM/BCP) ISO

19. มาตรฐานการตรวจสอบภายในสากล (*Global Internal Audit Standards*) และกรอบมาตรฐานวิชาชีพการตรวจสอบภายในสากล (*International Professional Practices Framework: IPPF*) ฉบับที่มีผลใช้บังคับ โดยมาตรฐานปัจจุบันมีผลตั้งแต่วันที่ 9 มกราคม 2025 The Institute of Internal Auditors

20. แนวคิด Three Lines ของ The Institute of Internal Auditors และแนวทางการประสานการให้ความเชื่อมั่น (*Assurance Coordination/Combined Assurance*) ฉบับที่มีผลใช้บังคับ The IIA Statements of Position

21. เป้าหมายการพัฒนาที่ยั่งยืน (*Sustainable Development Goals: SDGs*) และแนวคิดด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (*Environmental, Social and Governance: ESG*) ที่มหาวิทยาลัยนำมาประยุกต์ใช้

22. เกณฑ์คุณภาพการศึกษาเพื่อการดำเนินการที่เป็นเลิศ (*Education Criteria for Performance Excellence: EdPEx*) ฉบับที่มหาวิทยาลัยประกาศหรือกำหนดใช้

1.9 ปัจจัยแห่งความสำเร็จของการบริหารความเสี่ยง

การบริหารความเสี่ยงจะสามารถสร้าง ปกป้อง และเพิ่มคุณค่าให้แก่มหาวิทยาลัย รวมทั้งเกิดผลอย่างเป็นรูปธรรมได้ ต้องอาศัยปัจจัยแห่งความสำเร็จที่สำคัญ ดังนี้

1. ความมุ่งมั่นของผู้กำกับดูแลและผู้บริหาร (Governance and Leadership Commitment): สภามหาวิทยาลัยและผู้บริหารกำหนดทิศทาง แสดงพฤติกรรมต้นแบบ กำกับติดตาม สนับสนุนทรัพยากรที่จำเป็น และนำข้อมูลความเสี่ยงและโอกาสมาใช้ประกอบการตัดสินใจอย่างจริงจัง

2. การเชื่อมโยงกับยุทธศาสตร์และผลการดำเนินงาน (Strategy and Performance Integration): เชื่อมโยงความเสี่ยงกับวิสัยทัศน์ พันธกิจ วัตถุประสงค์เชิงยุทธศาสตร์ ตัวชี้วัดผลการดำเนินงาน การลงทุน โครงการสำคัญ งบประมาณ และผลลัพธ์ที่มหาวิทยาลัยต้องการบรรลุ

3. บทบาท ความรับผิดชอบ และอำนาจตัดสินใจที่ชัดเจน (Clear Accountability and Decision Rights): กำหนดเจ้าของความเสี่ยง (Risk Owner) เจ้าของมาตรการ (Action Owner) เจ้าของข้อมูล (Data Owner) ผู้มีอำนาจอนุมัติ ตลอดจนเส้นทางและระดับการยกระดับรายงานความเสี่ยงอย่างชัดเจนตามหลัก Three Lines

4. กรอบระดับความเสี่ยงที่ยอมรับได้ที่นำไปใช้จริง (Actionable Risk Appetite and Risk Tolerance): กำหนดระดับความสามารถในการรองรับความเสี่ยง (Risk Capacity) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) ให้ชัดเจน สื่อสารให้ผู้เกี่ยวข้องเข้าใจ และนำไปใช้ในการอนุมัติ ติดตาม และยกระดับการตัดสินใจ

5. ข้อมูลความเสี่ยงที่มีคุณภาพและเชื่อถือได้ (Reliable Risk Information): ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators: KRIs) และรายงานความเสี่ยงต้องมีนิยาม สูตรคำนวณ แหล่งข้อมูล เจ้าของข้อมูล ความถี่ในการรายงาน ค่าเป้าหมาย และเกณฑ์กระตุ้นการดำเนินการที่ชัดเจน โดยข้อมูลต้องถูกต้อง ครบถ้วน ทันเวลา และสามารถตรวจสอบย้อนกลับได้

6. การบูรณาการกับกระบวนการบริหารและงานประจำ (Integration into Management Processes): บูรณาการการบริหารความเสี่ยงเข้ากับการวางแผนยุทธศาสตร์ การจัดทำงบประมาณ การบริหารโครงการ การบริหารผลการดำเนินงาน การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ การประกันคุณภาพ การบริหารความต่อเนื่องขององค์กร (BCM/BCP) และการติดตามผลในทุกระดับ

7. วัฒนธรรมความเสี่ยงและสภาพแวดล้อมที่เอื้อต่อการรายงาน (Risk Culture and Speak-up Environment): ส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยง รับผิดชอบต่อความเสี่ยงในขอบเขตงาน และสามารถรายงานสัญญาณเตือน เหตุการณ์ ข้อผิดพลาด หรือข้อกังวลโดยสุจริตและได้รับการคุ้มครองอย่างเหมาะสม เพื่อให้เกิดการเรียนรู้และป้องกันการปกปิดข้อมูลสำคัญ

8. ความรู้และความสามารถของบุคลากร (Risk Competency and Capability): พัฒนาความรู้ ทักษะ และเครื่องมือในการกำหนดวัตถุประสงค์ ระบุ วิเคราะห์ ประเมิน ตอบสนอง ติดตาม และสื่อสารความเสี่ยงให้เหมาะสมกับบทบาท ความรับผิดชอบ และระดับการตัดสินใจของบุคลากรแต่ละกลุ่ม

9. การติดตาม สัญญาณเตือน และการยกระดับที่ทันเวลา (Monitoring, Early Warning and Timely Escalation): กำหนดรอบการติดตาม สัญญาณเตือนล่วงหน้า เกณฑ์การยกระดับรายงาน (Escalation Criteria) ผู้มีอำนาจตัดสินใจ และระยะเวลาการตอบสนองให้สอดคล้องกับระดับความรุนแรง ความเร่งด่วน และแนวโน้มของความเสี่ยง

10. การควบคุมและมาตรการตอบสนองที่มีประสิทธิผล (Effective Controls and Risk Responses): ออกแบบมาตรการให้ตอบสนองต่อสาเหตุหรือปัจจัยขับเคลื่อนความเสี่ยง มีผู้รับผิดชอบ ระยะเวลา ทรัพยากร และตัววัดผลสำเร็จที่ชัดเจน พร้อมประเมินทั้งความเพียงพอของการออกแบบและประสิทธิผลในการปฏิบัติ

11. การประสานงานและการให้ความเชื่อมั่นที่เหมาะสม (Coordinated Assurance): ประสานข้อมูลและแผนงานระหว่างฝ่ายบริหาร หน่วยงานกำกับเฉพาะด้าน ผู้ประเมิน และกองตรวจสอบภายใน เพื่อให้การให้ความเชื่อมั่นครอบคลุมความเสี่ยงสำคัญ ลดช่องว่างและความซ้ำซ้อน โดยคงไว้ซึ่งความเป็นอิสระและความเที่ยงธรรมของการตรวจสอบภายใน

12. การทบทวน เรียนรู้ และปรับปรุงอย่างต่อเนื่อง (Learning and Continual Improvement): ใช้ผลการติดตาม เหตุการณ์จริง ข้อร้องเรียน ข้อสังเกตจากการตรวจสอบ การทดสอบ BCM/BCP ความคิดเห็นของผู้มีส่วนได้ส่วนเสีย และบทเรียนที่ได้รับ มาทบทวนและพัฒนากรอบ กระบวนการ เครื่องมือ ข้อมูล และความสามารถด้านการบริหารความเสี่ยงอย่างต่อเนื่อง

หลักสำคัญ: ความสำเร็จของการบริหารความเสี่ยงมิได้วัดจากความครบถ้วนของเอกสารหรือรายงานเพียงอย่างเดียว แต่พิจารณาจากการนำข้อมูลความเสี่ยงไปใช้ตัดสินใจ การดำเนินมาตรการได้ทันเวลา ระดับความเสี่ยงคงเหลือที่อยู่ภายใน RA/RT และความสามารถของมหาวิทยาลัยในการบรรลุวัตถุประสงค์ภายใต้ความไม่แน่นอนอย่างต่อเนื่องและยั่งยืน

1.10 คำจำกัดความและศัพท์เฉพาะ

คำจำกัดความต่อไปนี้ใช้เพื่อสร้างความเข้าใจและมาตรฐานเดียวกันในการบริหารความเสี่ยงทั่วทั้งมหาวิทยาลัย หากคำใดมีกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานเฉพาะกำหนดความหมายไว้ ให้ใช้ความหมายตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานนั้นเป็นสำคัญ

1.10.1 หน่วยงาน บทบาท และผู้เกี่ยวข้อง

- **ผู้กำกับดูแล (Governing Body):** สภามหาวิทยาลัยแม่โจ้ ซึ่งทำหน้าที่กำหนดทิศทาง อนุมัตินโยบายและระดับความเสี่ยงที่ยอมรับได้ กำกับติดตาม และดูแลผลการดำเนินงานตามอำนาจหน้าที่
- **หัวหน้าหน่วยงานของรัฐ:** อธิการบดีมหาวิทยาลัยแม่โจ้ ตามความหมายและอำนาจหน้าที่ที่กฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกำหนด
- **คณะกรรมการที่เกี่ยวข้อง (Relevant Committees):** คณะกรรมการซึ่งมีหน้าที่เกี่ยวกับการบริหารความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน หรือการกำกับเฉพาะด้าน ตามข้อบังคับ คำสั่ง หรือมติที่มีผลใช้บังคับ

- **ส่วนงานหรือหน่วยงาน (Faculty/Unit):** ส่วนงานหรือหน่วยงานตามโครงสร้างของมหาวิทยาลัย และตามนิยามในข้อบังคับ ประกาศ หรือคำสั่งที่เกี่ยวข้อง
- **เจ้าของวัตถุประสงค์ (Objective Owner):** ผู้มีอำนาจและความรับผิดชอบต่อการบรรลุวัตถุประสงค์ ผลลัพธ์ หรือตัวชี้วัดที่กำหนด
- **เจ้าของความเสี่ยง (Risk Owner):** ผู้มีอำนาจและความรับผิดชอบในการประเมิน ตัดสินใจตอบสนอง ติดตาม และรายงานความเสี่ยงที่ได้รับมอบหมาย รวมทั้งเสนอการยอมรับหรือยกระดับความเสี่ยงตามอำนาจที่กำหนด
- **เจ้าของการควบคุม (Control Owner):** ผู้รับผิดชอบออกแบบ ดำเนินการ ติดตาม และจัดเก็บหลักฐานว่าการควบคุมที่ได้รับมอบหมายทำงานอย่างต่อเนื่องและมีประสิทธิผล
- **เจ้าของมาตรการ (Action Owner):** ผู้รับผิดชอบดำเนินมาตรการเพิ่มเติมตามแผนบริหารความเสี่ยงให้แล้วเสร็จ และส่งมอบผลผลิตหรือหลักฐานภายในระยะเวลาที่กำหนด
- **เจ้าของข้อมูล (Data Owner):** ผู้รับผิดชอบกำหนดมาตรฐาน ดูแลคุณภาพ ความถูกต้อง ความครบถ้วน ความมั่นคงปลอดภัย และความทันเวลาของข้อมูลที่ใช้ติดตามและรายงานความเสี่ยง
- **ผู้ประสานงานความเสี่ยง (Risk Coordinator/Risk Champion):** ผู้สนับสนุนและประสานการจัดทำทะเบียนความเสี่ยง แผนบริหารความเสี่ยง การติดตาม KRI การรวบรวมหลักฐาน และการรายงานของส่วนงาน โดยไม่รับผิดชอบแทนเจ้าของความเสี่ยง

1.10.2 คำศัพท์พื้นฐานด้านการบริหารความเสี่ยง

- **การบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM):** วัฒนธรรม ความสามารถและแนวปฏิบัติที่บูรณาการกับการกำหนดยุทธศาสตร์และการบริหารผลการดำเนินงาน เพื่อจัดการความเสี่ยงในการสร้าง รักษา และเพิ่มคุณค่า
- **ความเสี่ยง (Risk):** ผลกระทบของความไม่แน่นอนต่อวัตถุประสงค์ ซึ่งอาจก่อให้เกิดผลลัพธ์ทั้งในด้านลบหรือด้านบวก
- **โอกาส (Opportunity):** ความไม่แน่นอนหรือสถานการณ์ที่อาจนำไปสู่ผลลัพธ์ที่ดีกว่าคาด การสร้างนวัตกรรม หรือการเพิ่มคุณค่า ภายใต้กรอบการกำกับดูแลและระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้
- **ปัจจัยขับเคลื่อนความเสี่ยง (Risk Driver):** สาเหตุ เงื่อนไข หรือการเปลี่ยนแปลงภายในหรือภายนอกที่มีอิทธิพลต่อโอกาสเกิดหรือผลกระทบของความเสี่ยง
- **เหตุการณ์ความเสี่ยง (Risk Event):** เหตุการณ์หรือสถานการณ์ที่ยังไม่แน่นอนและอาจเกิดขึ้นในอนาคต โดยอาจส่งผลต่อการบรรลุวัตถุประสงค์
- **ปัญหา (Issue):** สภาพหรือข้อบกพร่องที่เกิดขึ้นแล้วและต้องได้รับการแก้ไข ควบคุม หรือติดตามจนยุติ
- **อุบัติการณ์หรือเหตุการณ์ที่เกิดขึ้นจริง (Incident):** เหตุการณ์ความเสี่ยงที่เกิดขึ้นแล้วและต้องได้รับการตอบสนอง ระงับเหตุ แก้ไข ฟื้นฟู หรือยกระดับตามระดับความรุนแรง

- **โอกาสเกิด (Likelihood):** ความน่าจะเป็นหรือความถี่ที่เหตุการณ์ความเสี่ยงอาจเกิดขึ้นภายในช่วงเวลาที่กำหนด
- **ผลกระทบ (Impact/Consequence):** ผลหรือระดับความรุนแรงที่เหตุการณ์ความเสี่ยงอาจก่อให้เกิดต่อวัตถุประสงค์ ยุทธศาสตร์ การเงิน การดำเนินงาน กฎหมาย ชื่อเสียง ความปลอดภัย สิ่งแวดล้อม หรือผู้มีส่วนได้ส่วนเสีย
- **ความเสี่ยงโดยธรรมชาติ (Inherent Risk):** ระดับความเสี่ยงก่อนพิจารณาผลของการควบคุมหรือมาตรการตอบสนองที่มีอยู่
- **ประสิทธิผลของการควบคุม (Control Effectiveness):** ผลการประเมินว่าการควบคุมได้รับการออกแบบอย่างเหมาะสม นำไปปฏิบัติจริง และทำงานได้อย่างต่อเนื่องตามวัตถุประสงค์
- **ความเสี่ยงคงเหลือ (Residual Risk):** ระดับความเสี่ยงภายหลังพิจารณาผลของการควบคุมที่มีอยู่และทำงานจริงแล้ว
- **ความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk):** ระดับความเสี่ยงที่คาดว่าจะเหลือภายหลังดำเนินมาตรการเพิ่มเติมครบถ้วนภายในระยะเวลาที่กำหนด
- **ความเสี่ยงเกิดใหม่ (Emerging Risk):** ความเสี่ยงใหม่หรือความเสี่ยงเดิมที่เปลี่ยนแปลงอย่างรวดเร็ว ซึ่งข้อมูลหรือความเข้าใจยังมีจำกัด แต่อาจส่งผลกระทบอย่างมีนัยสำคัญในอนาคต
- **ความสัมพันธ์ระหว่างความเสี่ยง (Risk Interdependency):** ความสัมพันธ์ที่ความเสี่ยงหนึ่งอาจเป็นสาเหตุ เพิ่มความรุนแรง หรือส่งผลต่อความเสี่ยงอื่น
- **การกระจุกตัวของความเสี่ยง (Risk Concentration):** สถานการณ์ที่ความเสี่ยงหลายรายการพึ่งพาปัจจัย แหล่งรายได้ ระบบ ผู้ให้บริการ หรือทรัพยากรเดียวกัน จนอาจก่อให้เกิดผลกระทบรวมในระดับสูง
- **ภาพรวมความเสี่ยง (Risk Profile/Portfolio):** ภาพรวมระดับ แนวโน้ม ความสัมพันธ์ และการกระจุกตัวของความเสี่ยงสำคัญที่มหาวิทยาลัยต้องบริหารร่วมกัน

1.10.3 ระดับการยอมรับและการตัดสินใจด้านความเสี่ยง

- **ความสามารถในการรองรับความเสี่ยง (Risk Capacity):** ระดับความเสี่ยงสูงสุดที่มหาวิทยาลัยสามารถรองรับได้โดยไม่กระทบต่อความอยู่รอด ข้อจำกัดตามกฎหมาย ฐานะการเงิน หรือความสามารถในการปฏิบัติพันธกิจสำคัญ
- **ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA):** ประเภทและระดับความเสี่ยงที่มหาวิทยาลัยยินดีรับในการดำเนินยุทธศาสตร์และบรรลุวัตถุประสงค์
- **ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT):** ขอบเขตความเบี่ยงเบนที่วัดได้จากเป้าหมาย ผลการดำเนินงาน หรือระดับความเสี่ยงที่มหาวิทยาลัยยอมให้เกิดขึ้นได้ โดยเมื่อเข้าใกล้หรือเกินขอบเขตต้องดำเนินมาตรการ ยกระดับรายงาน หรือเสนอผู้มีอำนาจตัดสินใจ
- **เหตุที่ไม่ยอมรับ (Zero Tolerance Event):** เหตุการณ์ที่มหาวิทยาลัยไม่ยอมรับและต้องรายงานหรือยกระดับทันทีตามนโยบาย โดยไม่รอผลคะแนนความเสี่ยงรวม

- **การยอมรับความเสี่ยง (Risk Acceptance):** การตัดสินใจโดยผู้มีอำนาจให้คงระดับความเสี่ยงไว้ โดยพิจารณาว่าอยู่ภายใน RA/RT มีเหตุผลรองรับ และมีการกำหนดเงื่อนไขหรือการติดตามที่เหมาะสม
- **การตัดสินใจโดยคำนึงถึงความเสี่ยง (Risk-informed Decision-making):** การใช้ข้อมูลความเสี่ยง โอกาส สมมติฐาน ทางเลือก และความไม่แน่นอนประกอบการตัดสินใจ โดยมิได้หมายถึงการหลีกเลี่ยงความเสี่ยงทั้งหมด
- **การยกระดับรายงานความเสี่ยง (Risk Escalation):** การส่งต่อข้อมูลความเสี่ยงไปยังผู้มีอำนาจตัดสินใจในระดับสูงขึ้น ตามเกณฑ์ ระยะเวลา และเส้นทางรายงานที่กำหนด

1.10.4 การติดตามและรายงานความเสี่ยง

- **ทะเบียนความเสี่ยง (Risk Register):** เอกสารหรือฐานข้อมูลที่ใช้บันทึกวัตถุประสงค์ ข้อความความเสี่ยง สาเหตุ ผลกระทบ การประเมิน การควบคุม ผู้รับผิดชอบ มาตรการ ตัวชี้วัด และผลการติดตามความเสี่ยง
- **แผนบริหารความเสี่ยง (Risk Treatment Plan):** แผนที่กำหนดมาตรการเพิ่มเติม เจ้าของมาตรการ ทรัพยากร ระยะเวลา ผลส่งมอบ ตัววัดความสำเร็จ และระดับความเสี่ยงคงเหลือเป้าหมาย
- **ตัวชี้วัดผลการดำเนินงาน (Key Performance Indicator: KPI):** ตัววัดความก้าวหน้าหรือความสำเร็จในการบรรลุวัตถุประสงค์และผลการดำเนินงาน
- **ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI):** ตัววัดระดับ แนวโน้ม หรือปัจจัยขับเคลื่อนความเสี่ยง ซึ่งเชื่อมโยงกับ RA/RT และกำหนดการดำเนินการเมื่อเข้าใกล้หรือเกินเกณฑ์
- **ตัวชี้วัดการควบคุมที่สำคัญ (Key Control Indicator: KCI):** ตัววัดว่าการควบคุมสำคัญได้รับการดำเนินการครบถ้วน ต่อเนื่อง และมีประสิทธิผลตามที่กำหนด
- **สัญญาณเตือนล่วงหน้า (Early Warning Signal: EWS):** ข้อมูล เหตุการณ์ หรือแนวโน้มที่บ่งชี้ว่าความเสี่ยงอาจเพิ่มขึ้นหรือเข้าใกล้เกณฑ์ที่กำหนด เพื่อให้สามารถเตรียมการก่อนเกิดผลกระทบอย่างมีนัยสำคัญ

1.10.5 การตอบสนอง การควบคุม และการให้ความเชื่อมั่น

- **การตอบสนองต่อความเสี่ยง (Risk Response):** การเลือกแนวทางจัดการความเสี่ยงหรือโอกาส เช่น หลีกเลี่ยง ลดหรือควบคุม แบ่งปันหรือถ่ายโอน ยอมรับ หรือใช้ประโยชน์จากโอกาส
- **การควบคุมภายใน (Internal Control):** นโยบาย กระบวนการ หรือกิจกรรมที่ออกแบบและดำเนินการเพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลต่อการบรรลุวัตถุประสงค์ด้านการดำเนินงาน การรายงาน และการปฏิบัติตามกฎหมาย
- **การให้ความเชื่อมั่น (Assurance):** การประเมินอย่างเป็นระบบเพื่อเพิ่มความเชื่อมั่นต่อความเพียงพอและประสิทธิผลของการกำกับดูแล การบริหารความเสี่ยง และการควบคุม
- **หลัก Three Lines:** หลักการจัดบทบาทระหว่างผู้กำกับดูแล ฝ่ายบริหารและสายงานที่หนึ่ง หน่วยงานสนับสนุนหรือกำกับในสายงานที่สอง และการตรวจสอบภายในซึ่งเป็นสายงานที่สาม เพื่อสนับสนุนการกำกับดูแล การบริหารความเสี่ยง และการให้ความเชื่อมั่นอย่างมีประสิทธิผล

- **ความเชื่อมโยงความเสี่ยง–การควบคุม–การให้ความเชื่อมั่น (Risk–Control–Assurance):** การเชื่อมความเสี่ยงสำคัญกับการควบคุมที่ตอบสนองต่อสาเหตุหรือผลกระทบ และแหล่งความเชื่อมั่นที่ประเมินว่าการควบคุมทำงานได้ตามที่ออกแบบ
- **การกำกับดูแล ความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ (Governance, Risk and Compliance: GRC):** แนวทางบูรณาการธรรมาภิบาล การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายหรือข้อกำหนด เพื่อให้การตัดสินใจ ความรับผิดชอบ การควบคุม และการรายงานเชื่อมโยงกัน
- **วัฒนธรรมความเสี่ยง (Risk Culture):** ค่านิยม ทัศนคติ ความรู้ พฤติกรรม และความรับผิดชอบที่มีอิทธิพลต่อวิธีที่บุคลากรเข้าใจ ตัดสินใจ รายงาน และจัดการความเสี่ยง

1.10.6 ความต่อเนื่อง ความยืดหยุ่น และความยั่งยืน

- **การบริหารความต่อเนื่องขององค์กร (Business Continuity Management: BCM):** กระบวนการบริหารแบบองค์รวมเพื่อเตรียมความพร้อม ตอบสนอง และฟื้นฟูภารกิจสำคัญให้อยู่ภายในระดับและระยะเวลาที่ยอมรับได้เมื่อเกิดเหตุหยุดชะงัก
- **แผนความต่อเนื่องในการดำเนินงาน (Business Continuity Plan: BCP):** แผนปฏิบัติที่กำหนดภารกิจสำคัญ ผู้รับผิดชอบ ทรัพยากร ขั้นตอนตอบสนอง วิธีดำเนินงานทดแทน การสื่อสาร และเป้าหมายการฟื้นตัวเมื่อเกิดเหตุหยุดชะงัก
- **ความยืดหยุ่นขององค์กร (Organizational Resilience):** ความสามารถของมหาวิทยาลัยในการคาดการณ์ เตรียมพร้อม ตอบสนอง ปรับตัว และฟื้นตัวจากการเปลี่ยนแปลงหรือเหตุหยุดชะงัก โดยยังสามารถรักษาพันธกิจสำคัญและสร้างคุณค่าได้
- **สิ่งแวดล้อม สังคม และธรรมาภิบาล (Environmental, Social and Governance: ESG):** กรอบพิจารณาปัจจัยและผลกระทบด้านสิ่งแวดล้อม สังคม และธรรมาภิบาลที่อาจมีผลต่อยุทธศาสตร์ การดำเนินงาน ความเชื่อมั่น และความยั่งยืนของมหาวิทยาลัย
- **ความปลอดภัย (Safety):** มิติผลกระทบร่วมที่ครอบคลุมชีวิต สุขภาพ อาชีวอนามัย อาคารสถานที่ ทรัพย์สิน และความปลอดภัยในการศึกษา การวิจัย การปฏิบัติงาน และการให้บริการ
- **ระดับการพัฒนาระบบบริหารความเสี่ยง (Risk Management Maturity):** ระดับความพร้อม ความสามารถ การบูรณาการ และประสิทธิผลของระบบบริหารความเสี่ยง ซึ่งใช้ประเมินช่องว่างและกำหนดแนวทางพัฒนาอย่างต่อเนื่อง

ระดับความเสี่ยงของมหาวิทยาลัย

มหาวิทยาลัยประเมินระดับความเสี่ยงโดยใช้สูตร

คะแนนความเสี่ยง (Risk Score) = โอกาสเกิด (Likelihood) × ผลกระทบ (Impact)

คะแนน	ระดับความเสี่ยง	รหัส	แนวทางดำเนินการขั้นต่ำ
1–4	ต่ำ (Low)	L	ยอมรับและติดตามตามรอบปกติ
5–9	ปานกลาง (Medium)	M	กำหนดมาตรการและติดตามโดยเจ้าของความเสี่ยง
10–15	สูง (High)	H	จัดทำแผนลดความเสี่ยงและรายงานฝ่ายบริหาร
16–25	สูงมาก (Extreme)	E	ยกระดับรายงานทันทีและเร่งดำเนินมาตรการ

คะแนนความเสี่ยงเป็นข้อมูลเริ่มต้นสำหรับการพิจารณา มิใช่ข้อยุติเพียงประการเดียว ต้องพิจารณาเกณฑ์ยกระดับเป็นกรณีพิเศษ (Override Criteria) ร่วมด้วย เช่น

- ผลกระทบอยู่ในระดับ 5 แม้คะแนนรวมไม่ถึงระดับสูงมาก
- เป็นเหตุที่ไม่ยอมรับ (Zero Tolerance Event)
- KRI เข้าใกล้หรือเกิน RT
- ความเสี่ยงกระทบหลายส่วนงานหรือมีการกระจุกตัวสูง
- ความเสี่ยงอาจกระทบวัตถุประสงค์เชิงยุทธศาสตร์ พันธกิจสำคัญ ชีวิต ความปลอดภัย กฎหมาย หรือชื่อเสียงอย่างมีนัยสำคัญ
- ระดับความเสี่ยงเพิ่มขึ้นอย่างรวดเร็ว หรือข้อมูลมีความไม่แน่นอนสูง

การใช้เกณฑ์ Override ต้องบันทึกเหตุผล หลักฐาน ผู้เสนอ ผู้มีอำนาจพิจารณา วันที่ตัดสินใจ มาตรการตอบสนอง และกำหนดเวลาทบทวนไว้ในทะเบียนความเสี่ยง

ส่วนที่ 2
นโยบายและกรอบการบริหารความเสี่ยง

2.1 ถ้อยแถลงการกำกับดูแลความเสี่ยงของมหาวิทยาลัย

สภามหาวิทยาลัยแม่โจ้ตระหนักว่า ความเสี่ยงและโอกาสเป็นส่วนหนึ่งของการกำหนดยุทธศาสตร์ การตัดสินใจ และการดำเนินพันธกิจภายใต้ความไม่แน่นอน จึงกำหนดให้การบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM) เป็นกลไกสำคัญของธรรมาภิบาล เพื่อสนับสนุนการบรรลุวิสัยทัศน์ พันธกิจ วัตถุประสงค์ และผลลัพธ์เชิงยุทธศาสตร์ ตลอดจนการสร้าง รักษา และเพิ่มคุณค่าให้แก่มหาวิทยาลัยและผู้มีส่วนได้ส่วนเสียอย่างต่อเนื่องและยั่งยืน

ภายใต้อำนาจหน้าที่ตามกฎหมายและข้อบังคับที่เกี่ยวข้อง สภามหาวิทยาลัยทำหน้าที่กำหนดทิศทางและกำกับดูแลความเพียงพอของระบบบริหารความเสี่ยง อนุมัตินโยบายและกรอบระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้ (Risk Appetite Framework) กำกับให้ฝ่ายบริหารจัดการความเสี่ยงสำคัญให้อยู่ภายในกรอบที่กำหนด และได้รับรายงานด้านความเสี่ยง การควบคุม และการให้ความเชื่อมั่นที่ถูกต้อง ครบถ้วน ทันเวลา และเพียงพอต่อการปฏิบัติหน้าที่กำกับดูแล

ฝ่ายบริหารรับผิดชอบนำทิศทาง นโยบาย และกรอบระดับความเสี่ยงที่ยอมรับได้ไปสู่การปฏิบัติ กำหนดเจ้าของวัตถุประสงค์และเจ้าของความเสี่ยง จัดสรรทรัพยากร ออกแบบและดำเนินมาตรการควบคุม ติดตามตัวชี้วัดความเสี่ยงที่สำคัญและสัญญาณเตือนล่วงหน้า ตลอดจนรายงานหรือยกระดับความเสี่ยงต่อผู้มีอำนาจตัดสินใจตามเกณฑ์และระยะเวลาที่กำหนด

มหาวิทยาลัยยึดหลักว่า ฝ่ายบริหารและส่วนงานเป็นเจ้าของความเสี่ยง การบริหารความเสี่ยงต้องบูรณาการกับการกำหนดยุทธศาสตร์ การบริหารผลการดำเนินงาน การจัดสรรทรัพยากร การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ และการบริหารความต่อเนื่อง โดยกองตรวจสอบภายในทำหน้าที่ให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระ และไม่บริหารความเสี่ยงแทนฝ่ายบริหาร

มหาวิทยาลัยส่งเสริมวัฒนธรรมที่เปิดกว้างต่อการรายงานความเสี่ยง สัญญาณเตือน เหตุการณ์ และข้อผิดพลาดโดยสุจริต เพื่อให้เกิดการเรียนรู้ การแก้ไข และการปรับปรุงอย่างต่อเนื่อง พร้อมทั้งไม่ยอมรับการปกปิดหรือบิดเบือนข้อมูล การทุจริต การกระทำผิดกฎหมาย หรือพฤติกรรมที่ขัดต่อจริยธรรมและหลักธรรมาภิบาล

หลักการกำกับดูแล: การบริหารความเสี่ยงต้องสนับสนุนการตัดสินใจบนฐานข้อมูล มิใช่เป็นเพียงการจัดทำเอกสารหรือรายงานตามรอบเวลา และต้องช่วยให้มหาวิทยาลัยสามารถสร้างคุณค่า คุ้มครองพันธกิจสำคัญ และรักษาความยืดหยุ่นภายใต้ความไม่แน่นอน

2.2 นโยบายการบริหารความเสี่ยงมหาวิทยาลัยแม่โจ้ (Maejo University Enterprise Risk Management Policy)

มหาวิทยาลัยแม่โจ้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงองค์กร (Enterprise Risk Management : ERM) ในฐานะกลไกสำคัญของการกำกับดูแลกิจการที่ดี (Good Governance) และการบริหารจัดการมหาวิทยาลัยให้สามารถบรรลุวิสัยทัศน์ พันธกิจ เป้าประสงค์เชิงยุทธศาสตร์ และผลลัพธ์ที่พึงประสงค์ได้อย่างมีประสิทธิภาพ ประสิทธิผล โปร่งใส ตรวจสอบได้ และสามารถสร้างคุณค่าให้แก่ผู้มีส่วนได้ส่วนเสียทุกกลุ่ม

มหาวิทยาลัยจึงกำหนดนโยบายการบริหารความเสี่ยงองค์กร โดยยึดหลักการและแนวปฏิบัติตามกรอบการบริหารความเสี่ยงสากล ได้แก่ COSO Enterprise Risk Management: Integrating with Strategy and Performance (COSO ERM 2017) มาตรฐาน ISO 31000:2018 หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ตลอดจนแนวทางการกำกับดูแลกิจการที่ดี การควบคุมภายใน การพัฒนาองค์กรสู่ความเป็นเลิศ (EdPEx) เป้าหมายการพัฒนาอย่างยั่งยืน (SDGs) และหลักการด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (Environmental, Social and Governance : ESG)

มหาวิทยาลัยกำหนดให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารงานปกติ การวางแผนยุทธศาสตร์ การกำหนดนโยบาย การตัดสินใจเชิงบริหาร การบริหารโครงการ การบริหารทรัพยากร และการติดตามผลการดำเนินงาน โดยบูรณาการการบริหารความเสี่ยงควบคู่กับการบริหารโอกาส (Risk and Opportunity Management) เพื่อสนับสนุนการสร้างคุณค่า (Value Creation) การรักษาคุณค่า (Value Preservation) และการเพิ่มคุณค่า (Value Enhancement) ให้แก่มหาวิทยาลัยอย่างยั่งยืน

มหาวิทยาลัยมุ่งส่งเสริมให้บุคลากรทุกระดับมีความตระหนักรู้ด้านความเสี่ยง (Risk Awareness) มีส่วนร่วมในการบริหารความเสี่ยง และร่วมกันสร้างวัฒนธรรมความเสี่ยงองค์กร (Risk Culture) ที่เข้มแข็ง โดยถือว่าการบริหารความเสี่ยงเป็นความรับผิดชอบร่วมกันของผู้บริหาร คณาจารย์ บุคลากร และผู้ปฏิบัติงานทุกคน

เพื่อให้การบริหารความเสี่ยงเป็นไปในทิศทางเดียวกันทั่วทั้งมหาวิทยาลัย จึงกำหนดนโยบาย ดังต่อไปนี้

1. การกำกับดูแลและความรับผิดชอบด้านการบริหารความเสี่ยง (Risk Governance and Accountability) มหาวิทยาลัยกำหนดให้การกำกับดูแลความเสี่ยงเป็นองค์ประกอบสำคัญของระบบธรรมาภิบาล โดยกำหนดโครงสร้าง บทบาท หน้าที่ และความรับผิดชอบของสภามหาวิทยาลัย ผู้บริหาร คณะกรรมการ ส่วนงาน และบุคลากรไว้อย่างชัดเจน พร้อมยึดหลัก Three Lines Model เพื่อให้การบริหารความเสี่ยง การควบคุมภายใน และการตรวจสอบภายในทำงานประสานกันอย่างมีประสิทธิภาพ โปร่งใส และตรวจสอบได้

2. การบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise-Wide Risk Management) มหาวิทยาลัยจะดำเนินการบริหารความเสี่ยงอย่างเป็นระบบ ครอบคลุมทุกพันธกิจ ทุกส่วนงาน ทุกกระบวนการ และทุกระดับการบริหาร โดยเชื่อมโยงกับยุทธศาสตร์ แผนปฏิบัติการ โครงการ และการดำเนินงานประจำ เพื่อสนับสนุนการบรรลุเป้าหมายของมหาวิทยาลัยอย่างมีประสิทธิผล

3. การกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite and Risk Tolerance) มหาวิทยาลัยจะกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance) ให้

สอดคล้องกับบริบท เป้าหมาย และศักยภาพในการบริหารจัดการขององค์กร เพื่อใช้เป็นกรอบในการตัดสินใจ การจัดลำดับความสำคัญ และการตอบสนองต่อความเสี่ยง

4. การตัดสินใจบนพื้นฐานของความเสี่ยง (Risk-informed Decision Making) มหาวิทยาลัยกำหนดให้การกำหนดนโยบาย การวางแผน การลงทุน การบริหารโครงการ และการตัดสินใจที่สำคัญทุกระดับพิจารณาข้อมูลความเสี่ยง โอกาส ระดับความเสี่ยงที่ยอมรับได้ และผลกระทบต่อผู้มีส่วนได้ส่วนเสีย เพื่อสนับสนุนการตัดสินใจเชิงยุทธศาสตร์อย่างมีข้อมูลรองรับ

5. การใช้มาตรฐานและแนวปฏิบัติเดียวกันทั่วทั้งองค์กร มหาวิทยาลัยกำหนดกระบวนการ เครื่องมือ หลักเกณฑ์ และรูปแบบการรายงานด้านการบริหารความเสี่ยงให้เป็นมาตรฐานเดียวกันทั่วทั้งองค์กร เพื่อให้เกิดความสอดคล้อง ความเข้าใจร่วมกัน และสามารถเปรียบเทียบผลการดำเนินงานได้อย่างมีประสิทธิภาพ

6. การตระหนักรู้ การมีส่วนร่วม และการสร้างวัฒนธรรมความเสี่ยงองค์กร ผู้บริหารทุกระดับและบุคลากรทุกคนต้องตระหนักถึงบทบาทหน้าที่ด้านการบริหารความเสี่ยง มีส่วนร่วมในการระบุ ประเมิน ติดตาม และรายงานความเสี่ยง รวมทั้งร่วมกันสร้างวัฒนธรรมความเสี่ยงองค์กร (Risk Culture) ให้เป็นส่วนหนึ่งของการปฏิบัติงานประจำ

7. การบริหารความเสี่ยงเพื่อการสร้างคุณค่า (Risk for Value Creation) มหาวิทยาลัยถือว่าการบริหารความเสี่ยงมิใช่เพียงการลดหรือควบคุมความเสี่ยง แต่เป็นเครื่องมือสำคัญในการสร้าง รักษา และเพิ่มคุณค่า สนับสนุนการสร้างนวัตกรรม การใช้ประโยชน์จากโอกาส และการพัฒนาองค์กรอย่างยั่งยืน

8. การบริหารความเสี่ยงเชิงรุกและความเสี่ยงเกิดใหม่ (Emerging Risks) มหาวิทยาลัยจะติดตาม วิเคราะห์ และประเมินปัจจัยภายในและภายนอก รวมถึงความเสี่ยงเกิดใหม่ เช่น การเปลี่ยนแปลงทางเทคโนโลยี ปัญญาประดิษฐ์ (AI) การเปลี่ยนแปลงด้านประชากรศาสตร์ การแข่งขันทางการศึกษา ภัยคุกคามทางไซเบอร์ การเปลี่ยนแปลงสภาพภูมิอากาศ และปัจจัยด้านภูมิรัฐศาสตร์ เพื่อเตรียมความพร้อมในการรับมืออย่างเหมาะสม

9. การใช้ข้อมูลและเทคโนโลยีดิจิทัลในการบริหารความเสี่ยง (Data-driven Risk Management) มหาวิทยาลัยส่งเสริมการใช้เทคโนโลยีดิจิทัล ระบบสารสนเทศ ข้อมูลเชิงวิเคราะห์ (Data Analytics) และปัญญาประดิษฐ์ (AI) เพื่อเพิ่มประสิทธิภาพในการติดตาม ประเมิน วิเคราะห์ และรายงานความเสี่ยง รวมถึงการพัฒนาระบบเตือนภัยล่วงหน้า (Early Warning System) และตัวชี้วัดความเสี่ยง (Key Risk Indicators: KRIs)

10. การบริหารความมั่นคงปลอดภัยสารสนเทศและความเสี่ยงไซเบอร์ มหาวิทยาลัยให้ความสำคัญกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และความมั่นคงของระบบสารสนเทศ เพื่อสนับสนุนการเป็นมหาวิทยาลัยดิจิทัลและสร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสีย

11. การบูรณาการกับการควบคุมภายในและธรรมาภิบาล การบริหารความเสี่ยงต้องดำเนินการควบคู่กับระบบการควบคุมภายใน การกำกับดูแลกิจการที่ดี การตรวจสอบภายใน และการติดตามประเมินผลการดำเนินงาน เพื่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลว่ามหาวิทยาลัยสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้

12. การพัฒนาศักยภาพบุคลากร มหาวิทยาลัยจะสนับสนุนการพัฒนาความรู้ ทักษะ และสมรรถนะด้านการบริหารความเสี่ยง การควบคุมภายใน และธรรมาภิบาลของผู้บริหารและบุคลากรอย่างต่อเนื่อง เพื่อยกระดับวุฒิภาวะด้านการบริหารความเสี่ยงขององค์กร

13. การบริหารความต่อเนื่องขององค์กรและการเสริมสร้างความยืดหยุ่น (Business Continuity Management and Organizational Resilience) มหาวิทยาลัยจะจัดให้มีระบบบริหารความต่อเนื่องขององค์กร (Business Continuity Management: BCM) และแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อเตรียมความพร้อมในการตอบสนองต่อเหตุการณ์ฉุกเฉิน ภัยพิบัติ หรือภาวะวิกฤติ พร้อมทั้งพัฒนาองค์กรให้มีความยืดหยุ่น (Organizational Resilience) สามารถฟื้นตัวและดำเนินภารกิจได้อย่างต่อเนื่อง

14. การติดตาม ทบทวน และปรับปรุงอย่างต่อเนื่อง (Continuous Improvement) มหาวิทยาลัยจะติดตาม ประเมินผล และทบทวนประสิทธิผลของระบบบริหารความเสี่ยงอย่างสม่ำเสมอ โดยใช้ผลการประเมินวุฒิภาวะด้านการบริหารความเสี่ยง (Risk Maturity Assessment) ผลการตรวจสอบภายใน บทเรียนจากเหตุการณ์ (Lessons Learned) และข้อเสนอแนะจากผู้มีส่วนได้ส่วนเสีย เพื่อปรับปรุงระบบบริหารความเสี่ยงให้สอดคล้องกับการเปลี่ยนแปลงของยุทธศาสตร์ สภาพแวดล้อม เทคโนโลยี และกฎหมายอย่างต่อเนื่อง

ประกาศ ณ วันที่ .....

(รองศาสตราจารย์ ดร.เทพ พงษ์พานิช)
นายกสภามหาวิทยาลัย

2.3 นโยบายระดับความเสี่ยงที่ยอมรับได้

มหาวิทยาลัยแม่โจ้กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) เพื่อใช้เป็นกรอบในการกำกับดูแล การตัดสินใจเชิงบริหาร การจัดสรรทรัพยากร และการบริหารความเสี่ยงให้สอดคล้องกับวิสัยทัศน์ พันธกิจ เป้าประสงค์เชิงยุทธศาสตร์ และความสามารถในการรองรับความเสี่ยงของมหาวิทยาลัย (Risk Capacity)

การกำหนดระดับความเสี่ยงที่ยอมรับได้สะท้อนถึงระดับความเสี่ยงที่มหาวิทยาลัยยินดีรับเพื่อให้บรรลุเป้าหมายเชิงยุทธศาสตร์ โดยคำนึงถึงผลกระทบที่อาจเกิดขึ้นต่อผู้เรียน บุคลากร ผู้มีส่วนได้ส่วนเสีย ชื่อเสียง ความมั่นคงทางการเงิน และความยั่งยืนขององค์กร ทั้งนี้ มหาวิทยาลัยกำหนดระดับความเสี่ยงที่ยอมรับได้ในแต่ละมิติดังต่อไปนี้

1. ด้านการจัดการศึกษาและคุณภาพผู้เรียน/บัณฑิต (Education and Student/Graduate Quality)

มหาวิทยาลัยมุ่งรักษามาตรฐานคุณภาพการศึกษา คุณภาพผู้เรียน และคุณภาพบัณฑิตในทุกระดับการศึกษา ทั้งหลักสูตรระดับปริญญา (Degree Programs) และหลักสูตรการเรียนรู้ตลอดชีวิตหรือหลักสูตรที่ไม่มุ่งให้ปริญญา (Non-Degree Programs) เพื่อสร้างความเชื่อมั่นแก่ผู้เรียน ผู้ปกครอง ผู้ใช้บัณฑิต และสังคม

มหาวิทยาลัยให้ความสำคัญอย่างยิ่งต่อผลสัมฤทธิ์การเรียนรู้ มาตรฐานวิชาการ คุณภาพหลักสูตร การพัฒนาทักษะแห่งอนาคต และประสบการณ์การเรียนรู้ของผู้เรียน จึงกำหนดระดับความเสี่ยงที่ยอมรับได้ **ระดับต่ำ (Low Appetite)** เนื่องจากความผิดพลาดหรือความบกพร่องในด้านดังกล่าวอาจส่งผลกระทบโดยตรงต่อคุณภาพบัณฑิต มาตรฐานการศึกษา และชื่อเสียงของมหาวิทยาลัยในระยะยาว

2. ด้านการวิจัย นวัตกรรม และการสร้างองค์ความรู้ (Research, Innovation and Knowledge Creation)

มหาวิทยาลัยมีเป้าหมายในการเป็นมหาวิทยาลัยแห่งนวัตกรรมและการพัฒนาเทคโนโลยี โดยเฉพาะด้านการเกษตร อาหาร สิ่งแวดล้อม และการพัฒนาชุมชน จึงต้องสนับสนุนการคิดค้นสิ่งใหม่ การสร้างองค์ความรู้ การวิจัยขั้นแนวหน้า และการถ่ายทอดเทคโนโลยีสู่การใช้ประโยชน์เชิงสังคมและเชิงพาณิชย์

มหาวิทยาลัยยินดีรับความเสี่ยงในระดับที่เหมาะสมเพื่อสนับสนุนการสร้างนวัตกรรมและการพัฒนางานวิจัยที่มีผลกระทบสูง จึงกำหนดระดับความเสี่ยงที่ยอมรับได้ **ระดับปานกลาง (Medium Appetite)**

อย่างไรก็ตาม ในประเด็นที่เกี่ยวข้องกับจริยธรรมการวิจัย ความซื่อสัตย์ทางวิชาการ การละเมิดทรัพย์สินทางปัญญา หรือการดำเนินการที่ไม่เป็นไปตามมาตรฐานวิชาชีพและมาตรฐานสากล มหาวิทยาลัยกำหนด **ระดับความเสี่ยงที่ยอมรับได้ต่ำมาก (Low Appetite) หรือไม่มีระดับความเสี่ยงที่ยอมรับได้ (Zero Appetite) ตามลักษณะของเหตุการณ์**

3. ด้านสมรรถนะและความยั่งยืนทางการเงิน (Financial Performance and Sustainability)

มหาวิทยาลัยมุ่งรักษาความมั่นคงทางการเงิน ความสามารถในการพึ่งพาตนเอง และความยั่งยืนทางการคลัง เพื่อรองรับการดำเนินภารกิจในระยะยาว โดยกำหนดระดับความเสี่ยงที่ยอมรับได้ ดังนี้

3.1 การปฏิบัติตามวินัยการเงินการคลัง

มหาวิทยาลัยยึดมั่นในการบริหารงบประมาณ การเงิน และทรัพย์สินของรัฐอย่างโปร่งใส ถูกต้องและเป็นไปตามกฎหมาย ระเบียบ และหลักธรรมาภิบาล **ไม่มีระดับความเสี่ยงที่ยอมรับได้ (Zero Appetite)** สำหรับการทุจริต การใช้จ่ายงบประมาณโดยมิชอบ การกระทำผิดวินัยทางการเงินการคลัง หรือการดำเนินการที่ก่อให้เกิดความเสียหายอย่างมีนัยสำคัญต่อมหาวิทยาลัย

3.2 การลงทุนและการสร้างรายได้

มหาวิทยาลัยสามารถยอมรับความเสี่ยงในระดับที่เหมาะสมจากการลงทุน การบริหารทรัพย์สิน และการพัฒนาแหล่งรายได้ใหม่ เพื่อสนับสนุนการเติบโตและความยั่งยืนทางการเงิน **ระดับปานกลาง (Medium Appetite)** โดยต้องมีการวิเคราะห์ความคุ้มค่า ผลตอบแทน และความเสี่ยงอย่างรอบคอบภายใต้หลักการบริหารจัดการที่ดี

4. ด้านการปฏิบัติตามกฎหมาย ระเบียบ และมาตรฐาน (Compliance)

มหาวิทยาลัยยึดมั่นในหลักนิติธรรม ความถูกต้อง โปร่งใส และความรับผิดชอบต่อสังคม โดยการดำเนินงานทุกด้านต้องเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ มาตรฐานวิชาชีพ จรรยาบรรณ และหลักธรรมาภิบาล ดังนั้น มหาวิทยาลัยจึงกำหนด **ไม่มีระดับความเสี่ยงที่ยอมรับได้ (Zero Appetite)** สำหรับการกระทำที่ขัดต่อกฎหมาย การทุจริต การคอร์รัปชัน การเลือกปฏิบัติ การละเมิดจริยธรรม หรือการกระทำที่ส่งผลกระทบต่อความน่าเชื่อถือและความถูกต้ององค์กร

5. ด้านข้อมูลและเทคโนโลยีสารสนเทศ (Data and Information Technology)

มหาวิทยาลัยดำเนินภารกิจและให้บริการผ่านระบบดิจิทัลและระบบสารสนเทศเป็นสำคัญ จึงให้ความสำคัญต่อความมั่นคงปลอดภัยไซเบอร์ ความถูกต้องของข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และความต่อเนื่องของระบบสารสนเทศ มหาวิทยาลัยกำหนดระดับความเสี่ยงที่ยอมรับได้ **ระดับต่ำ (Low Appetite)** เนื่องจากเหตุการณ์ด้านเทคโนโลยีสารสนเทศอาจส่งผลกระทบต่อการดำเนินงาน การให้บริการ ความเชื่อมั่น และชื่อเสียงของมหาวิทยาลัย

6. ด้านภาพลักษณ์ ชื่อเสียง และความเชื่อมั่นขององค์กร (Reputation)

มหาวิทยาลัยมุ่งรักษาภาพลักษณ์ ชื่อเสียง และความน่าเชื่อถือที่สั่งสมมาอย่างยาวนาน โดยการดำเนินงานทุกด้านต้องคำนึงถึงผลกระทบต่อความเชื่อมั่นของผู้เรียน ผู้ปกครอง ศิษย์เก่า ภาคีเครือข่าย และสังคม มหาวิทยาลัยกำหนดระดับความเสี่ยงที่ยอมรับได้ **ระดับต่ำ (Low Appetite)** สำหรับกิจกรรมหรือการดำเนินงานที่อาจส่งผลกระทบต่อชื่อเสียง ภาพลักษณ์ และความไว้วางใจจากสาธารณชน

7. ด้านความปลอดภัย สุขภาพ และสวัสดิภาพ (Safety, Health and Well-being)

มหาวิทยาลัยให้ความสำคัญสูงสุดต่อความปลอดภัยในชีวิต สุขภาพ อนามัย และทรัพย์สินของนักศึกษา บุคลากร ผู้รับบริการ และประชาชนที่เกี่ยวข้อง มหาวิทยาลัยกำหนดระดับความเสี่ยงที่ยอมรับได้ **ระดับต่ำ (Low Appetite)** สำหรับเหตุการณ์ทั่วไปที่อาจส่งผลกระทบต่อความปลอดภัยและสุขภาพ และกำหนด **ไม่มีระดับความเสี่ยงที่ยอมรับได้ (Zero Appetite)** สำหรับเหตุการณ์ที่ก่อให้เกิดการเสียชีวิต การบาดเจ็บร้ายแรง การเจ็บป่วยรุนแรง หรือความเสียหายร้ายแรงต่อทรัพย์สินอันเกิดจากการละเลยหรือไม่ปฏิบัติตามมาตรการด้านความปลอดภัยที่กำหนดไว้

การกำหนดระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance)

มหาวิทยาลัยและส่วนงานสามารถกำหนดระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance) ภายใต้กรอบระดับความเสี่ยงที่ยอมรับได้ของมหาวิทยาลัย เพื่อให้สอดคล้องกับลักษณะภารกิจ บริบทการดำเนินงาน และสภาพแวดล้อมที่เปลี่ยนแปลงไป โดยต้องไม่ขัดต่อหลักเกณฑ์ นโยบาย และระดับความเสี่ยงที่มหาวิทยาลัยกำหนด

การกำหนด Risk Tolerance ต้องสามารถวัดผลได้อย่างชัดเจน มีตัวชี้วัดหรือเกณฑ์ควบคุมที่เหมาะสม และได้รับการทบทวนเป็นประจำ เพื่อให้สามารถสนับสนุนการบรรลุเป้าหมายเชิงยุทธศาสตร์ ควบคู่ไปกับการรักษาความเชื่อมั่นของผู้มีส่วนได้ส่วนเสียและความยั่งยืนของมหาวิทยาลัยในระยะยาว

ตารางที่ 2-1 ระดับความเสี่ยงที่ยอมรับได้ของมหาวิทยาลัย จำแนกตามมิติ

มิติ	ระดับโดยรวม	เจตนารมณ์และขอบเขต
1. **การจัดการศึกษาและคุณภาพผู้เรียน/บัณฑิต**	ต่ำ	➢ รักษามาตรฐานหลักสูตร ผลลัพธ์การเรียนรู้ คุณภาพบัณฑิต และสิทธิของผู้เรียน ไม่ยอมรับการลดมาตรฐานที่มีนัยสำคัญ
2. **การวิจัย นวัตกรรม และการใช้ประโยชน์**	ปานกลาง	➢ ยอมรับความไม่แน่นอนที่ผ่านการประเมินเพื่อส่งเสริมนวัตกรรม งานวิจัยผลกระทบสูง และการใช้ประโยชน์ ภายใต้กรอบจริยธรรม ความปลอดภัย และกฎหมาย
3. **ความมั่นคงและความยั่งยืนทางการเงิน**	ต่ำถึงปานกลาง	➢ ยอมรับความผันผวนอย่างจำกัดเพื่อเพิ่มรายได้ ลงทุน และใช้ทรัพย์สินให้เกิดประโยชน์ โดยต้องรักษาสภาพคล่อง วินัยการเงิน และความสามารถในการดำเนินพันธกิจ
4. **การปฏิบัติตามกฎหมาย ธรรมาภิบาล และจริยธรรม**	ต่ำมาก / สำหรับเหตุร้ายแรง	➢ ไม่ยอมรับการทุจริต การกระทำผิดกฎหมายโดยเจตนา การประพฤติมิชอบร้ายแรง ผลประโยชน์ทับซ้อนที่ไม่เปิดเผย การคุกคาม การลอกเลียนผลงาน หรือการกระทำผิดจริยธรรมการวิจัยร้ายแรง
5. **ข้อมูล เทคโนโลยี ไซเบอร์ และข้อมูลส่วนบุคคล**	ต่ำ	➢ ยอมรับความเสี่ยงจำกัดสำหรับนวัตกรรมดิจิทัลภายใต้การควบคุมที่เหมาะสม แต่ไม่ยอมรับการละเลยข้อกำหนดพื้นฐาน การรั่วไหลร้ายแรง หรือการเข้าถึงข้อมูลโดยมิชอบ
6. **ชื่อเสียง ภาพลักษณ์ และความไว้วางใจ**	ต่ำ	➢ ให้ความสำคัญกับความถูกต้อง โปร่งใส และการสื่อสารที่รับผิดชอบ โดยเหตุที่อาจทำลายความไว้วางใจอย่างรุนแรงต้องยกระดับทันที
7. **ความปลอดภัย สุขภาพ และสวัสดิภาพ**	ต่ำ/ ศูนย์ สำหรับเหตุร้ายแรง	➢ ยอมรับความเสี่ยงทั่วไปได้เฉพาะภายใต้มาตรการที่เหมาะสม และไม่ยอมรับการเสียชีวิต การบาดเจ็บร้ายแรง หรือความเสียหายรุนแรงที่เกิดจากการละเลยมาตรการที่กำหนด

เหตุที่ไม่ยอมรับ (Zero Tolerance Event)

เหตุที่ไม่ยอมรับ (Zero Tolerance Event) หมายถึง เหตุการณ์ พฤติการณ์ หรือสัญญาณที่เข้าเกณฑ์ซึ่งมหาวิทยาลัยไม่ยอมรับ และต้องระงับเหตุ รายงาน หรือยกระดับไปยังผู้มีอำนาจตัดสินใจทันที โดยไม่รอผลคะแนนความเสี่ยงรวม ทั้งนี้ รวมถึงกรณีที่มีข้อสงสัยอย่างมีเหตุผลหรือมีข้อมูลเบื้องต้นเพียงพอที่จะต้องตรวจสอบข้อเท็จจริง เช่น

1. การทุจริต การคอร์รัปชัน การรับสินบน ผลประโยชน์ทับซ้อนที่ไม่ได้เปิดเผย หรือการใช้ทรัพย์สินและงบประมาณของมหาวิทยาลัยโดยมิชอบ
2. การเสียชีวิต การบาดเจ็บร้ายแรง หรือเหตุการณ์ที่อาจก่อให้เกิดอันตรายร้ายแรงต่อชีวิตและสุขภาพ โดยไม่ต้องรอผลการพิจารณาว่าเกิดจากการละเลยมาตรการหรือไม่
3. การกระทำที่เป็นการฝ่าฝืนกฎหมาย ระเบียบ ข้อบังคับ จริยธรรม หรือหลักธรรมาภิบาลอย่างร้ายแรง
4. การคุกคามหรือการล่วงละเมิดทางเพศ การเลือกปฏิบัติ การใช้ความรุนแรง หรือการละเมิดสิทธิมนุษยชนอย่างร้ายแรง

5. การลอกเลียนผลงาน การสร้างหรือบิดเบือนข้อมูล การละเมิดจริยธรรมการวิจัย หรือการประพฤติมิชอบทางวิชาการและการวิจัยอย่างร้ายแรง

6. การรั่วไหล การสูญหาย การเข้าถึงโดยมิชอบ หรือการทำลายข้อมูลสำคัญหรือข้อมูลส่วนบุคคล ซึ่งอาจส่งผลกระทบรุนแรงต่อเจ้าของข้อมูล พันธกิจ หรือชื่อเสียงของมหาวิทยาลัย

7. เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่กระทบต่อระบบหรือบริการสำคัญในวงกว้าง หรืออาจทำให้พันธกิจสำคัญของมหาวิทยาลัยหยุดชะงัก

8. เหตุการณ์ด้านสิ่งแวดล้อม ความปลอดภัย หรือสาธารณภัยที่อาจก่อให้เกิดผลกระทบรุนแรงต่อบุคคล ชุมชน ทรัพย์สิน หรือสิ่งแวดล้อม

9. การปกปิด ทำลาย บิดเบือน หรือรายงานข้อมูลสำคัญอันเป็นเท็จ รวมถึงการขัดขวางการตรวจสอบหรือการสอบสวนข้อเท็จจริง

เมื่อพบเหตุหรือสัญญาณที่เข้าเกณฑ์ ผู้เกี่ยวข้องต้องดำเนินการตามลำดับความจำเป็น ได้แก่

- ระงับหรือจำกัดความเสียหายและคุ้มครองชีวิตเป็นลำดับแรก
- รักษาข้อมูล เอกสาร พยานหลักฐาน และความลับที่เกี่ยวข้อง
- รายงานผ่านช่องทางและภายในระยะเวลาที่กำหนด
- แจ้งหน่วยงานตามกฎหมายหรือหน่วยงานกำกับดูแลเมื่อเข้าเงื่อนไข
- ตรวจสอบข้อเท็จจริงโดยเป็นธรรมและรักษาสิทธิของผู้เกี่ยวข้อง
- ดำเนินมาตรการแก้ไข เยียวยา ฟื้นฟู และป้องกันการเกิดซ้ำ
- ติดตามและรายงานผลต่อผู้มีอำนาจจนกว่าเหตุการณ์จะได้รับการจัดการอย่างเหมาะสม

มหาวิทยาลัยต้องคุ้มครองผู้รายงาน ผู้ร้องเรียน พยาน และผู้ให้ข้อมูลโดยสุจริตจากการตอบโต้หรือการปฏิบัติที่ไม่เป็นธรรม พร้อมรักษาความลับตามกฎหมายและระเบียบที่เกี่ยวข้อง

การกำหนด Zero Tolerance มิได้หมายความว่ามหาวิทยาลัยรับรองว่าเหตุการณ์จะไม่เกิดขึ้น แต่หมายถึงมหาวิทยาลัยไม่ยอมรับการเพิกเฉย การปกปิด หรือการปล่อยให้เหตุดังกล่าวดำเนินต่อไป และเมื่อพบเหตุหรือข้อสงสัยที่มีมูล ต้องดำเนินการและยกระดับโดยไม่ชักช้า

ทั้งนี้ การรายงานหรือยกระดับเหตุไม่ถือเป็นข้อยุติว่าบุคคลใดกระทำความผิด การวินิจฉัยความรับผิดต้องเป็นไปตามกระบวนการตรวจสอบข้อเท็จจริง กฎหมาย และหลักความเป็นธรรม

การกำหนด อนุมัติ และทบทวนระดับความเบี่ยงเบนที่ยอมรับได้ *(Risk Tolerance Approval and Review)*

ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) ต้องกำหนดให้สอดคล้องกับวัตถุประสงค์ ตัวชี้วัด ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) ข้อจำกัดตามกฎหมาย และความสามารถในการตอบสนองของมหาวิทยาลัย โดยต้องมีความชัดเจน สามารถวัดผล ติดตาม และนำไปใช้ตัดสินใจได้

การกำหนด RT ต้องระบุอย่างน้อย ดังนี้

1. วัตถุประสงค์หรือผลการดำเนินงานที่เกี่ยวข้อง

2. ตัวชี้วัดและคำจำกัดความของตัวชี้วัด
3. ค่า RA และช่วงหรือจุดเริ่มต้นของ RT
4. เกณฑ์ที่ถือว่าเกิน RT
5. แหล่งข้อมูล เจ้าของข้อมูล และความถี่ในการติดตาม
6. เจ้าของความเสี่ยงและผู้มีอำนาจตัดสินใจ
7. มาตรการที่ต้องดำเนินการเมื่อเข้าใกล้หรือเกิน RT
8. เส้นทางและระยะเวลาในการยกระดับรายงาน

การอนุมัติและนำ RT ไปใช้ให้เป็นไปตามหลักการ ดังนี้

- **ระดับมหาวิทยาลัย:** RA/RT สำหรับความเสี่ยงสำคัญหรือมิติความเสี่ยงระดับมหาวิทยาลัย ต้องผ่านการพิจารณาของคณะกรรมการที่เกี่ยวข้องและเสนอผู้มีอำนาจอนุมัติตามโครงสร้างการกำกับดูแล
- **ระดับส่วนงาน:** ส่วนงานอาจกำหนด RT ที่เข้มงวดกว่ากรอบของมหาวิทยาลัยตามลักษณะภารกิจ ขนาด ความซับซ้อน และระดับความเสี่ยงของตน โดยได้รับอนุมัติจากหัวหน้าส่วนงานและรายงานต่อหน่วยงานกำกับที่เกี่ยวข้อง
- ส่วนงานต้องไม่กำหนด RT ที่ผ่อนคลายกว่ากรอบระดับมหาวิทยาลัย เว้นแต่ผ่านการวิเคราะห์เหตุผล ผลกระทบ และมาตรการรองรับ และได้รับอนุมัติจากผู้มีอำนาจตามตารางอำนาจอนุมัติความเสี่ยง (Risk Acceptance Authority Matrix)
- ห้ามกำหนด RT เพื่อผ่อนคลายข้อกำหนดตามกฎหมาย ข้อห้ามด้านจริยธรรม หรือเหตุ Zero Tolerance ของมหาวิทยาลัย
- เมื่อผลการติดตามเข้าใกล้ RT ต้องเฝ้าระวังและเตรียมมาตรการแก้ไข และเมื่อเกิน RT ต้องดำเนินมาตรการ ยกระดับรายงาน และเสนอผู้มีอำนาจพิจารณาภายในระยะเวลาที่กำหนด

RA/RT ต้องได้รับการทบทวนอย่างน้อยปีละหนึ่งครั้ง และเมื่อเกิดกรณีใดกรณีหนึ่ง ดังต่อไปนี้

- วัตถุประสงค์ ยุทธศาสตร์ หรือตัวชี้วัดเปลี่ยนแปลง
- กฎหมาย ข้อกำหนด หรือนโยบายสำคัญเปลี่ยนแปลง
- บริบทหรือข้อมูลฐานเปลี่ยนแปลงอย่างมีนัยสำคัญ
- เกิดเหตุ Zero Tolerance เหตุวิกฤต หรือความเสียหายรุนแรง
- ผลการติดตามเกิน RT ติดต่อกันหรือเกิดซ้ำ
- การควบคุมสำคัญไม่ทำงานหรือไม่มีประสิทธิผล
- มีความเสี่ยงเกิดใหม่หรือความสัมพันธ์ของความเสี่ยงเปลี่ยนแปลง
- มีข้อสังเกตสำคัญจากการตรวจสอบหรือหน่วยงานกำกับดูแล

ผลการกำหนดอนุมัติ หรือปรับเปลี่ยน RT ต้องบันทึกเหตุผล ข้อมูลประกอบ ผู้เสนอ ผู้อนุมัติ วันที่มีผลใช้บังคับ มาตรการรองรับ และวันที่ทบทวนครั้งถัดไปไว้ในทะเบียนความเสี่ยงหรือระบบที่มหาวิทยาลัยกำหนดอย่างครบถ้วน

2.4 วิสัยทัศน์ด้านการบริหารความเสี่ยง

“เป็นมหาวิทยาลัยที่บริหารความเสี่ยงและการควบคุมภายในอย่างบูรณาการ เชื่อมโยงยุทธศาสตร์ ตัดสินใจบนฐานข้อมูล และมีความยืดหยุ่นเพื่อสร้างคุณค่าอย่างยั่งยืน”

“A risk-informed and resilient university where integrated risk management and internal control support strategy, data-driven decision-making, and sustainable value creation.”

องค์ประกอบสำคัญของวิสัยทัศน์ ได้แก่

- **บูรณาการ (Integrated):** ความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ และการให้ความเชื่อมั่นทำงานเชื่อมโยงกัน
- **เชื่อมโยงยุทธศาสตร์ (Strategy-aligned):** ใช้ความเสี่ยงและโอกาสสนับสนุนการบรรลุเป้าหมายของมหาวิทยาลัย
- **ตัดสินใจบนฐานข้อมูล (Data-driven Decision-making):** ใช้ RA/RT, KRI และสัญญาณเตือนล่วงหน้าประกอบการตัดสินใจ
- **มีความยืดหยุ่น (Resilient):** สามารถเตรียมพร้อม ตอบสนอง ปรับตัว และฟื้นตัวจากเหตุหยุดชะงัก
- **สร้างคุณค่าอย่างยั่งยืน (Sustainable Value Creation):** สร้าง รักษา และเพิ่มคุณค่าให้แก่มหาวิทยาลัยและผู้มีส่วนได้ส่วนเสีย

2.5 วัตถุประสงค์เชิงนโยบาย

นโยบายการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้มีวัตถุประสงค์เพื่อ

1. สนับสนุนการบรรลุยุทธศาสตร์: สนับสนุนการบรรลุวิสัยทัศน์ พันธกิจ วัตถุประสงค์เชิงยุทธศาสตร์ ตัวชี้วัด และผลลัพธ์สำคัญของมหาวิทยาลัยภายใต้ความไม่แน่นอน

2. ยกระดับคุณภาพการตัดสินใจ: ส่งเสริมให้การกำหนดนโยบาย การลงทุน การอนุมัติโครงการ การจัดลำดับความสำคัญ และการจัดสรรทรัพยากร ใช้ข้อมูลความเสี่ยงและโอกาสประกอบการตัดสินใจอย่างเป็นระบบ (Risk-informed and Data-driven Decision-making)

3. บริหารความเสี่ยงภายในกรอบที่ยอมรับได้: กำกับให้การดำเนินงานและการตัดสินใจสอดคล้องกับความสามารถในการรองรับความเสี่ยง (Risk Capacity) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT)

4. บูรณาการการบริหารความเสี่ยงทั่วทั้งองค์กร: เชื่อมโยงความเสี่ยงระหว่างยุทธศาสตร์ พันธกิจ ส่วนงาน กระบวนการ โครงการ และบุคคลภายนอก โดยพิจารณาความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัวของความเสี่ยง เพื่อป้องกันการบริหารแบบแยกส่วน

5. ลดผลกระทบและเสริมสร้างความยืดหยุ่น: ป้องกันและลดความสูญเสียหรือผลกระทบที่ไม่พึงประสงค์ พร้อมเพิ่มความพร้อมในการคาดการณ์ เตรียมการ ตอบสนอง และฟื้นตัวจากเหตุฉุกเฉิน ภาวะวิกฤต เหตุหยุดชะงัก และความเสี่ยงเกิดใหม่

6. เสริมสร้างธรรมาภิบาลและการให้ความเชื่อมั่น: บูรณาการธรรมาภิบาล การบริหารความเสี่ยง การปฏิบัติตามกฎเกณฑ์ การควบคุมภายใน และการให้ความเชื่อมั่นตามแนวทาง GRC และหลัก Three Lines เพื่อให้เกิดความโปร่งใส ความรับผิดชอบ และการตรวจสอบได้

7. ส่งเสริมวัฒนธรรมและความรับผิดชอบร่วมกัน: สร้างความตระหนัก ความรู้ ความสามารถ ความเป็นเจ้าของความเสี่ยง และสภาพแวดล้อมที่เอื้อต่อการรายงานข้อมูลหรือข้อกังวลโดยสุจริตของผู้บริหารและบุคลากรทุกระดับ

8. สร้างคุณค่าและความยั่งยืน: สนับสนุนการบริหารโอกาส การสร้าง รักษา และเพิ่มคุณค่า ตลอดจนเสริมสร้างความเป็นเลิศ ความเชื่อมั่น ความปลอดภัย ความรับผิดชอบด้าน ESG และความยั่งยืนของมหาวิทยาลัยในระยะยาว

“การบริหารความเสี่ยงของมหาวิทยาลัยมุ่งสนับสนุนยุทธศาสตร์และการตัดสินใจบนฐานข้อมูล ให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้ พร้อมสร้างคุณค่า ความเชื่อมั่น ความยืดหยุ่น และความยั่งยืนให้แก่มหาวิทยาลัย”

2.6 โครงสร้างกรอบการบริหารความเสี่ยงที่มหาวิทยาลัยประยุกต์ใช้

มหาวิทยาลัยแม่โจ้ใช้กฎหมาย หลักเกณฑ์ มาตรฐาน และกรอบแนวปฏิบัติแต่ละชุดตามวัตถุประสงค์และขอบเขตที่แตกต่างกัน โดยบูรณาการให้เป็นระบบบริหารความเสี่ยงเดียวของมหาวิทยาลัย ดังนี้

ตารางที่ 2-2 *กรอบอ้างอิงและการประยุกต์ใช้ในระบบบริหารความเสี่ยงของมหาวิทยาลัย*

กรอบอ้างอิง	บทบาทหลักในการประยุกต์ใช้	การนำมาใช้ในระบบของมหาวิทยาลัย
1. **หลักเกณฑ์กระทรวงการคลังด้านการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ**	เป็นข้อกำหนดพื้นฐานสำหรับการจัดให้มีระบบบริหารความเสี่ยงของหน่วยงานของรัฐ	ใช้กำหนดองค์ประกอบขั้นต่ำ โครงสร้างความรับผิดชอบ แผนบริหารความเสี่ยง การติดตาม การรายงาน และหลักฐานการดำเนินงาน
2. COSO Enterprise Risk Management—Integrating with Strategy and Performance (2017)	เชื่อมโยงการกำกับดูแล ยุทธศาสตร์ ผลการดำเนินงาน ความเสี่ยง และการสร้างคุณค่า	ใช้กำหนดการกำกับดูแลและวัฒนธรรม การเชื่อมโยงความเสี่ยงกับยุทธศาสตร์ การพิจารณาภาพรวมความเสี่ยง (Risk Portfolio) และการใช้ข้อมูลความเสี่ยงประกอบการตัดสินใจ
3. ISO 31000:2018 Risk Management—Guidelines	กำหนดหลักการ กรอบ และกระบวนการบริหารความเสี่ยงที่สามารถใช้กับทุกประเภทความเสี่ยงและทุกระดับ	ใช้ออกแบบกระบวนการกำหนดขอบเขตและบริบท การระบุ วิเคราะห์ ประเมิน ตอบสนอง ติดตาม ทบทวน สื่อสาร และปรึกษาหารือ

กรอบอ้างอิง	บทบาทหลักในการประยุกต์ใช้	การนำมาใช้ในระบบของมหาวิทยาลัย
4. **COSO Internal Control—Integrated Framework (2013) และ หลักเกณฑ์กระทรวงการคลังด้านการควบคุมภายใน**	กำหนดองค์ประกอบสำหรับการออกแบบ ดำเนินการ และประเมินระบบควบคุมภายใน	ใช้ประเมินความเพียงพอของการออกแบบและประสิทธิผลของการควบคุม รวมทั้งจัดทำรายงานการควบคุมภายในและแผนปรับปรุง
5. **The IIA's Three Lines Model และ มาตรฐานการตรวจสอบภายในที่มีผลใช้บังคับ**	กำหนดความสัมพันธ์ระหว่างผู้กำกับดูแล ฝ่ายบริหาร หน้าที่กำกับเฉพาะด้าน และการให้ความเชื่อมั่นอย่างเป็นอิสระ	ใช้กำหนดบทบาทของสภามหาวิทยาลัย ฝ่ายบริหาร สายงานที่หนึ่ง สายงานที่สอง กองตรวจสอบภายใน และผู้ให้ความเชื่อมั่นอื่น โดยไม่ให้การตรวจสอบภายในบริหารความเสี่ยงแทนฝ่ายบริหาร
6. **ISO 22301:2019 Business Continuity Management Systems และฉบับแก้ไขเพิ่มเติม**	กำหนดหลักการและข้อกำหนดด้านการบริหารความต่อเนื่องขององค์กร	ใช้เชื่อมโยงความเสี่ยงกับการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) การจัดทำ BCM/BCP การกำหนดเป้าหมายการฟื้นตัว การทดสอบแผน และการเสริมสร้างความยืดหยุ่นขององค์กร
7. **Governance, Risk and Compliance: GRC**	เป็นแนวทางบูรณาการธรรมาภิบาล การบริหารความเสี่ยง และการปฏิบัติตามกฎเกณฑ์	ใช้เชื่อมโยงวัตถุประสงค์ ความเสี่ยง กฎหมาย การควบคุม ผู้รับผิดชอบ การรายงาน และการให้ความเชื่อมั่น เพื่อลดช่องว่างและความซ้ำซ้อน
8. **เกณฑ์คุณภาพการศึกษาเพื่อการดำเนินการที่เป็นเลิศ (EdPEx)**	เชื่อมโยงบริบท การนำองค์กร ยุทธศาสตร์ ลูกค้า บุคลากร การปฏิบัติการ และผลลัพธ์	ใช้บูรณาการข้อมูลความเสี่ยงกับการวางแผน การบริหารผลการดำเนินงาน การประเมินประสิทธิผล และการปรับปรุงองค์กร
9. **SDGs และ ESG**	เป็นกรอบพิจารณาความยั่งยืนและผลกระทบต่อผู้มีส่วนได้ส่วนเสีย	ใช้พิจารณาปัจจัยและผลกระทบร่วมด้านสิ่งแวดล้อม สังคม ธรรมาภิบาล ความปลอดภัย ชื่อเสียง และความยั่งยืนในการประเมินและตัดสินใจด้านความเสี่ยง

หลักการบูรณาการกรอบอ้างอิง

กรอบอ้างอิงดังกล่าวมีบทบาทสนับสนุนและเสริมกัน มิใช่กระบวนการหลายชุดที่ส่วนงานต้องดำเนินการซ้ำ มหาวิทยาลัยจึงกำหนดให้

1. ใช้กระบวนการบริหารความเสี่ยงกลาง แบบฟอร์มกลาง ฐานข้อมูลกลาง และเส้นทางการรายงานชุดเดียวกัน

2. เชื่อมโยงวัตถุประสงค์ ความเสี่ยง การควบคุม กฎหมายหรือข้อกำหนด ตัวชี้วัด มาตรการ และแหล่งการให้ความเชื่อมั่นไว้ในระบบเดียวกัน

3. จัดทำตารางเทียบเคียงกรอบอ้างอิง (Framework Crosswalk) เพื่อแสดงว่าองค์ประกอบและกระบวนการของมหาวิทยาลัยตอบสนองต่อกฎหมาย หลักเกณฑ์ และมาตรฐานแต่ละชุดอย่างไร

4. ใช้หลักความเหมาะสมตามสัดส่วน (Proportionality) โดยคำนึงถึงภารกิจ ขนาด ความซับซ้อน และระดับความเสี่ยงของแต่ละส่วนงาน

5. ยึดกฎหมาย ข้อบังคับ และหลักเกณฑ์ที่มีผลใช้บังคับเป็นลำดับแรก ส่วนมาตรฐานและกรอบแนวปฏิบัติภายนอกให้นำมาประยุกต์ใช้ตามบริบทและนโยบายของมหาวิทยาลัย

หลักการบูรณาการ—ระบบเดียว หลายกรอบอ้างอิง (One Integrated System, Multiple Frameworks): มหาวิทยาลัยใช้กระบวนการกลาง คำศัพท์ เกณฑ์ เครื่องมือ ฐานข้อมูล และหลักฐานร่วมเท่าที่เหมาะสม เพื่อสนับสนุนการกำกับดูแล การบริหารความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ การบริหารความต่อเนื่อง การประกันคุณภาพ และการให้ความเชื่อมั่น โดยมุ่งลดความซ้ำซ้อนและภาระในการดำเนินงานของส่วนงาน ทั้งนี้ ต้องไม่ลดทอนข้อกำหนดเฉพาะตามกฎหมาย หลักเกณฑ์ หรือมาตรฐานแต่ละกรอบ

2.7 กรอบ COSO ERM 2017

COSO Enterprise Risk Management—Integrating with Strategy and Performance (2017) ประกอบด้วย 5 องค์ประกอบและ 20 หลักการ ซึ่งมีความเชื่อมโยงและสนับสนุนกัน มหาวิทยาลัยนำมาประยุกต์ใช้เพื่อบูรณาการการบริหารความเสี่ยงเข้ากับการกำกับดูแล การกำหนดยุทธศาสตร์ และการบริหารผลการดำเนินงาน ดังนี้

1) การกำกับดูแลและวัฒนธรรมองค์กร *(Governance and Culture)*

1. **กำกับดูแลความเสี่ยงโดยผู้กำกับดูแล:** สภามหาวิทยาลัยกำกับทิศทาง นโยบาย กรอบ RA/RT และความเพียงพอของระบบบริหารความเสี่ยง
2. **จัดตั้งโครงสร้างการดำเนินงาน:** กำหนดโครงสร้าง บทบาท อำนาจตัดสินใจ ความรับผิดชอบ และเส้นทางการรายงานอย่างชัดเจน
3. **กำหนดวัฒนธรรมที่พึงประสงค์:** ส่งเสริมวัฒนธรรมที่ตระหนักถึงความเสี่ยง เปิดเผย โปร่งใส และเอื้อต่อการรายงานโดยสุจริต
4. **แสดงความมุ่งมั่นต่อค่านิยมหลัก:** ผู้กำกับดูแล ผู้บริหาร และบุคลากรปฏิบัติตามค่านิยม จริยธรรม และหลักธรรมาภิบาลของมหาวิทยาลัย
5. **ดึงดูด พัฒนา และรักษาบุคลากรที่มีความสามารถ:** พัฒนาความรู้ ทักษะ และความสามารถด้านการบริหารความเสี่ยงให้เหมาะสมกับบทบาท

2) ยุทธศาสตร์และการกำหนดวัตถุประสงค์ *(Strategy and Objective-Setting)*

6. **วิเคราะห์บริบทขององค์กรและการดำเนินงาน:** วิเคราะห์ปัจจัยภายใน ภายนอก ผู้มีส่วนได้ส่วนเสีย สมมติฐาน และแนวโน้มที่อาจส่งผลต่อมหาวิทยาลัย

7. กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite): กำหนดประเภทและระดับความเสี่ยงที่มหาวิทยาลัยยินดีรับในการดำเนินยุทธศาสตร์และบรรลุวัตถุประสงค์

8. ประเมินยุทธศาสตร์ทางเลือก: พิจารณาความเสี่ยง โอกาส ผลได้ ผลเสีย และความสอดคล้องกับ Risk Appetite ก่อนเลือกยุทธศาสตร์หรือแนวทางสำคัญ

9. กำหนดวัตถุประสงค์ขององค์กรและการดำเนินงาน: กำหนดวัตถุประสงค์ ตัวชี้วัด และผลลัพธ์ให้ชัดเจน สามารถประเมินความเสี่ยงที่อาจส่งผลต่อการบรรลุเป้าหมายได้

3) ผลการดำเนินงาน *(Performance)*

10. ระบุความเสี่ยง: ระบุเหตุการณ์ สาเหตุ ปัจจัยขับเคลื่อน และผลกระทบที่อาจมีต่อวัตถุประสงค์

11. ประเมินความรุนแรงของความเสี่ยง: ประเมินโอกาสเกิด ผลกระทบ ประสิทธิผลของการควบคุม และระดับความเสี่ยงคงเหลือ

12. จัดลำดับความสำคัญของความเสี่ยง: จัดลำดับโดยพิจารณาคะแนนความเสี่ยง RA/RT ความเร่งด่วน ความสัมพันธ์ และผลกระทบต่อยุทธศาสตร์

13. ดำเนินการตอบสนองต่อความเสี่ยง: เลือกและดำเนินแนวทางหลีกเลี่ยง ลดหรือควบคุม แบ่งปันหรือถ่ายโอน ยอมรับ หรือใช้ประโยชน์จากโอกาส

14. พัฒนามุมมองภาพรวมความเสี่ยง (Portfolio View): พิจารณาความสัมพันธ์ ผลกระทบร่วม การกระจุกตัว และระดับความเสี่ยงรวมในภาพมหาวิทยาลัย ไม่พิจารณาเฉพาะรายส่วนงาน

4) การทบทวนและปรับปรุง *(Review and Revision)*

15. ประเมินการเปลี่ยนแปลงที่มีสาระสำคัญ: ติดตามการเปลี่ยนแปลงด้านยุทธศาสตร์ กฎหมาย เทคโนโลยี เศรษฐกิจ สังคม สิ่งแวดล้อม และโครงสร้างองค์กรที่อาจเปลี่ยนระดับความเสี่ยง

16. ทบทวนความเสี่ยงและผลการดำเนินงาน: เปรียบเทียบผลจริงกับวัตถุประสงค์ KPI, KRI, RA/RT และระดับความเสี่ยงเป้าหมาย

17. ปรับปรุงการบริหารความเสี่ยงองค์กร: ใช้ผลการติดตาม เหตุการณ์จริง ข้อสังเกตจากการตรวจสอบ และบทเรียนมาพัฒนากรอบ กระบวนการ การควบคุม และความสามารถของบุคลากร

5) สารสนเทศ การสื่อสาร และการรายงาน *(Information, Communication and Reporting)*

18. ใช้ประโยชน์จากสารสนเทศและเทคโนโลยี: ใช้ข้อมูล ระบบสารสนเทศ การวิเคราะห์ข้อมูล และเทคโนโลยีสนับสนุนการติดตาม คาดการณ์ และตัดสินใจด้านความเสี่ยง

19. สื่อสารข้อมูลความเสี่ยง: สื่อสารข้อมูลความเสี่ยง โอกาส ความรับผิดชอบ และเกณฑ์การดำเนินการให้เหมาะสมกับผู้รับสารและระดับการตัดสินใจ

20. รายงานความเสี่ยง วัฒนธรรม และผลการดำเนินงาน: จัดทำรายงานที่ถูกต้อง ครบถ้วน ทันเวลา และแสดงความเชื่อมโยงระหว่างวัตถุประสงค์ ความเสี่ยง การควบคุม มาตรการ และผลลัพธ์

หลักการนำไปประยุกต์ใช้

การนำ 20 หลักการไปใช้ให้พิจารณาตามความเหมาะสมกับบริบท ภารกิจ ขนาด ความซับซ้อน และระดับความเสี่ยงของมหาวิทยาลัยและส่วนงาน โดยต้องเชื่อมโยงกับกระบวนการและหลักฐานที่สามารถตรวจสอบได้ ทั้งนี้

- หลักการทั้ง 20 ประการเป็นองค์ประกอบที่เชื่อมโยงกัน มิใช่ขั้นตอนที่ต้องดำเนินการเรียงตามลำดับ
- ไม่จำเป็นต้องจัดทำแบบฟอร์มหรือรายงานแยกสำหรับแต่ละหลักการ
- หลักฐานหนึ่งรายการอาจสนับสนุนได้มากกว่าหนึ่งหลักการ
- ควรใช้ข้อมูลและหลักฐานจากกระบวนการบริหารงานตามปกติให้มากที่สุด
- หน่วยงานผู้รับผิดชอบควรจัดทำตารางเทียบเคียง (COSO ERM Crosswalk) เพื่อแสดงกระบวนการผู้รับผิดชอบ และหลักฐานที่รองรับแต่ละหลักการ
- การประยุกต์ใช้กรอบ COSO ERM ไม่ถือเป็นการรับรองความสอดคล้อง เว้นแต่ผ่านการประเมินตามเกณฑ์และขอบเขตที่มหาวิทยาลัยกำหนด

2.8 การประยุกต์ใช้หลักการบริหารความเสี่ยงตาม ISO 31000:2018

มหาวิทยาลัยประยุกต์ใช้หลักการบริหารความเสี่ยงตาม ISO 31000:2018 จำนวน 8 ประการ เพื่อสนับสนุนการสร้างและปกป้องคุณค่า ดังนี้

ตารางที่ 2-3 หลักการ ISO 31000:2018 และแนวทางการประยุกต์ใช้ของมหาวิทยาลัย

หลักการ	แนวทางการประยุกต์ใช้ของมหาวิทยาลัย
1.บูรณาการ (Integrated)	บูรณาการการบริหารความเสี่ยงเข้ากับการกำกับดูแล การกำหนดยุทธศาสตร์ การวางแผน การจัดทำงบประมาณ การบริหารโครงการ การจัดสรรทรัพยากร การควบคุมภายใน และการตัดสินใจทุกระดับ
2.มีโครงสร้างและครอบคลุม (Structured and Comprehensive)	ใช้กระบวนการ คำศัพท์ เกณฑ์ประเมิน แบบฟอร์ม และแนวทางรายงานที่เป็นระบบและเป็นมาตรฐานเดียวกัน เพื่อให้สามารถเปรียบเทียบ ติดตาม และรวบรวมผลในภาพมหาวิทยาลัยได้
3.เหมาะสมกับบริบท (Customized)	ปรับระดับรายละเอียด วิธีการ และเครื่องมือให้เหมาะสมกับวัตถุประสงค์ ภารกิจ ขนาด โครงสร้าง วัฒนธรรม ความซับซ้อน และระดับความเสี่ยงของมหาวิทยาลัยและแต่ละส่วนงาน
4.มีส่วนร่วม (Inclusive)	เปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องมีส่วนร่วมอย่างเหมาะสมและทันเวลา เพื่อให้ได้รับข้อมูล มุมมอง ความรู้เฉพาะด้าน และความเข้าใจความเสี่ยงที่รอบด้าน
5.พลวัต (Dynamic)	ติดตามการเปลี่ยนแปลงของบริบท ปัจจัยขับเคลื่อนความเสี่ยง ความเสี่ยงเกิดใหม่ KRI และสัญญาณเตือนล่วงหน้า พร้อมปรับการประเมินและมาตรการให้ทันต่อสถานการณ์

หลักการ	แนวทางการประยุกต์ใช้ของมหาวิทยาลัย
6. ใช้สารสนเทศที่ดีที่สุดเท่าที่มี (Best Available Information)	ใช้ข้อมูลในอดีต ข้อมูลปัจจุบัน การวิเคราะห์แนวโน้ม และการคาดการณ์ประกอบการตัดสินใจ พร้อมระบุแหล่งข้อมูล คุณภาพข้อมูล ข้อจำกัด ความไม่แน่นอน และสมมติฐานอย่างโปร่งใส
7. คำนึงถึงปัจจัยมนุษย์และวัฒนธรรม (Human and Cultural Factors)	พิจารณาค่านิยม พฤติกรรม ความรู้ ความสามารถ แรงจูงใจ อคติ การสื่อสาร และวัฒนธรรมองค์กรที่อาจส่งผลต่อการตัดสินใจและประสิทธิผลของการบริหารความเสี่ยง
8. ปรับปรุงอย่างต่อเนื่อง (Continual Improvement)	ใช้ผลการติดตาม เหตุการณ์จริง ข้อร้องเรียน ข้อสังเกตจากการตรวจสอบ การทดสอบแผน และบทเรียนที่ได้รับมาพัฒนากรอบ กระบวนการ ข้อมูล เครื่องมือ การควบคุม และความสามารถด้านความเสี่ยงอย่างต่อเนื่อง

หลักการทั้ง 8 ประการเป็นคุณลักษณะของระบบบริหารความเสี่ยงที่มีประสิทธิผล มิใช่ขั้นตอนการปฏิบัติงานที่ต้องดำเนินการเรียงตามลำดับ และต้องประยุกต์ใช้ร่วมกันตลอดกระบวนการบริหารความเสี่ยง

2.9 ความเชื่อมโยงกับแผนยุทธศาสตร์มหาวิทยาลัย

มหาวิทยาลัยกำหนดให้การบริหารความเสี่ยงและการบริหารยุทธศาสตร์เป็นกระบวนการที่เชื่อมโยงกันทั้งในขั้นการกำหนด การนำไปปฏิบัติ การติดตาม และการทบทวนยุทธศาสตร์ โดยมีหลักการดังนี้

1. เชื่อมโยงกับวัตถุประสงค์อย่างชัดเจน: ความเสี่ยงทุกเรื่องต้องเชื่อมโยงกับวิสัยทัศน์ พันธกิจ วัตถุประสงค์ ผลลัพธ์เชิงยุทธศาสตร์ ตัวชี้วัดผลการดำเนินงาน หรือภารกิจที่ต้องคุ้มครองอย่างชัดเจน

2. พิจารณาความเสี่ยงตั้งแต่ขั้นกำหนดยุทธศาสตร์: การจัดทำหรือทบทวนแผนยุทธศาสตร์ต้องพิจารณาบริบท ผู้มีส่วนได้ส่วนเสีย สมมติฐาน ความเสี่ยง โอกาส ความสามารถในการรองรับความเสี่ยง RA/RT และความเสี่ยงของยุทธศาสตร์ทางเลือกก่อนตัดสินใจ

3. ประเมินความเสี่ยงก่อนอนุมัติโครงการสำคัญ: นโยบาย โครงการ การลงทุน หรือภาระผูกพันที่มีนัยสำคัญ ต้องได้รับการประเมินความเสี่ยง ความคุ้มค่า ความพร้อม ข้อจำกัดตามกฎหมาย ผลกระทบต่อผู้มีส่วนได้ส่วนเสีย และผลกระทบต่อภาพรวมความเสี่ยงของมหาวิทยาลัยก่อนอนุมัติ

4. กำหนดความรับผิดชอบและตัวชี้วัด: วัตถุประสงค์เชิงยุทธศาสตร์และโครงการสำคัญต้องกำหนดเจ้าของวัตถุประสงค์ เจ้าของความเสี่ยง KPI, KRI, RA/RT มาตรการตอบสนอง และเส้นทางการรายงานที่ชัดเจน

5. พิจารณาความเสี่ยงในภาพรวมมหาวิทยาลัย: ความเสี่ยงที่กระทบหลายส่วนงาน มีความสัมพันธ์หรือการกระจุกตัวสูง เกิน RT เกินอำนาจยอมรับของส่วนงาน หรืออาจกระทบวัตถุประสงค์เชิงยุทธศาสตร์อย่างมีนัยสำคัญ ต้องยกระดับเพื่อเสนอพิจารณาบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัย (University-level/Enterprise Risk)

6. ติดตามความเสี่ยงควบคู่กับผลการดำเนินงาน: รายงานผลยุทธศาสตร์ต้องแสดงทั้งผลการดำเนินงานตาม KPI แนวโน้มความเสี่ยงตาม KRI สถานะ RA/RT ประสิทธิผลของการควบคุม และความก้าวหน้าของมาตรการสำคัญ

7. ใช้ผลการติดตามประกอบการตัดสินใจ: เมื่อผลการดำเนินงานไม่เป็นไปตามเป้าหมาย KRI เข้าใกล้หรือเกิน RT สมมติฐานเปลี่ยนแปลง หรือการควบคุมไม่เพียงพอ ต้องใช้ข้อมูลดังกล่าวประกอบการปรับแผน ปรับมาตรการ จัดสรรทรัพยากร หรือยกระดับการตัดสินใจโดยไม่ชักช้า

8. ทบทวนยุทธศาสตร์และภาพรวมความเสี่ยงร่วมกัน: มหาวิทยาลัยต้องทบทวนความสอดคล้องระหว่างยุทธศาสตร์ ผลการดำเนินงาน และภาพรวมความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อบริบทเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.10 ความเชื่อมโยงกับการควบคุมภายในและการให้ความเชื่อมั่น

การบริหารความเสี่ยงใช้เพื่อระบุ วิเคราะห์ และประเมินความไม่แน่นอนที่อาจส่งผลต่อวัตถุประสงค์ ขณะที่การควบคุมภายในเป็นนโยบาย กระบวนการ ระบบ และกิจกรรมที่ออกแบบและดำเนินการเพื่อจัดการความเสี่ยงและให้ความเชื่อมั่นอย่างสมเหตุสมผลต่อการบรรลุวัตถุประสงค์ด้านการดำเนินงาน การรายงาน และการปฏิบัติตามกฎหมาย

มหาวิทยาลัยกำหนดให้ความเสี่ยงสำคัญเชื่อมโยงกับการควบคุม ผู้รับผิดชอบ หลักฐานการปฏิบัติ และแหล่งการให้ความเชื่อมั่น โดยใช้แนวทางความเชื่อมโยงความเสี่ยง–การควบคุม–การให้ความเชื่อมั่น (Risk–Control–Assurance) ดังนี้

วัตถุประสงค์ ⟶ ความเสี่ยง ⟶ การควบคุม ⟶ หลักฐานการปฏิบัติ ⟶ ความเสี่ยงคงเหลือ ⟶ การให้ความเชื่อมั่น ⟶ การปรับปรุง

การประเมินการควบคุม

มหาวิทยาลัยกำหนดให้ประเมินการควบคุมอย่างน้อย 3 มิติ ได้แก่

1. ความเหมาะสมของการออกแบบ (Design Adequacy): การควบคุมตอบสนองต่อสาเหตุหรือผลกระทบของความเสี่ยง มีผู้รับผิดชอบ ความถี่ ขั้นตอน และหลักฐานที่ชัดเจนหรือไม่

2. การนำไปใช้ (Implementation): การควบคุมได้รับการนำไปใช้จริง ครอบคลุมหน่วยงานหรือกระบวนการตามขอบเขตที่กำหนดหรือไม่

3. ประสิทธิผลในการปฏิบัติงาน (Operating Effectiveness): การควบคุมทำงานอย่างต่อเนื่อง ถูกต้องทันเวลา และสามารถลดโอกาสเกิดหรือผลกระทบของความเสี่ยงได้ตามวัตถุประสงค์หรือไม่

ผลการประเมินต้องมีหลักฐานที่เพียงพอและตรวจสอบย้อนกลับได้ เช่น เอกสารอนุมัติ รายงานจากระบบบันทึกการปฏิบัติงาน ผลการทดสอบ ตัวอย่างรายการ ข้อยกเว้น หรือข้อบกพร่องที่ตรวจพบ และใช้เป็นข้อมูลประกอบการประเมินความเสี่ยงคงเหลือ (Residual Risk)

หากพบว่าการควบคุมออกแบบไม่เหมาะสม ยังไม่ได้นำไปใช้ หรือทำงานไม่มีประสิทธิผล ต้องไม่ถือว่าการควบคุมนั้นช่วยลดระดับความเสี่ยงได้เต็มที่ และต้องกำหนดมาตรการปรับปรุง เจ้าของมาตรการ ระยะเวลา และการติดตามผลอย่างชัดเจน

การให้ความเชื่อมั่น

กองตรวจสอบภายในทำหน้าที่ให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรม โดย

- ไม่เป็นเจ้าของความเสี่ยงหรือเจ้าของการควบคุม
- ไม่กำหนด RA/RT หรือยอมรับความเสี่ยงแทนฝ่ายบริหาร
- ไม่เลือกหรือดำเนินมาตรการควบคุมที่ตนมีหน้าที่ตรวจสอบ
- ไม่รับผิดชอบต่อผลการบริหารความเสี่ยงแทนฝ่ายบริหาร

หากกองตรวจสอบภายในได้รับมอบหมายภารกิจให้คำปรึกษาหรือบทบาทอื่นที่อาจกระทบต่อความเป็นอิสระ ต้องได้รับอนุมัติ กำหนดขอบเขต เปิดเผยผลกระทบ และจัดให้มีมาตรการคุ้มครองความเป็นอิสระอย่างเหมาะสม

มหาวิทยาลัยกำหนดให้จัดทำแผนผังการให้ความเชื่อมั่น (Assurance Map) สำหรับความเสี่ยงสำคัญระดับมหาวิทยาลัย เพื่อระบุ

- ความเสี่ยงและการควบคุมสำคัญ
- ฝ่ายบริหารหรือเจ้าของการควบคุม
- หน่วยงานกำกับและติดตามในสายงานที่สอง
- กองตรวจสอบภายในและผู้ให้ความเชื่อมั่นภายนอก
- ขอบเขตและความถี่ของการประเมิน
- ระดับความเป็นอิสระของแหล่งความเชื่อมั่น
- ช่องว่างหรือความซ้ำซ้อนของการกำกับและตรวจสอบ

ส่วนงานให้นำแนวทางดังกล่าวไปใช้ตามหลักความเหมาะสมตามสัดส่วน (Proportionality) โดยไม่สร้างภาระเอกสารเกินความจำเป็น

2.11 ความเชื่อมโยงกับการพัฒนาองค์กรสู่ความเป็นเลิศ

การบริหารความเสี่ยงสนับสนุนการพัฒนาองค์กรตามเกณฑ์คุณภาพการศึกษาเพื่อการดำเนินการที่เป็นเลิศ (Education Criteria for Performance Excellence: EdPEx) โดยเชื่อมโยงความเสี่ยงและโอกาสกับองค์ประกอบสำคัญ ได้แก่

1. บริบทองค์กร: ใช้ข้อมูลบริบท ความท้าทาย ความได้เปรียบเชิงยุทธศาสตร์ และความคาดหวังของผู้มีส่วนได้ส่วนเสียเป็นข้อมูลในการระบุความเสี่ยงและโอกาส

2. การนำองค์กร: สนับสนุนให้ผู้กำกับดูแลและผู้บริหารกำหนดทิศทาง กำกับความเสี่ยง ส่งเสริมจริยธรรม และสร้างความรับผิดชอบต่อผลลัพธ์

3. ยุทธศาสตร์: ใช้ข้อมูลความเสี่ยง สมมติฐาน โอกาส และ RA/RT ประกอบการกำหนดวัตถุประสงค์เชิงยุทธศาสตร์ แผนปฏิบัติการ และการจัดสรรทรัพยากร

4. ผู้เรียน ลูกค้า และผู้มีส่วนได้ส่วนเสีย: ประเมินความเสี่ยงที่อาจกระทบความต้องการ ความคาดหวัง ความพึงพอใจ ความผูกพัน ความเชื่อมั่น และประสบการณ์ของผู้รับบริการ

5. การวัด การวิเคราะห์ และการจัดการความรู้: ใช้ KPI, KRI สัญญาณเตือนล่วงหน้า การวิเคราะห์ข้อมูลและบทเรียนจากเหตุการณ์สนับสนุนการตัดสินใจและการเรียนรู้ขององค์กร

6. บุคลากร: ประเมินความเสี่ยงด้านกำลังคน สมรรถนะ ความผูกพัน สุขภาวะ ความปลอดภัย การสืบทอดตำแหน่ง และความพร้อมต่อการเปลี่ยนแปลง

7. การปฏิบัติการ: เชื่อมโยงความเสี่ยงกับกระบวนการสำคัญ การควบคุมภายใน ผู้ส่งมอบ เทคโนโลยี ความต่อเนื่อง และความยืดหยุ่นของการดำเนินงาน

8. ผลลัพธ์: ติดตามความสัมพันธ์ระหว่างผลการดำเนินงาน ระดับความเสี่ยง ประสิทธิผลของการควบคุม และความก้าวหน้าของมาตรการ เพื่อใช้ปรับปรุงผลลัพธ์อย่างต่อเนื่อง

ส่วนงานต้องใช้ข้อมูลความเสี่ยงและโอกาสเป็นข้อมูลป้อนกลับในการทบทวนผลการดำเนินงาน การเรียนรู้และการปรับปรุงกระบวนการ โดยใช้ข้อมูลและหลักฐานจากระบบงานปกติร่วมกัน เพื่อลดการจัดทำรายงานหรือหลักฐานที่ซ้ำซ้อน

2.12 ความเชื่อมโยงกับ ESG และการพัฒนาอย่างยั่งยืน

มหาวิทยาลัยกำหนดให้การระบุ วิเคราะห์ ประเมิน และตอบสนองต่อความเสี่ยง พิจารณาปัจจัยและผลกระทบด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (Environmental, Social and Governance: ESG) ที่อาจส่งผลต่อยุทธศาสตร์ พันธกิจ ผู้มีส่วนได้ส่วนเสีย ชื่อเสียง และความยั่งยืนของมหาวิทยาลัย ดังนี้

ตารางที่ 2-4 มิติ ESG และประเด็นที่ควรพิจารณาในการบริหารความเสี่ยง

มิติ	ประเด็นที่ควรพิจารณา
สิ่งแวดล้อม (Environmental: E)	การเปลี่ยนแปลงสภาพภูมิอากาศทั้งความเสี่ยงทางกายภาพและความเสี่ยงจากการเปลี่ยนผ่าน ภัยพิบัติ ความหลากหลายทางชีวภาพ การใช้พลังงาน น้ำ และทรัพยากร มลพิษ ของเสีย และผลกระทบจากการดำเนินงานต่อสิ่งแวดล้อม
สังคม (Social: S)	สุขภาพและความปลอดภัย สิทธิมนุษยชน ความเสมอภาคและการไม่เลือกปฏิบัติ การคุกคามทางเพศ ความเป็นอยู่ของนักศึกษาและบุคลากร การเข้าถึงการศึกษา ความสัมพันธ์กับชุมชน และผลกระทบต่อผู้มีส่วนได้ส่วนเสีย
ธรรมาภิบาล (Governance: G)	โครงสร้างการกำกับดูแล จริยธรรม ความโปร่งใส การป้องกันการทุจริตและผลประโยชน์ทับซ้อน การปฏิบัติตามกฎหมาย การคุ้มครองข้อมูล ธรรมาภิบาลด้าน AI และความรับผิดชอบต่อการตัดสินใจ

มหาวิทยาลัยใช้ ESG เป็นมิติผลกระทบร่วมและป้ายกำกับข้ามประเภทความเสี่ยง (Cross-cutting Impact/Tag) เพื่อแสดงความเชื่อมโยงกับความเสี่ยงหลักทั้งด้านกลยุทธ์ การดำเนินงาน การเงิน และการปฏิบัติตามกฎหมายและธรรมาภิบาล โดยไม่จำเป็นต้องจัดทำทะเบียนความเสี่ยง ESG แยกซ้ำ

อย่างไรก็ตาม หากประเด็น ESG มีผลกระทบอย่างมีนัยสำคัญต่อวัตถุประสงค์เชิงยุทธศาสตร์ พันธกิจสำคัญ หรือผู้มีส่วนได้ส่วนเสีย มหาวิทยาลัยหรือส่วนงานต้องกำหนดเป็นความเสี่ยงหลักตามประเภทที่เหมาะสม พร้อมระบุเจ้าของความเสี่ยง KRI, RA/RT มาตรการ และเส้นทางการรายงานอย่างชัดเจน

การพิจารณาความสำคัญของประเด็น ESG ควรคำนึงถึงอย่างน้อย

- ขนาดและความรุนแรงของผลกระทบ
- โอกาสเกิดและระยะเวลาที่อาจเกิดผล
- จำนวนและความเปราะบางของผู้ได้รับผลกระทบ
- ข้อกำหนดตามกฎหมายและพันธกรณีของมหาวิทยาลัย
- ความคาดหวังของผู้มีส่วนได้ส่วนเสีย
- ผลกระทบต่อยุทธศาสตร์ การเงิน ชื่อเสียง และความต่อเนื่อง
- ความสามารถในการแก้ไข เยียวยา หรือฟื้นฟูผลกระทบ

2.13 แนวปฏิบัติขั้นต่ำด้านการบริหารความเสี่ยง

ทุกส่วนงานต้องดำเนินการบริหารความเสี่ยงตามมาตรฐานขั้นต่ำดังต่อไปนี้ โดยประยุกต์ใช้ตามหลักความเหมาะสมตามสัดส่วน (Proportionality) ให้สอดคล้องกับภารกิจ ขนาด ความซับซ้อน และระดับความเสี่ยงของส่วนงาน

1. กำหนดวัตถุประสงค์และบริบท: กำหนดวัตถุประสงค์ ผลลัพธ์หรือตัวชี้วัด เจ้าของวัตถุประสงค์ ขอบเขต และบริบทภายในและภายนอกที่เกี่ยวข้อง

2. ระบุและเขียนข้อความความเสี่ยง: ระบุความเสี่ยงโดยใช้โครงสร้างสาเหตุ–เหตุการณ์–ผลกระทบ (Cause–Event–Impact) และกำหนดเจ้าของความเสี่ยง (Risk Owner) ให้ชัดเจน

3. ประเมินความเสี่ยงโดยธรรมชาติ: ประเมินความเสี่ยงโดยธรรมชาติ (Inherent Risk) โดยยังไม่พิจารณาผลของการควบคุมหรือมาตรการที่มีอยู่

4. ระบุและประเมินการควบคุม: ระบุการควบคุมที่มีอยู่ เจ้าของการควบคุม และหลักฐานการปฏิบัติ พร้อมประเมินความเหมาะสมของการออกแบบ (Design Adequacy) การนำไปใช้ (Implementation) และประสิทธิผลในการปฏิบัติงาน (Operating Effectiveness)

5. ประเมินความเสี่ยงคงเหลือ: ประเมินความเสี่ยงคงเหลือ (Residual Risk) โดยอ้างอิงหลักฐานว่าการควบคุมได้รับการนำไปใช้และทำงานจริง หากไม่มีหลักฐานเพียงพอ ต้องไม่ถือว่าการควบคุมนั้นมีประสิทธิผลเต็มที่

6. เปรียบเทียบกับกรอบ RA/RT: เปรียบเทียบระดับความเสี่ยงคงเหลือกับ Risk Appetite และ Risk Tolerance เลือกแนวทางตอบสนอง และจัดทำแผนบริหารความเสี่ยง (Risk Treatment Plan) สำหรับความเสี่ยงที่เกินเกณฑ์หรือจำเป็นต้องปรับปรุงเพิ่มเติม

7. กำหนดตัวชี้วัดความเสี่ยง: กำหนด KRI โดยระบุนิยาม สูตรคำนวณ หน่วยวัด แหล่งข้อมูล เจ้าของข้อมูล ความถี่ ค่า RA ช่วงเฝ้าระวังหรือ RT และเงื่อนไขการดำเนินการ (Trigger/Action) เมื่อเข้าใกล้หรือเกินเกณฑ์

8. ติดตามและรายงานตามระดับความเสี่ยง: ติดตามความเสี่ยงอย่างน้อยรายไตรมาส โดยความเสี่ยงระดับสูงมากต้องรายงานทันทีเมื่อพบและติดตามอย่างน้อยรายเดือน หรือถี่กว่านั้นตามสถานการณ์และคำสั่งของผู้มีอำนาจ

9. รายงานเหตุสำคัญโดยไม่ชักช้า: รายงานเหตุ Zero Tolerance เหตุวิกฤต และเหตุที่อาจกระทบชีวิต พันธกิจสำคัญ กฎหมาย ข้อมูล ชื่อเสียง หรือผู้มีส่วนได้ส่วนเสียอย่างรุนแรงทันทีตามช่องทางและระยะเวลาที่มหาวิทยาลัยกำหนด โดยไม่รอรอบรายงานปกติ

10. ทบทวนเมื่อมีการเปลี่ยนแปลง: ทบทวนความเสี่ยงเมื่อวัตถุประสงค์ ยุทธศาสตร์ บริบท กฎหมาย โครงสร้าง บุคลากร เทคโนโลยี ระบบงาน ผู้ให้บริการ หรือเหตุการณ์สำคัญเปลี่ยนแปลงอย่างมีนัยสำคัญ

11. จัดเก็บหลักฐานให้ตรวจสอบย้อนกลับได้: จัดเก็บหลักฐานการระบุและประเมินความเสี่ยง การประเมินการควบคุม การอนุมัติ การยอมรับความเสี่ยง การดำเนินมาตรการ และผลการติดตามตามระยะเวลาที่กฎหมายและมหาวิทยาลัยกำหนด

12. ยกระดับและปรับปรุงอย่างต่อเนื่อง: เมื่อ KRI เกิน RT การควบคุมสำคัญไม่ทำงาน มาตรการล่าช้า หรือความเสี่ยงเพิ่มขึ้นอย่างมีนัยสำคัญ ต้องวิเคราะห์สาเหตุ กำหนดการแก้ไข และยกระดับต่อผู้มีอำนาจตามเกณฑ์ที่กำหนด

เกณฑ์ระดับความเสี่ยง มหาวิทยาลัยใช้สูตร

คะแนนความเสี่ยง (Risk Score) = โอกาสเกิด (Likelihood) × ผลกระทบ (Impact)

ตารางที่ 2-5 เกณฑ์ระดับความเสี่ยงและแนวทางดำเนินการขั้นต่ำ

คะแนน	ระดับความเสี่ยง	รหัส	แนวทางดำเนินการขั้นต่ำ
1–4	ต่ำ (Low)	L	ยอมรับและติดตามตามรอบปกติ
5–9	ปานกลาง (Medium)	M	กำหนดมาตรการและติดตามโดยเจ้าของความเสี่ยง
10–15	สูง (High)	H	จัดทำแผนลดความเสี่ยงและรายงานฝ่ายบริหาร
16–25	สูงมาก (Extreme)	E	ยกระดับรายงานทันทีและเร่งดำเนินมาตรการ

เกณฑ์ยกระดับเป็นกรณีพิเศษ

ให้ใช้เกณฑ์ยกระดับเป็นกรณีพิเศษ (Override Criteria) ร่วมกับคะแนนความเสี่ยง ดังนี้

1. ผลกระทบระดับ 5 ให้จัดการอย่างน้อยตามแนวทางของความเสี่ยงระดับสูง แม้คะแนนรวมอยู่ในระดับต่ำกว่า

2. เหตุ Zero Tolerance ให้ยกระดับรายงานและดำเนินการเทียบเท่าความเสี่ยงระดับสูงมากทันที โดยไม่ต้องรอการคำนวณคะแนน ทั้งนี้ การประเมินระดับความเสี่ยงหลังเหตุการณ์ให้ดำเนินการแยกตามกระบวนการปกติ

3. กรณี KRI เกิน RT ความเสี่ยงกระทบหลายส่วนงาน เกินอำนาจยอมรับของส่วนงาน มีการกระจุกตัวสูง หรืออาจกระทบวัตถุประสงค์เชิงยุทธศาสตร์อย่างมีนัยสำคัญ ให้ยกระดับเสนอผู้มีอำนาจพิจารณาว่าควรบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัย (University-level/Enterprise Risk) หรือไม่

4. การยกระดับเป็น Enterprise Risk ไม่เกิดขึ้นโดยอัตโนมัติจากคะแนนหรือ KRI เพียงตัวเดียว แต่ต้องพิจารณาความสำคัญเชิงยุทธศาสตร์ ขอบเขตผลกระทบ ความเร่งด่วน อำนาจจัดการ และการประเมินในภาพรวมมหาวิทยาลัยร่วมกัน

การใช้ Override ต้องบันทึกเหตุผล หลักฐาน ผู้เสนอ ผู้พิจารณา วันที่ตัดสินใจ มาตรการตอบสนอง และกำหนดเวลาทบทวนไว้ในทะเบียนความเสี่ยง

2.14 วัฒนธรรมความเสี่ยงองค์กร

มหาวิทยาลัยส่งเสริมวัฒนธรรมความเสี่ยงองค์กร (Risk Culture) เพื่อให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของพฤติกรรม การปฏิบัติงาน และการตัดสินใจในทุกระดับ โดยมีองค์ประกอบสำคัญ ดังนี้

1. ภาวะผู้นำและพฤติกรรมต้นแบบ (Tone from the Top): ผู้กำกับดูแลและผู้บริหารแสดงความมุ่งมั่น ใช้ข้อมูลความเสี่ยงในการตัดสินใจ สนับสนุนทรัพยากร และรับผิดชอบต่อผลของการตัดสินใจ

2. ความตระหนักด้านความเสี่ยง (Risk Awareness): บุคลากรเข้าใจวัตถุประสงค์ ความเสี่ยงสำคัญ RA/RT สัญญาณเตือน และผลกระทบที่อาจเกิดจากการตัดสินใจหรือการปฏิบัติงานของตน

3. ความเป็นเจ้าของความเสี่ยง (Risk Ownership): เจ้าของความเสี่ยงมีอำนาจ ข้อมูล ทรัพยากร และความรับผิดชอบในการจัดการความเสี่ยงอย่างชัดเจน โดยไม่ผลักภาระให้ผู้ประสานงานความเสี่ยง

4. ความรับผิดชอบต่อการตัดสินใจ (Risk Accountability): ผู้เกี่ยวข้องรับผิดชอบต่อการตัดสินใจ การดำเนินมาตรการ คุณภาพข้อมูล และผลลัพธ์ภายใต้บทบาทและอำนาจของตน

5. การสื่อสารอย่างเปิดเผยและปลอดภัย (Speak-up and Transparency): บุคลากรสามารถรายงานความเสี่ยง สัญญาณเตือน เหตุการณ์ ข้อผิดพลาด หรือข้อกังวลโดยสุจริตได้อย่างปลอดภัย โดยไม่ปกปิดข้อมูลสำคัญ และได้รับความคุ้มครองจากการตอบโต้ตามกฎหมายและระเบียบที่เกี่ยวข้อง

6. การตัดสินใจโดยคำนึงถึงความเสี่ยง (Risk-informed Decision-making): ผู้บริหารใช้ข้อมูลความเสี่ยง โอกาส สมมติฐาน และ RA/RT ประกอบการอนุมัติ ปรับเปลี่ยน ชะลอ หรือยุตินโยบาย แผนงาน โครงการ และการลงทุน

7. การเรียนรู้จากความเสี่ยง (Risk Learning): มหาวิทยาลัยวิเคราะห์สาเหตุราก (Root Cause) เรียนรู้จากเหตุการณ์จริง เหตุการณ์เกือบเกิดความเสียหาย (Near Miss) ข้อร้องเรียน ข้อผิดพลาด และข้อสังเกตจากการตรวจสอบ เพื่อแก้ไขเชิงระบบและป้องกันการเกิดซ้ำ

8. ความรู้และความสามารถ (Risk Competency): ผู้กำกับดูแล ผู้บริหาร เจ้าของความเสี่ยง เจ้าของมาตรการ ผู้ประสานงาน และบุคลากรได้รับการพัฒนาความรู้และทักษะที่เหมาะสมกับบทบาทอย่างต่อเนื่อง

9. การท้าทายอย่างสร้างสรรค์ (Constructive Challenge): หน่วยงานสายงานที่สองและผู้เกี่ยวข้องสามารถตั้งคำถาม ทบทวนสมมติฐาน และเสนอข้อสังเกตต่อการประเมินหรือการตัดสินใจด้านความเสี่ยงอย่างสร้างสรรค์

การประเมินวัฒนธรรมความเสี่ยง

การประเมินวัฒนธรรมความเสี่ยงต้องใช้ข้อมูลจากหลายแหล่งทั้งเชิงปริมาณและเชิงคุณภาพ เช่น

- ผลสำรวจความคิดเห็นหรือการรับรู้ของบุคลากร
- พฤติกรรมและความรวดเร็วในการรายงานเหตุการณ์
- จำนวนเหตุที่รายงาน เหตุที่รายงานล่าช้า และเหตุที่เกิดซ้ำ
- ความตรงเวลาของมาตรการและคุณภาพของหลักฐาน
- คุณภาพและความครบถ้วนของทะเบียนความเสี่ยง
- ผลการประเมินการควบคุมและข้อสังเกตจากการตรวจสอบ
- การใช้ข้อมูลความเสี่ยงในรายงานการประชุมและการตัดสินใจ
- การยกระดับความเสี่ยงเมื่อเกิน RA/RT
- ผลการเรียนรู้และการแก้ไขสาเหตุราก

ไม่ควรประเมินวัฒนธรรมความเสี่ยงจากจำนวนผู้เข้าร่วมการอบรมหรือจำนวนกิจกรรมเพียงอย่างเดียว แต่ต้องพิจารณาการเปลี่ยนแปลงด้านพฤติกรรม คุณภาพการตัดสินใจ ความโปร่งใส และผลลัพธ์จากการบริหารความเสี่ยงร่วมด้วย

ส่วนที่ 3
โครงสร้างการกำกับดูแลและบทบาทหน้าที่ความรับผิดชอบ

3.1 หลักการกำกับดูแลการบริหารความเสี่ยง

มหาวิทยาลัยแม่โจ้กำหนดให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของระบบธรรมาภิบาล การกำหนดยุทธศาสตร์ การบริหารผลการดำเนินงาน การจัดสรรทรัพยากร การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ และการตัดสินใจทุกระดับ โดยมีเป้าหมายเพื่อสร้าง รักษา และเพิ่มคุณค่า ภายใต้ระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้

การกำกับดูแลการบริหารความเสี่ยงยึดหลักสำคัญ ดังนี้

1. การกำกับดูแลโดยสภามหาวิทยาลัย (Governing Body Oversight): สภามหาวิทยาลัยกำหนดทิศทาง อนุมัตินโยบายและกรอบระดับความเสี่ยงที่ยอมรับได้ กำกับฝ่ายบริหาร และได้รับรายงานเกี่ยวกับความเสี่ยง การควบคุม และการให้ความเชื่อมั่นที่ถูกต้อง ครบถ้วน ทันเวลา และเพียงพอต่อการกำกับดูแล

2. ความรับผิดชอบของฝ่ายบริหาร (Management Accountability): อธิการบดีและผู้บริหารรับผิดชอบนำทิศทางและนโยบายไปปฏิบัติ บริหารความเสี่ยงและการควบคุม จัดสรรทรัพยากร และรับผิดชอบต่อผลการดำเนินงานภายในขอบเขตอำนาจหน้าที่

3. ความเป็นเจ้าของความเสี่ยง (Risk Ownership): เจ้าของวัตถุประสงค์ เจ้าของกระบวนการ และเจ้าของความเสี่ยงต้องมีอำนาจ ข้อมูล ทรัพยากร และความรับผิดชอบที่ชัดเจน โดยไม่ผลักภาระการบริหารความเสี่ยงให้หน่วยงานสนับสนุนหรือผู้ประสานงาน

4. การแบ่งบทบาทตามหลัก Three Lines: แยกบทบาทของผู้บริหารและสายงานที่หนึ่งซึ่งเป็นเจ้าของความเสี่ยง ออกจากสายงานที่สองซึ่งสนับสนุน ติดตาม และท้าทายอย่างสร้างสรรค์ และสายงานที่สามซึ่งให้ความเชื่อมั่นอย่างเป็นอิสระ

5. การตัดสินใจภายในขอบเขตอำนาจ (Decision within Delegated Authority): การยอมรับความเสี่ยงต้องอยู่ภายใน RA/RT และอำนาจที่ได้รับมอบหมาย พร้อมมีเหตุผล ข้อมูล หลักฐาน เงื่อนไข และระยะเวลาทบทวนที่ชัดเจน ห้ามยอมรับเหตุ Zero Tolerance หรือความเสี่ยงที่เกินอำนาจโดยไม่ยกระดับรายงาน

6. การพิจารณาความเสี่ยงในภาพรวม (Portfolio View): พิจารณาความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัวของความเสี่ยงในระดับมหาวิทยาลัย ไม่บริหารความเสี่ยงเฉพาะรายส่วนงานหรือแบบแยกส่วน

7. ความโปร่งใสและการยกระดับอย่างทันเวลา (Transparency and Timely Escalation): รายงานข้อมูลความเสี่ยงอย่างถูกต้อง ครบถ้วน และทันเวลา โดยไม่ปกปิด บิดเบือน หรือล่าช้าในการรายงานเหตุการณ์หรือความเสี่ยงที่มีนัยสำคัญ

8. คุณภาพข้อมูลและการตรวจสอบย้อนกลับ (Data Quality and Traceability): ข้อมูลที่ใช้ประเมิน ติดตาม และตัดสินใจด้านความเสี่ยงต้องมีแหล่งข้อมูล เจ้าของข้อมูล นิยาม วิธีคำนวณ และหลักฐานที่สามารถตรวจสอบย้อนกลับได้

9. การประสานการให้ความเชื่อมั่น (Coordinated Assurance): ประสานงานระหว่างฝ่ายบริหาร สายงานที่สอง กองตรวจสอบภายใน และผู้ให้ความเชื่อมั่นภายนอก เพื่อลดความซ้ำซ้อน ปิดช่องว่าง และเพิ่มความครอบคลุมของการให้ความเชื่อมั่น

10. การทบทวนและปรับปรุงอย่างต่อเนื่อง (Continual Improvement): ใช้ผลการติดตาม เหตุการณ์จริง ข้อร้องเรียน ข้อสังเกตจากการตรวจสอบ การทดสอบแผน และบทเรียนมาปรับปรุงระบบบริหารความเสี่ยงอย่างต่อเนื่อง

3.2 โครงสร้างการกำกับดูแลการบริหารความเสี่ยง

มหาวิทยาลัยกำหนดโครงสร้างการกำกับดูแล การบริหาร การปฏิบัติ และการให้ความเชื่อมั่นตามหลัก Three Lines โดยแบ่งบทบาทที่เชื่อมโยงกัน ดังนี้

ตารางที่ 3-1 กลุ่มบทบาท องค์ประกอบ และหน้าที่หลักในการกำกับดูแลความเสี่ยง

กลุ่มบทบาท	องค์ประกอบ	หน้าที่หลัก
ผู้กำกับดูแล (Governing Body)	สภามหาวิทยาลัย คณะกรรมการตรวจสอบประจำมหาวิทยาลัย และคณะกรรมการที่สภามหาวิทยาลัยแต่งตั้งหรือมอบหมายให้กำกับด้านความเสี่ยง	กำหนดทิศทาง อนุมัตินโยบายและกรอบ RA/RT กำกับฝ่ายบริหาร และรับรายงานด้านความเสี่ยง การควบคุม และการให้ความเชื่อมั่น
ฝ่ายบริหารระดับมหาวิทยาลัย (University Management)	อธิการบดี คณะกรรมการบริหารมหาวิทยาลัย คณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน และผู้บริหารระดับมหาวิทยาลัย	นำนโยบายไปปฏิบัติ บริหารภาพรวมความเสี่ยง จัดลำดับความสำคัญ จัดสรรทรัพยากร ตัดสินใจภายในอำนาจ และรายงานต่อผู้กำกับดูแล
สายงานที่หนึ่ง (First Line)	ผู้บริหารส่วนงาน เจ้าของวัตถุประสงค์ เจ้าของกระบวนการ เจ้าของความเสี่ยง เจ้าของการควบคุม เจ้าของมาตรการ และเจ้าของข้อมูล	ระบุ ประเมิน ตอบสนอง ควบคุม ติดตาม และรายงานความเสี่ยงในงานที่รับผิดชอบ รวมทั้งดำเนินมาตรการและจัดเก็บหลักฐาน
สายงานที่สอง (Second Line)	หน่วยงานบริหารความเสี่ยงและการควบคุมภายใน ฝ่ายกฎหมายและ Compliance หน่วยงานด้านไซเบอร์และ PDPA ความปลอดภัย BCM/BCP และหน้าที่กำกับเฉพาะด้าน	จัดทำกรอบ มาตรฐาน เกณฑ์ เครื่องมือ และข้อมูล ให้คำปรึกษา ประสานงาน ติดตาม และท้าทายอย่างสร้างสรรค์ โดยไม่บริหารความเสี่ยงแทนสายงานที่หนึ่ง
สายงานที่สาม (Third Line)	กองตรวจสอบภายใน	ให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรมต่อความเพียงพอและประสิทธิผลของการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายใน

กลุ่มบทบาท	องค์ประกอบ	หน้าที่หลัก
ผู้ให้ความเชื่อมั่นอื่นและภายนอก (Other and External Assurance Providers)	ผู้สอบบัญชี ผู้ประเมินภายนอก หน่วยรับรอง ผู้เชี่ยวชาญ และหน่วยงานกำกับดูแล	ให้ความเชื่อมั่นหรือผลการประเมินตามขอบเขต อำนาจหน้าที่ ความเชี่ยวชาญ และระดับความเป็นอิสระของแต่ละหน่วยงาน

หลักการสำคัญในการใช้โครงสร้าง

1. คณะกรรมการที่อยู่ในชั้นผู้กำกับดูแลต้องได้รับการแต่งตั้งหรือมอบหมายจากสภามหาวิทยาลัยและมีสายการรายงานต่อสภามหาวิทยาลัยอย่างชัดเจน

2. คณะกรรมการฝ่ายบริหารทำหน้าที่อำนวยการ กลั่นกรอง ติดตาม และตัดสินใจภายในอำนาจของฝ่ายบริหาร มิใช่ผู้ให้ความเชื่อมั่นอย่างเป็นอิสระ

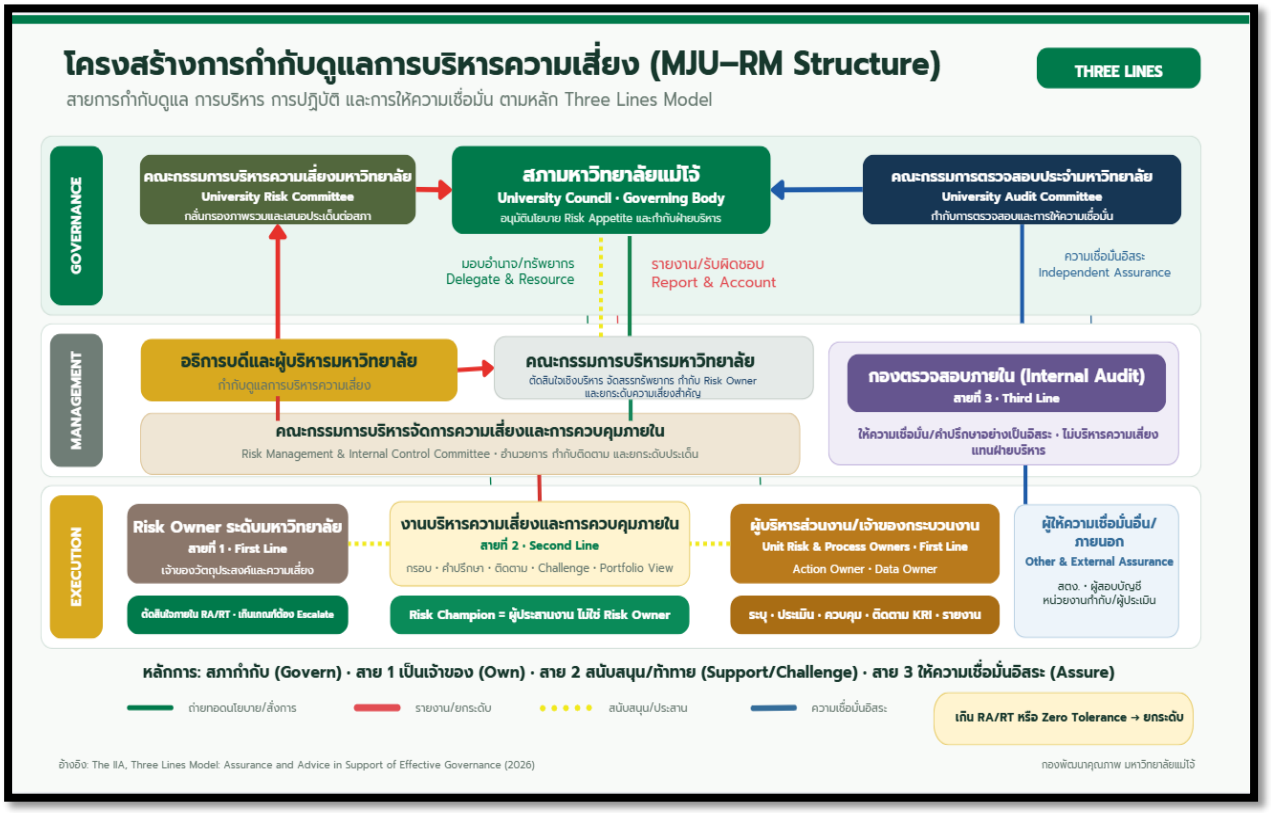
3. สายงานที่หนึ่งเป็นเจ้าของวัตถุประสงค์ ความเสี่ยง การควบคุม และผลการดำเนินงาน

4. สายงานที่สองสนับสนุน ให้คำปรึกษา ติดตาม และท้าทายอย่างสร้างสรรค์ แต่ไม่รับผิดชอบแทนเจ้าของความเสี่ยง

5. กองตรวจสอบภายในต้องไม่ถูกรวมเป็นหน่วยปฏิบัติการ เจ้าของความเสี่ยง หรือผู้บริหารมาตรการควบคุม เนื่องจากต้องรักษาความเป็นอิสระและความเที่ยงธรรมในการประเมินการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายใน

6. ผู้ให้ความเชื่อมั่นภายนอกไม่ถือเป็นสายงานที่สามของมหาวิทยาลัย แต่เป็นแหล่งความเชื่อมั่นเพิ่มเติมที่ควรนำมาประสานใน Assurance Map

ภาพที่ 3-1 *โครงสร้างการกำกับดูแลการบริหารความเสี่ยง มหาวิทยาลัยแม่โจ้ (MJU–RM Structure)*



ที่มา: มหาวิทยาลัยแม่โจ้ ประยุกต์จาก *The IIA's Three Lines Model: Assurance and Advice in Support of Effective Governance (2026)*

3.3 บทบาท หน้าที่ และความรับผิดชอบ

บทบาท หน้าที่ อำนาจตัดสินใจ และสายการรายงานด้านการบริหารความเสี่ยงให้เป็นไปตามกฎหมาย ข้อบังคับ กฎบัตร คำสั่งแต่งตั้ง และการมอบอำนาจที่มีผลใช้บังคับ โดยมีหลักสำคัญว่า ฝ่ายบริหารและส่วนงานเป็นเจ้าของความเสี่ยง สายงานที่สองทำหน้าที่สนับสนุนและท้าทายอย่างสร้างสรรค์ และสายงานที่สามให้ความเชื่อมั่นอย่างเป็นอิสระ

3.3.1 สภามหาวิทยาลัย

1. อนุมัติถ้อยแถลงการกำกับดูแลความเสี่ยง นโยบายการบริหารความเสี่ยง และกรอบระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้ (Risk Appetite Framework)

2. กำกับให้ฝ่ายบริหารจัดให้มีระบบบริหารความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ และการบริหารความต่อเนื่องที่เหมาะสมและมีประสิทธิผล

3. กำกับติดตามความเสี่ยงเชิงยุทธศาสตร์ ความเสี่ยงระดับสูงมาก เหตุ Zero Tolerance และความเสี่ยงที่อยู่นอกกรอบ Risk Appetite หรือเกินอำนาจยอมรับของฝ่ายบริหาร

4. พิจารณาภาพรวมความเสี่ยงของมหาวิทยาลัย (Risk Portfolio) แนวโน้ม KRI ความสัมพันธ์และการกระจุกตัวของความเสี่ยง รวมทั้งประเด็นที่ต้องใช้อำนาจหรือทรัพยากรระดับสภามหาวิทยาลัย

5. รับรายงานเกี่ยวกับความเสี่ยง การควบคุม และการให้ความเชื่อมั่นจากคณะกรรมการตรวจสอบ คณะกรรมการที่เกี่ยวข้อง กองตรวจสอบภายใน หรือผู้ให้ความเชื่อมั่นอื่น ตามสายการรายงานที่กำหนด

6. กำกับวัฒนธรรมองค์กร ธรรมาภิบาล ความโปร่งใส ความรับผิดชอบ และการเปิดเผยข้อมูลอย่างเหมาะสม

7. ทบทวนความเพียงพอของการกำกับดูแลความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อบริบทเปลี่ยนแปลงอย่างมีนัยสำคัญ

3.3.2 คณะกรรมการตรวจสอบประจำมหาวิทยาลัย

1. กำกับดูแลความเป็นอิสระ ความเที่ยงธรรม ทรัพยากร ขอบเขต แผนงาน และผลการปฏิบัติงานของกองตรวจสอบภายในตามกฎบัตรที่มีผลใช้บังคับ

2. สอบทานความเพียงพอและความน่าเชื่อถือของข้อมูลด้านความเสี่ยง การควบคุมภายใน การกำกับดูแล และการให้ความเชื่อมั่นที่เสนอต่อสภามหาวิทยาลัย

3. พิจารณาข้อค้นพบและข้อบกพร่องที่มีนัยสำคัญ เหตุทุจริต การไม่ปฏิบัติตามกฎหมาย และความก้าวหน้าในการแก้ไขของฝ่ายบริหาร

4. ติดตามกรณีที่ฝ่ายบริหารยอมรับความเสี่ยงในระดับที่อาจไม่เหมาะสม หรือไม่ดำเนินการแก้ไขข้อบกพร่องที่มีนัยสำคัญภายในระยะเวลาที่กำหนด

5. ประสานกับผู้สอบบัญชี ผู้ประเมินภายนอก หน่วยงานกำกับดูแล และผู้ให้ความเชื่อมั่นอื่นตามความเหมาะสม

6. รายงานข้อสังเกต ข้อเสนอแนะ และประเด็นสำคัญต่อสภามหาวิทยาลัย

คณะกรรมการตรวจสอบไม่บริหารความเสี่ยงหรือเลือกมาตรการควบคุมแทนฝ่ายบริหาร

3.3.3 คณะกรรมการบริหารความเสี่ยงมหาวิทยาลัย

1. กลั่นกรองและเสนอแนะนโยบาย กรอบ RA/RT และการเปลี่ยนแปลงสาระสำคัญต่อสภามหาวิทยาลัย

2. พิจารณาภาพรวมความเสี่ยงระดับมหาวิทยาลัย ความเชื่อมโยง การกระจุกตัว แนวโน้ม และความเพียงพอของมาตรการตอบสนอง

3. ติดตามความเสี่ยงที่เกิน RA/RT ความเสี่ยงระดับสูงและสูงมาก เหตุ Zero Tolerance ความเสี่ยงเกิดใหม่ และประเด็นที่กระทบหลายส่วนงาน

4. ท้าทายสมมติฐาน คุณภาพข้อมูล การประเมินความเสี่ยง KRI ระดับความเสี่ยงคงเหลือเป้าหมาย และความเพียงพอของทรัพยากรอย่างสร้างสรรค์

5. เสนอประเด็นที่ต้องการการตัดสินใจ การจัดสรรทรัพยากร หรือการกำกับเพิ่มเติมต่ออธิการบดีหรือสภามหาวิทยาลัยตามสายการรายงาน

6. รายงานต่อสภามหาวิทยาลัยตามรอบที่กำหนด และรายงานโดยไม่ชักช้าเมื่อเกิดเหตุการณ์สำคัญ

องค์ประกอบ อำนาจ วาระการดำรงตำแหน่ง การประชุม องค์ประชุม และสายการรายงาน ให้เป็นไปตามกฎบัตรหรือคำสั่งแต่งตั้งที่มีผลใช้บังคับ

3.3.4 อธิการบดีและคณะผู้บริหาร

1. นำนโยบายและกรอบ RA/RT ไปสู่การปฏิบัติทั่วทั้งมหาวิทยาลัย
2. กำหนดเจ้าของวัตถุประสงค์ เจ้าของความเสี่ยง เจ้าของการควบคุม เจ้าของมาตรการ และเจ้าของข้อมูล
3. อนุมัติภาพรวมความเสี่ยง แผนบริหารความเสี่ยง และการจัดสรรทรัพยากรภายในขอบเขตอำนาจ
4. ตัดสินใจหลีกเลี่ยง ลดหรือควบคุม แบ่งปันหรือถ่ายโอน ยอมรับความเสี่ยง หรือใช้ประโยชน์จากโอกาสภายในอำนาจที่ได้รับมอบหมาย
5. กำกับให้เหตุการณ์สำคัญได้รับการระงับ ควบคุม แก้ไข เยียวยา ฟื้นฟู สื่อสาร และรายงานอย่างทันเวลา
6. ทบทวน KPI, KRI สถานะ RA/RT ผลการประเมินการควบคุม และระดับความเสี่ยงคงเหลือเป้าหมายเพื่อสั่งการหรือปรับการจัดสรรทรัพยากร
7. รายงานต่อคณะกรรมการบริหารความเสี่ยงและสภามหาวิทยาลัยตามเกณฑ์และสายการรายงานที่กำหนด
8. ส่งเสริมวัฒนธรรมที่กล้ารายงาน ไม่ปกปิดข้อมูล ท้าทายอย่างสร้างสรรค์ และเรียนรู้จากเหตุการณ์

3.3.5 คณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน

1. ขับเคลื่อนนโยบาย กรอบ และแผนงานที่ฝ่ายบริหารอนุมัติ
2. กลั่นกรองทะเบียนความเสี่ยง ภาพรวมความเสี่ยง KRI ผลการประเมินการควบคุม และรายงานผลก่อนเสนอฝ่ายบริหาร
3. ติดตามมาตรการที่ล่าช้า ความเสี่ยงที่เกิน RT และข้อบกพร่องของการควบคุมที่มีนัยสำคัญ
4. ประสานการบริหารความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ BCM/BCP และการรายงานที่เกี่ยวข้อง
5. พิจารณาความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัวของความเสี่ยงในภาพมหาวิทยาลัย
6. เสนอการยกระดับ ประเด็นตัดสินใจ การจัดสรรทรัพยากร และแนวทางแก้ไขต่ออธิการบดีหรือคณะผู้บริหาร

คณะกรรมการชุดนี้เป็นกลไกของฝ่ายบริหาร มิใช่ผู้ให้ความเชื่อมั่นอย่างเป็นอิสระ

3.3.6 ผู้บริหารส่วนงาน เจ้าของวัตถุประสงค์ และเจ้าของความเสี่ยง

1. กำหนดวัตถุประสงค์ บริบท ตัวชี้วัด และผลลัพธ์ที่ต้องการบรรลุ
2. ระบุความเสี่ยงด้วยโครงสร้าง Cause–Event–Impact และจัดทำทะเบียนความเสี่ยง
3. ประเมิน Inherent Risk การควบคุมที่มีอยู่ และ Residual Risk โดยใช้ข้อมูลและหลักฐานที่เพียงพอ

4. กำหนด KRI พร้อมนิยาม สูตร แหล่งข้อมูล เจ้าของข้อมูล ความถี่ RA/RT และ Trigger/Action

5. เลือกการตอบสนอง จัดทำ Risk Treatment Plan และกำหนด Target Residual Risk

6. กำกับการดำเนินการควบคุมและมาตรการเพิ่มเติมให้แล้วเสร็จและเกิดผลตามกำหนด

7. ยอมรับความเสี่ยงเฉพาะภายในอำนาจและกรอบ RA/RT พร้อมบันทึกเหตุผล หลักฐาน เงื่อนไข และระยะเวลาทบทวน

8. รายงานเหตุการณ์และยกระดับความเสี่ยงโดยไม่รอรอบปกติเมื่อเข้าเกณฑ์

9. ทบทวนความเสี่ยงเมื่อวัตถุประสงค์ บริบท กฎหมาย ระบบงาน การควบคุม หรือเหตุการณ์เปลี่ยนแปลงอย่างมีนัยสำคัญ

10.รับผิดชอบต่อคุณภาพและความครบถ้วนของข้อมูลความเสี่ยงในขอบเขตที่ตนกำกับ

ผู้บริหารส่วนงานยังคงรับผิดชอบต่อภาพรวมความเสี่ยงของส่วนงาน แม้จะมอบหมายบุคคลอื่นเป็น Risk Owner หรือ Action Owner

3.3.7 เจ้าของการควบคุม เจ้าของมาตรการ เจ้าของข้อมูล และผู้ประสานงาน

เจ้าของการควบคุม (Control Owner)

- ดำเนินการควบคุมตามรูปแบบและความถี่ที่กำหนด
- ประเมินและจัดเก็บหลักฐานว่าการควบคุมทำงานจริง
- รายงานข้อยกเว้นหรือการควบคุมที่ไม่ทำงานต่อ Risk Owner

เจ้าของมาตรการ (Action Owner)

- ดำเนินมาตรการตามขอบเขต ระยะเวลา และทรัพยากรที่ได้รับอนุมัติ
- รายงานความก้าวหน้า ปัญหา ผลส่งมอบ และหลักฐาน
- แจ้ง Risk Owner ทันทีเมื่อมาตรการมีแนวโน้มล่าช้าหรือไม่บรรลุผล

เจ้าของข้อมูล (Data Owner)

- กำหนดและดูแลนิยาม สูตร แหล่งข้อมูล และวิธีรวบรวมข้อมูล
- รับผิดชอบความถูกต้อง ครบถ้วน ทันเวลา ความมั่นคงปลอดภัย และการตรวจสอบย้อนกลับของข้อมูล
- แจ้งข้อจำกัดหรือความผิดปกติของข้อมูลที่อาจกระทบการตัดสินใจ

ผู้ประสานงานความเสี่ยง (Risk Coordinator/Risk Champion)

- ประสานการจัดทำทะเบียนความเสี่ยง แผนมาตรการ การติดตาม และการรายงาน
- ให้คำแนะนำเบื้องต้นเกี่ยวกับแบบฟอร์ม เกณฑ์ และปฏิทินดำเนินงาน
- รวบรวมข้อมูลและติดตามความครบถ้วนของหลักฐาน

ผู้ประสานงานความเสี่ยงไม่ใช่ Risk Owner และไม่ยอมรับหรือบริหารความเสี่ยงแทนผู้บริหาร

3.3.8 หน่วยงานด้านการบริหารความเสี่ยงและการควบคุมภายใน

1. พัฒนากรอบ คู่มือ เกณฑ์ เครื่องมือ แบบฟอร์ม ระบบข้อมูล และปฏิทินการดำเนินงาน
2. ให้คำปรึกษา อำนวยความสะดวก และท้าทายคุณภาพการประเมินอย่างสร้างสรรค์
3. สอบทานความครบถ้วนและความสอดคล้องของ Risk Register, RA/RT, KRI และแผนมาตรการ โดยไม่รับรองความถูกต้องแทนเจ้าของข้อมูลหรือ Risk Owner
4. รวบรวม วิเคราะห์ และจัดทำ Portfolio View, Dashboard และรายงานเพื่อสนับสนุนการตัดสินใจ
5. ติดตามเกณฑ์ Escalation มาตรการล่าช้า สถานะ RA/RT และคุณภาพข้อมูล พร้อมเสนอการยกระดับ
6. พัฒนาความสามารถ วัฒนธรรมความเสี่ยง และระดับการพัฒนาระบบบริหารความเสี่ยงอย่างต่อเนื่อง
7. ประสานกับกองแผนงาน กองคลัง ฝ่ายกฎหมาย กองเทคโนโลยีดิจิทัล หน่วยงาน BCM/ความปลอดภัย และหน้าที่กำกับเฉพาะด้าน

หน่วยงานด้านความเสี่ยงไม่เป็นเจ้าของความเสี่ยง ไม่เลือกหรือดำเนินมาตรการแทน Risk Owner และไม่ยอมรับความเสี่ยงแทนผู้มีอำนาจ

3.3.9 หน่วยงานกำกับเฉพาะด้านในสายงานที่สอง

หน่วยงานด้านกฎหมายและ Compliance ไซเบอร์และ PDPA การเงิน ความปลอดภัย BCM/BCP คุณภาพ สิ่งแวดล้อม และหน้าที่กำกับเฉพาะด้าน มีหน้าที่

1. กำหนดมาตรฐาน แนวปฏิบัติ และเกณฑ์เฉพาะด้านตามอำนาจหน้าที่
2. ให้คำปรึกษาและสนับสนุนส่วนงานในการปฏิบัติตามข้อกำหนด
3. ติดตาม วิเคราะห์ และท้าทายความเพียงพอของการบริหารความเสี่ยงเฉพาะด้าน
4. รายงานหรือยกระดับข้อบกพร่องและความเสี่ยงที่มีนัยสำคัญตามเส้นทางที่กำหนด
5. ประสานข้อมูลกับหน่วยงานบริหารความเสี่ยงและกองตรวจสอบภายใน โดยไม่รับผิดชอบแทนสายงานที่หนึ่ง

3.3.10 กองตรวจสอบภายใน

1. ให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรมต่อการกำกับดูแล การบริหารความเสี่ยงและการควบคุมภายใน
2. จัดทำแผนตรวจสอบตามฐานความเสี่ยง โดยใช้ข้อมูลของฝ่ายบริหารร่วมกับการประเมินความเสี่ยงอย่างเป็นอิสระของกองตรวจสอบภายใน
3. ประเมินความเหมาะสมของการออกแบบ การนำไปใช้ และประสิทธิผลในการปฏิบัติงานของการควบคุมตามขอบเขตการตรวจสอบ

4. รายงานข้อค้นพบ สาเหตุ ผลกระทบ ระดับความสำคัญ และข้อเสนอแนะต่อฝ่ายบริหารและคณะกรรมการตรวจสอบ

5. ติดตามสถานะการดำเนินการตามข้อเสนอแนะ โดยไม่รับผิดชอบแทนฝ่ายบริหารในการแก้ไข

6. ประสานกับผู้ให้ความเชื่อมั่นอื่นเพื่อเพิ่มความครอบคลุมและลดความซ้ำซ้อน

กองตรวจสอบภายในไม่กำหนด RA/RT ไม่เป็นเจ้าของทะเบียนความเสี่ยง ไม่ตัดสินใจยอมรับความเสี่ยง และไม่เลือกหรือดำเนินมาตรการควบคุมที่ตนต้องตรวจสอบ

หากได้รับมอบหมายบทบาทอื่นที่อาจกระทบต่อความเป็นอิสระ ต้องได้รับอนุมัติจากผู้กำกับดูแล กำหนดขอบเขตและระยะเวลา เปิดเผยผลกระทบ และจัดให้มีมาตรการคุ้มครอง รวมทั้งผู้ให้ความเชื่อมั่นที่เป็นอิสระในเรื่องนั้นตามความเหมาะสม

3.3.11 บุคลากรทุกคน

1. เข้าใจวัตถุประสงค์ ความเสี่ยง และการควบคุมที่เกี่ยวข้องกับงานของตน
2. ปฏิบัติตามกฎหมาย นโยบาย ขั้นตอน และมาตรการควบคุมที่กำหนด
3. รายงานเหตุผิดปกติ สัญญาณเตือน เหตุการณ์เกือบเกิดความเสียหาย (Near Miss) ข้อผิดพลาด หรือการควบคุมที่ไม่ทำงานโดยสุจริตและทันเวลา
4. ให้ข้อมูลที่ถูกต้อง ครบถ้วน และร่วมดำเนินมาตรการตามบทบาทที่ได้รับมอบหมาย
5. รักษาข้อมูลและหลักฐานที่เกี่ยวข้อง และไม่ปกปิด บิดเบือน หรือทำลายข้อมูลสำคัญ
6. เรียนรู้จากเหตุการณ์และพัฒนาความรู้ความสามารถตามบทบาทอย่างต่อเนื่อง

3.4 การกำกับดูแลตามหลัก Three Lines

มหาวิทยาลัยประยุกต์ใช้หลัก Three Lines เพื่อกำหนดความสัมพันธ์ระหว่างการกำกับดูแล การบริหาร การปฏิบัติ การสนับสนุนกำกับ และการให้ความเชื่อมั่น โดยแต่ละบทบาทต้องประสานงานและแลกเปลี่ยนข้อมูลกันอย่างเหมาะสม โดยไม่ทำให้ความรับผิดชอบ ความเป็นเจ้าของความเสี่ยง หรือความเป็นอิสระคลุมเครือ

ตารางที่ 3-2 *บทบาท ผู้เกี่ยวข้อง ความรับผิดชอบหลัก และขอบเขตที่ต้องระวัง*

บทบาท	ผู้เกี่ยวข้อง	ความรับผิดชอบหลัก	ขอบเขตที่ต้องระวัง
ผู้กำกับดูแล (Governing Body)	สภามหาวิทยาลัยและคณะกรรมการของสภาตามที่ได้รับมอบหมาย	กำหนดทิศทาง อนุมัตินโยบายและกรอบ RA/RT กำกับฝ่ายบริหาร และรับรายงานด้านความเสี่ยง การควบคุม และการให้ความเชื่อมั่น	ไม่บริหารงานประจำ ไม่เป็นเจ้าของความเสี่ยงหรือการควบคุม และไม่ตัดสินใจแทนฝ่ายบริหารในเรื่องที่ได้มอบอำนาจแล้ว
สายงานที่หนึ่ง (First Line)	อธิการบดี ฝ่ายบริหาร ผู้บริหารส่วนงาน เจ้าของวัตถุประสงค์	บริหารความเสี่ยงและโอกาสออกแบบและดำเนินการควบคุม	ไม่ผลักภาระความเป็นเจ้าของความเสี่ยงให้หน่วยงานบริหาร

บทบาท	ผู้เกี่ยวข้อง	ความรับผิดชอบหลัก	ขอบเขตที่ต้องระวัง
	เจ้าของกระบวนการ เจ้าของความเสี่ยง เจ้าของการควบคุม เจ้าของมาตรการ และเจ้าของข้อมูล	ตัดสินใจ ดำเนินมาตรการ ติดตาม รายงาน และรับผิดชอบต่อผลลัพธ์	ความเสี่ยง ผู้ประสานงาน หรือกองตรวจสอบภายใน
สายงานที่สอง (Second Line)	หน่วยงานบริหารความเสี่ยงและการควบคุมภายใน กฎหมายและ Compliance ไซเบอร์และ PDPA ความปลอดภัย BCM/BCP คุณภาพ การเงิน และหน้าที่กำกับเฉพาะด้าน	กำหนดกรอบ มาตรฐาน เกณฑ์ และเครื่องมือ ให้คำปรึกษา สนับสนุน ติดตาม วิเคราะห์ ท้าทายอย่างสร้างสรรค์ และรายงานภาพรวม	ไม่บริหารความเสี่ยงหรือดำเนินมาตรการแทน Risk Owner และไม่ให้ความเชื่อมั่นอย่างเป็นอิสระในงานที่ตนออกแบบหรือรับผิดชอบ
สายงานที่สาม (Third Line)	กองตรวจสอบภายใน	ให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรม เกี่ยวกับการกำกับดูแล การบริหารความเสี่ยง และการควบคุม	ไม่กำหนด RA/RT ไม่เป็นเจ้าของความเสี่ยงหรือทะเบียนความเสี่ยง และไม่เลือก ยอมรับ หรือดำเนินมาตรการแทนฝ่ายบริหาร
ผู้ให้ความเชื่อมั่นอื่น (Other Assurance Providers)	ผู้สอบบัญชี ผู้ประเมินภายนอก หน่วยรับรอง ผู้เชี่ยวชาญ และหน่วยงานกำกับดูแล	ให้ความเชื่อมั่นหรือผลการประเมินตามขอบเขต อำนาจหน้าที่ และความเชี่ยวชาญ	ต้องระบุขอบเขต หลักฐาน ข้อจำกัด และระดับความเป็นอิสระให้ชัดเจน และไม่ถือเป็นสายงานที่สามของมหาวิทยาลัย

การทำงานร่วมกันตาม Three Lines ต้องอาศัยการสื่อสาร การประสานงาน และการแลกเปลี่ยนข้อมูลอย่างเหมาะสม โดยยึดหลักว่า **สภามหาวิทยาลัยกำกับ — ฝ่ายบริหารและสายงานที่หนึ่งเป็นเจ้าของ — สายงานที่สองสนับสนุนและท้าทาย — สายงานที่สามให้ความเชื่อมั่นอย่างเป็นอิสระ**

3.5 ตารางบทบาทและความรับผิดชอบด้านการบริหารความเสี่ยง *(Risk Management RACI Matrix)*

- **A – Accountable:** ผู้รับผิดชอบสูงสุดต่อผลลัพธ์และมีอำนาจอนุมัติ
- **R – Responsible:** ผู้ดำเนินการหลักหรือจัดทำผลผลิต
- **C – Consulted:** ผู้ให้คำปรึกษา ให้ข้อมูล หรือร่วมพิจารณา
- **I – Informed:** ผู้ที่ต้องได้รับทราบข้อมูลหรือผลการตัดสินใจ

หลักการสำคัญคือ กิจกรรมหนึ่งควรมี **A เพียงหนึ่งบทบาทในแต่ละระดับการตัดสินใจ** ส่วนกิจกรรมที่อำนาจเปลี่ยนไปตามระดับความเสี่ยง ให้ใช้เครื่องหมาย **A*** และอ้างอิงตารางอำนาจยอมรับและยกระดับความเสี่ยง

ตารางที่ 3-3 ตารางบทบาทและความรับผิดชอบด้านการบริหารความเสี่ยง (Risk Management RACI Matrix)

กิจกรรม	สภา	คกก. ตรวจสอบ	คกก.บริหารความเสี่ยง	อธิการบดี/ฝ่ายบริหาร	หน่วยบริหารความเสี่ยง	ผู้บริหารส่วนงาน	Risk/Action/ Data Owner	ตรวจสอบภายใน
1. อนุมัตินโยบายและกรอบ Risk Appetite	A	C	R	C	C	I	I	I
2. จัดทำข้อเสนอ RA/RT และเกณฑ์กลาง	I	I	C	A	R	C	C	I
3. จัดทำและเสนอภาพรวมความเสี่ยงระดับมหาวิทยาลัย	I	I	C	A	R	C	R	I
4. ระบุ ประเมิน และจัดทำ Risk Register ของส่วนงาน	I	I	I	I	C	A	R	I
5. ออกแบบและดำเนินการควบคุมหรือมาตรการ	I	I	I	I/C	C	A	R	I
6. กำหนด KRI และรับรองคุณภาพข้อมูล	I	I	I	C	C	A	R	I
7. รวบรวม วิเคราะห์ และรายงาน Portfolio View	I	I	C	A	R	C	R	I
8. ยอมรับความเสี่ยงภายในอำนาจ	A*	I	C	A*	C	A*	R	I
9. ระงับเหตุและจัดการเหตุการณ์หรือภาวะวิกฤต	I	I	I/C	A*	C	A*	R	I
10. ให้ความเชื่อมั่นอย่างเป็นอิสระ	I	A	I	C	C	C	C	R

กิจกรรม	สภา	คกก. ตรวจสอบ	คกก.บริหารความเสี่ยง	อธิการบดี/ฝ่ายบริหาร	หน่วยบริหารความเสี่ยง	ผู้บริหารส่วนงาน	Risk/Action/ Data Owner	ตรวจสอบภายใน
ต่อระบบ ERM และการควบคุม								
11. ดำเนินการแก้ไขข้อสังเกตจากการตรวจสอบ	I	C	I	A*	I/C	A*	**R**	I
12. ติดตามและรายงานสถานะการแก้ไขอย่างเป็นอิสระ	I	**A**	I	C	I	C	C	**R**
13. ทบทวนนโยบายและกรอบ Risk Appetite	**A**	C	R	C/R	**R**	C	C	I/C
14. ทบทวนคู่มือกระบวนการและระดับการพัฒนาระบบ	I	C	C	**A**	**R**	C	C	I/C

หมายเหตุประกอบ RACI

1. **A*** หมายถึง ผู้มีอำนาจรับผิดชอบสูงสุดแตกต่างกันตามระดับความเสี่ยง ขอบเขตผลกระทบ และวงเงิน หรืออำนาจที่ได้รับมอบหมาย โดยในแต่ละกรณีต้องมี A เพียงหนึ่งราย

2. การยอมรับความเสี่ยงต้องอ้างอิงตารางอำนาจยอมรับและยกระดับความเสี่ยง (Risk Acceptance and Escalation Authority Matrix) และต้องไม่เกิน RA/RT หรือข้อจำกัดตามกฎหมาย

3. Risk Owner เป็นผู้รับผิดชอบดำเนินการหลัก แต่ผู้บริหารส่วนงานยังคงเป็นผู้รับผิดชอบสูงสุดต่อความเสี่ยงและผลการดำเนินงานของส่วนงาน

4. Data Owner รับผิดชอบคุณภาพของข้อมูล KRI ส่วน Risk Owner รับผิดชอบการตีความข้อมูลและการตัดสินใจตอบสนองต่อความเสี่ยง

5. หน่วยบริหารความเสี่ยงรวบรวม วิเคราะห์ และท้าทายคุณภาพข้อมูล แต่ไม่รับรองความถูกต้องแทน Risk Owner หรือ Data Owner

6. กองตรวจสอบภายในติดตามและรายงานสถานะการแก้ไขอย่างเป็นอิสระ แต่ฝ่ายบริหาร ผู้บริหารส่วนงาน และเจ้าของมาตรการเป็นผู้รับผิดชอบต่อการแก้ไขข้อสังเกต

7. คณะกรรมการบริหารความเสี่ยงจะมีสถานะ R หรือ C ตามอำนาจในกฎบัตร หากเป็นคณะกรรมการฝ่ายบริหารต้องไม่กำหนดให้รับผิดชอบต่อสภามหาวิทยาลัยโดยตรง เว้นแต่คำสั่งแต่งตั้งกำหนดไว้

8. ตารางนี้เป็นกรอบกลาง ต้องทบทวนให้ตรงกับกฎหมาย ข้อบังคับ กฎบัตร คำสั่งแต่งตั้ง และการมอบอำนาจที่มีผลใช้บังคับ หากขัดหรือแย้งกัน ให้ยึดเอกสารให้อำนาจและปรับปรุง RACI ให้สอดคล้องโดยไม่ชักช้า

3.6 สายการรายงานและการยกระดับความเสี่ยง

มหาวิทยาลัยกำหนดสายการรายงานและการยกระดับความเสี่ยงให้สอดคล้องกับระดับความรุนแรง ความเร่งด่วน ขอบเขตผลกระทบ และอำนาจตัดสินใจ โดยแยกเป็น 2 ลักษณะ ได้แก่

1. **การรายงานความเสี่ยงตามรอบ (Periodic Risk Reporting):** ใช้สำหรับการติดตามระดับความเสี่ยง KRI ประสิทธิผลของการควบคุม ความก้าวหน้าของมาตรการ และแนวโน้มตามรอบที่กำหนด
2. **การรายงานเหตุการณ์หรือภาวะวิกฤต (Incident/Crisis Escalation):** ใช้เมื่อเกิดเหตุจริง เหตุ Zero Tolerance หรือสถานการณ์ที่ต้องมีการตัดสินใจและระงับเหตุโดยทันที โดยไม่ต้องรอรอบรายงานปกติ

3.6.1 สายการรายงานหลัก

1. **ระดับส่วนงาน:**
   ผู้พบเหตุหรือเจ้าของข้อมูล ⟶ ผู้บังคับบัญชาหรือเจ้าของความเสี่ยง ⟶ หัวหน้าส่วนงาน
2. **ระดับมหาวิทยาลัย:**
   หัวหน้าส่วนงานหรือ Risk Owner ⟶ หน่วยบริหารความเสี่ยง ⟶ อธิการบดีหรือคณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน
3. **ระดับผู้กำกับดูแล:**
   อธิการบดีหรือคณะกรรมการบริหารความเสี่ยงมหาวิทยาลัย ⟶ สภามหาวิทยาลัยหรือคณะกรรมการของสภาที่เกี่ยวข้อง ตามระดับความรุนแรงและอำนาจตัดสินใจ
4. **สายการตรวจสอบที่เป็นอิสระ:**
   ผู้อำนวยการกองตรวจสอบภายใน ⟶ คณะกรรมการตรวจสอบประจำมหาวิทยาลัย ⟶ สภามหาวิทยาลัย โดยเป็นอิสระจากสายการบริหารความเสี่ยงของฝ่ายบริหาร
5. **สายการรายงานเฉพาะด้าน:**
   ให้รายงานต่อหน่วยงานหรือผู้รับผิดชอบเฉพาะด้าน เช่น กฎหมาย ไซเบอร์และ PDPA ความปลอดภัย BCM/BCP การสื่อสารภาวะวิกฤต หรือหน่วยงานกำกับดูแลภายนอก ตามกฎหมาย นโยบาย และแผนที่เกี่ยวข้อง

3.6.2 หลักการรายงานเหตุการณ์สำคัญ

การรายงานเหตุการณ์ไม่ทดแทนการระงับหรือควบคุมเหตุ ผู้พบเหตุและผู้รับผิดชอบต้องดำเนินการตามลำดับความจำเป็น ดังนี้

1. คุ้มครองชีวิต สุขภาพ และความปลอดภัยเป็นลำดับแรก
2. ระงับหรือจำกัดการขยายตัวของความเสียหาย
3. คุ้มครองข้อมูล ระบบ ทรัพย์สิน และพันธกิจสำคัญ

4. รักษาพยานหลักฐานและบันทึกลำดับเหตุการณ์
5. รายงานต่อผู้มีอำนาจและหน่วยงานเฉพาะด้าน
6. สื่อสารผ่านผู้ที่ได้รับมอบหมายหรือโฆษกที่มีอำนาจ
7. แก้ไข เยียวยา ฟื้นฟู และป้องกันการเกิดซ้ำ

สำหรับเหตุ Zero Tolerance เหตุวิกฤต หรือเหตุที่อาจกระทบชีวิต ข้อมูลสำคัญ หรือพันธกิจในวงกว้าง ให้รายงานตรงต่อผู้มีอำนาจตัดสินใจและแจ้งหน่วยบริหารความเสี่ยงหรือหน่วยงานเฉพาะด้านในเวลาเดียวกัน โดยไม่ให้หน่วยบริหารความเสี่ยงเป็นจุดผ่านที่อาจทำให้การตอบสนองล่าช้า

3.6.3 ตารางการรายงานและการยกระดับ *(Reporting and Escalation Matrix)*

ตารางที่ 3-4 *ตารางการรายงานและการยกระดับความเสี่ยง (Reporting and Escalation Matrix)*

เหตุหรือระดับความเสี่ยง	เวลารายงาน	เส้นทางรายงานขั้นต่ำ	สาระขั้นต่ำ
เหตุ Zero Tolerance เหตุวิกฤต ผลกระทบระดับ 5 หรือภัยคุกคามต่อชีวิตและข้อมูลสำคัญ	แจ้งเหตุทันที และจัดทำรายงานเบื้องต้นไม่เกิน 24 ชั่วโมง	ผู้พบเหตุ ⟶ ผู้บังคับบัญชา/Risk Owner/ผู้บัญชาการเหตุการณ์ ⟶ อธิการบดีหรือประธานคณะกรรมการที่เกี่ยวข้อง พร้อมแจ้งหน่วยงานเฉพาะด้านและผู้กำกับดูแลตามอำนาจ	ข้อเท็จจริงที่ยืนยันได้ ผลกระทบเบื้องต้น การระงับเหตุ ผู้รับผิดชอบจัดการเหตุ การรักษาหลักฐาน การสื่อสาร และการตัดสินใจเร่งด่วน
ความเสี่ยงระดับสูงมาก 16–25 หรือ Residual Risk ระดับสูงมาก	รายงานทันทีและไม่เกิน 24 ชั่วโมง	Risk Owner ⟶ หัวหน้าส่วนงาน ⟶ อธิการบดี/คณะกรรมการฝ่ายบริหาร พร้อมแจ้งหน่วยบริหารความเสี่ยง	คะแนนและเหตุผล สาเหตุ การควบคุมและช่องว่าง มาตรการเร่งด่วน เจ้าของมาตรการ ทรัพยากร และ Target Residual Risk
KRI เกิน RT ความเสี่ยงระดับสูง 10–15 การควบคุมสำคัญไม่ทำงานหรือมาตรการสำคัญล่าช้า	ภายใน 3 วันทำการหรือเร็วกว่าตาม Trigger ที่กำหนด	Risk Owner ⟶ หัวหน้าส่วนงาน ⟶ หน่วยบริหารความเสี่ยง ⟶ ผู้บริหารที่กำกับ	แนวโน้มและสาเหตุ ผลกระทบ การควบคุมที่บกพร่อง แผนแก้ไข (Corrective Action) ผู้รับผิดชอบ และกำหนดแล้วเสร็จ
ความเสี่ยงระดับปานกลาง 5–9	อย่างน้อยรายไตรมาส หรือตามรอบที่กำหนด	Risk Owner ⟶ หัวหน้าส่วนงาน	สถานะ KRI ประสิทธิผลของการควบคุม ความก้าวหน้าของมาตรการ แนวโน้ม และประเด็นที่ต้องตัดสินใจ
ความเสี่ยงระดับต่ำ 1–4	ตามรอบการบริหารงานปกติ	ผู้รับผิดชอบ ⟶ Risk Owner	การเปลี่ยนแปลงสำคัญและหลักฐานยืนยันว่าการควบคุมยังทำงานอย่างเหมาะสม

ระยะเวลาในตารางเป็นเกณฑ์กลาง หากกฎหมาย แผนฉุกเฉิน แผนเผชิญเหตุ แผนสื่อสารภาวะวิกฤต นโยบายไซเบอร์และ PDPA หรือข้อกำหนดเฉพาะกำหนดระยะเวลาที่เข้มงวดกว่า ให้ใช้ระยะเวลาที่เข้มงวดกว่า

3.6.4 การติดตามและปิดเหตุ

ภายหลังการรายงานเบื้องต้น เจ้าของความเสี่ยงหรือผู้รับผิดชอบจัดการเหตุต้อง

- รายงานความคืบหน้าตามความถี่ที่ผู้มีอำนาจกำหนด
- ประเมินผลกระทบและระดับความเสี่ยงที่ปรับปรุงแล้ว
- วิเคราะห์สาเหตุราก (Root Cause Analysis)
- จัดทำมาตรการแก้ไขและป้องกันการเกิดซ้ำ (Corrective and Preventive Action: CAPA)
- ประเมินความเสียหาย การเยียวยา และผลกระทบต่อผู้มีส่วนได้ส่วนเสีย
- จัดทำรายงานสรุปและบทเรียนภายหลังเหตุการณ์
- เสนอผู้มีอำนาจอนุมัติการปิดเหตุและกำหนดการติดตามภายหลัง

การปิดเหตุไม่ทำให้การติดตามมาตรการหรือความรับผิดตามกฎหมาย ระเบียบ หรือข้อบังคับสิ้นสุดลง หากยังมีการดำเนินการที่ต้องติดตามต่อเนื่อง

3.6.5 การยกระดับเป็นความเสี่ยงระดับมหาวิทยาลัย

ความเสี่ยงต้องได้รับการเสนอพิจารณายกระดับเป็นความเสี่ยงระดับมหาวิทยาลัย เมื่อมีลักษณะอย่างน้อยประการหนึ่ง ดังนี้

- กระทบวัตถุประสงค์เชิงยุทธศาสตร์หรือพันธกิจสำคัญ
- กระทบหลายส่วนงานหรือเกินขีดความสามารถของส่วนงานเดียว
- เกิน RA/RT หรือเกินอำนาจยอมรับของผู้บริหารระดับส่วนงาน
- มีความสัมพันธ์หรือการกระจุกตัวที่อาจทำให้ผลกระทบรุนแรงขึ้น
- ต้องใช้ทรัพยากรหรือการตัดสินใจระดับมหาวิทยาลัย
- อาจกระทบกฎหมาย ชีวิต ความปลอดภัย ชื่อเสียง หรือความเชื่อมั่นอย่างมีนัยสำคัญ

การยกระดับเป็น Enterprise Risk ต้องผ่านการกลั่นกรองและอนุมัติตามอำนาจที่กำหนด มิได้เกิดขึ้นโดยอัตโนมัติจากคะแนนหรือ KRI เพียงตัวเดียว

3.7 หลักการความรับผิดชอบร่วมกัน

การบริหารความเสี่ยงเป็นความรับผิดชอบร่วมกันของบุคลากรทุกระดับ แต่ความรับผิดชอบร่วมกันต้องไม่ทำให้ความเป็นเจ้าของ อำนาจตัดสินใจ หรือความรับผิดชอบต่อผลลัพธ์คลุมเครือ โดยกำหนดหลักการดังนี้

1. ความเสี่ยงแต่ละรายการต้องมีเจ้าของความเสี่ยงหลัก (Lead Risk Owner) หนึ่งรายซึ่งมีอำนาจเพียงพอในการตัดสินใจ จัดสรรทรัพยากร และรับผิดชอบต่อผลลัพธ์

2. กรณีความเสี่ยงเกี่ยวข้องกับหลายส่วนงาน อาจกำหนดเจ้าของความเสี่ยงร่วมได้ แต่ต้องระบุ Lead Risk Owner ผู้รับผิดชอบสูงสุดและกลไกการประสานงานให้ชัดเจน

3. การควบคุมสำคัญแต่ละรายการต้องมีเจ้าของการควบคุม (Control Owner)

4. มาตรการเพิ่มเติมทุกมาตรการต้องมีเจ้าของมาตรการ (Action Owner) ผลส่งมอบ และกำหนดเวลา

5. KRI ทุกตัวต้องมีเจ้าของข้อมูล (Data Owner) ซึ่งรับผิดชอบคุณภาพและความทันเวลาของข้อมูล

6. ผู้ประสานงานความเสี่ยง (Risk Coordinator/Risk Champion) ทำหน้าที่สนับสนุนและประสานงาน แต่ไม่เป็นเจ้าของความเสี่ยงแทนผู้บริหาร

บุคลากรต้องรายงานข้อมูล ความเสี่ยง สัญญาณเตือน เหตุการณ์ และข้อผิดพลาดโดยสุจริต ถูกต้อง และทันเวลา ขณะที่ผู้บริหารต้องสร้างสภาพแวดล้อมที่ปลอดภัยต่อการรายงาน รักษาความลับ คุ้มครองผู้รายงานโดยสุจริตจากการตอบโต้ และใช้ข้อมูลเพื่อระงับเหตุ แก้ไขสาเหตุ และปรับปรุงระบบ มากกว่ามุ่งกล่าวโทษโดยปราศจากข้อเท็จจริง

3.8 กฎบัตรคณะกรรมการบริหารความเสี่ยง

กฎบัตรคณะกรรมการบริหารความเสี่ยงเป็นเอกสารกำหนดวัตถุประสงค์ อำนาจ หน้าที่ ความรับผิดชอบ และสายการรายงานของคณะกรรมการ เพื่อให้การกำกับดูแลความเสี่ยงมีความชัดเจน โปร่งใส และไม่ซ้ำซ้อนกับคณะกรรมการตรวจสอบหรือฝ่ายบริหาร

กฎบัตรควรกำหนดสาระอย่างน้อย ดังนี้

1. สถานะและวัตถุประสงค์: ระบุว่าคณะกรรมการได้รับการแต่งตั้งโดยสภามหาวิทยาลัยหรือฝ่ายบริหาร มีวัตถุประสงค์และขอบเขตการกำกับความเสี่ยงระดับใด

2. ความสัมพันธ์และสายการรายงาน: กำหนดความสัมพันธ์กับสภามหาวิทยาลัย คณะกรรมการตรวจสอบ อธิการบดี คณะกรรมการบริหารมหาวิทยาลัย และคณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายในให้ชัดเจน

3. องค์ประกอบและคุณสมบัติ: กำหนดจำนวนและคุณสมบัติของกรรมการ ประธาน เลขานุการ ผู้เข้าร่วมประชุม ตลอดจนความรู้และประสบการณ์ที่จำเป็นด้านยุทธศาสตร์ การเงิน กฎหมาย เทคโนโลยี ความปลอดภัย และการบริหารความเสี่ยง

4. วาระและการพ้นจากตำแหน่ง: กำหนดวาระ การแต่งตั้งใหม่ การลาออก การพ้นจากตำแหน่ง และการแต่งตั้งทดแทน

5. อำนาจหน้าที่: กำหนดอำนาจเข้าถึงข้อมูล เรียกผู้เกี่ยวข้องเข้าชี้แจง ขอเอกสาร ขอความเห็นจากผู้เชี่ยวชาญ และเสนอเรื่องต่อผู้มีอำนาจตัดสินใจ

6. ขอบเขตความรับผิดชอบ: กำหนดหน้าที่ในการกลั่นกรองและทบทวนนโยบาย กรอบ RA/RT ภาพรวมความเสี่ยง KRI ความเสี่ยงเกิดใหม่ ความสัมพันธ์และการกระจุกตัวของความเสี่ยง ความเพียงพอของมาตรการ และประเด็นที่ต้องตัดสินใจ

7. ขอบเขตอำนาจตัดสินใจ: ระบุให้ชัดว่าคณะกรรมการมีอำนาจอนุมัติ ให้ความเห็นชอบ กลั่นกรอง ให้ข้อเสนอแนะ หรือเสนอเรื่องต่อผู้มีอำนาจในแต่ละกรณี โดยไม่ใช้อำนาจเกินกว่าที่ได้รับมอบหมาย

8. การประชุม: กำหนดให้ประชุมอย่างน้อยรายไตรมาส และสามารถจัดประชุมพิเศษเมื่อเกิดเหตุสำคัญ ความเสี่ยงสูงมาก เหตุ Zero Tolerance หรือความเสี่ยงเกิน RA/RT

9. องค์ประชุมและการลงมติ: กำหนดองค์ประชุม วิธีลงมติ การใช้สิทธิออกเสียง การบันทึกความเห็นต่าง และการดำเนินการกรณีคะแนนเสียงเท่ากัน

10. ผลประโยชน์ทับซ้อนและการรักษาความลับ: กำหนดให้กรรมการเปิดเผยผลประโยชน์ทับซ้อน งดร่วมพิจารณาหรือลงมติในเรื่องที่เกี่ยวข้อง และรักษาความลับหรือข้อมูลส่วนบุคคลตามกฎหมาย

11. วาระและข้อมูลประกอบการประชุม: กำหนดผู้รับผิดชอบจัดทำวาระ คุณภาพข้อมูล ระยะเวลาจัดส่งเอกสาร และการบันทึกมติ ผู้รับผิดชอบ และกำหนดเวลา

12. การรายงาน: กำหนดรูปแบบ ความถี่ สาระสำคัญ และเส้นทางการรายงานต่อสภามหาวิทยาลัยหรือฝ่ายบริหาร รวมทั้งการรายงานทันทีเมื่อเกิดเหตุสำคัญ

13. การประสานงาน: กำหนดการประสานกับคณะกรรมการตรวจสอบ กองตรวจสอบภายใน และคณะกรรมการหรือหน่วยงานเฉพาะด้าน เพื่อลดความซ้ำซ้อนและปิดช่องว่างการกำกับดูแล

14. แผนการดำเนินงานประจำปี: กำหนดปฏิทินการพิจารณานโยบาย RA/RT พอร์ตความเสี่ยง รายงานตามรอบ และประเด็นเชิงลึกที่ต้องติดตาม

15. การประเมินและทบทวน: กำหนดให้ประเมินผลการปฏิบัติงานของคณะกรรมการและทบทวนกฎบัตรอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อโครงสร้างและอำนาจหน้าที่เปลี่ยนแปลง

ข้อความกฎบัตรในคู่มือเป็นเพียงกรอบอ้างอิง ไม่ทดแทนกฎบัตรหรือคำสั่งแต่งตั้งที่ได้รับอนุมัติอย่างเป็นทางการ หากข้อความแตกต่างกัน ให้ยึดกฎบัตรหรือคำสั่งแต่งตั้งที่มีผลใช้บังคับ

3.9 อำนาจการยอมรับความเสี่ยง

การยอมรับความเสี่ยง (Risk Acceptance) หมายถึง การตัดสินใจโดยผู้มีอำนาจให้คงความเสี่ยงไว้ภายใต้การควบคุมและเงื่อนไขที่กำหนด โดยอาจเป็นการยอมรับภายหลังพิจารณาว่ามาตรการที่มีอยู่เพียงพอ หรือการยอมรับเป็นการชั่วคราวระหว่างดำเนินมาตรการเพิ่มเติม

การยอมรับความเสี่ยงมิใช่

- การยกเว้นการปฏิบัติตามกฎหมายหรือข้อกำหนด
- การอนุญาตให้เกิดเหตุ Zero Tolerance
- การยกเลิกหน้าที่ติดตามและรายงาน
- การโอนความรับผิดชอบจาก Risk Owner ไปยังผู้อนุมัติ
- การยอมรับโดยอาศัยคะแนนความเสี่ยงเพียงอย่างเดียว

ตารางที่ 3-5 *ระดับความเสี่ยงและกรอบอำนาจในการยอมรับความเสี่ยง*

ระดับความเสี่ยง	กรอบอำนาจที่เสนอ	เงื่อนไขขั้นต่ำ
ต่ำ 1–4 (L)	Risk Owner หรือหัวหน้าส่วนงานตามอำนาจที่ได้รับมอบหมาย	อยู่ภายใน RA/RT ไม่มีข้อห้ามตามกฎหมายหรือ Zero Tolerance การควบคุมทำงาน และติดตามตามรอบปกติ
ปานกลาง 5–9 (M)	หัวหน้าส่วนงานหรือผู้บริหารที่ได้รับมอบหมาย	ต้องพิจารณาความสอดคล้องกับ RA/RT มีเหตุผลและหลักฐานรองรับ กำหนด KRI การควบคุม มาตรการตามความเหมาะสม และวันที่ทบทวน
สูง 10–15 (H)	อธิการบดีหรือผู้บริหารระดับมหาวิทยาลัยที่ได้รับมอบอำนาจ โดยผ่านการกลั่นกรองตามโครงสร้างมหาวิทยาลัย	ไม่ยอมรับเป็นการดำเนินงานปกติหากเกิน RA/RT ต้องมีแผนลดความเสี่ยง Target Residual Risk เจ้าของมาตรการ ทรัพยากร ระยะเวลาสิ้นสุด และรายงานคณะกรรมการที่เกี่ยวข้อง
สูงมาก 16–25 (E)	ไม่ควรยอมรับเป็นการดำเนินงานปกติ ต้องยกระดับทันที การคงความเสี่ยงไว้ชั่วคราวให้เป็นไปตามอำนาจที่ได้รับอนุมัติและรายงานผู้กำกับดูแล	ใช้เฉพาะเมื่อไม่สามารถหยุดการดำเนินงานได้ทันที หรือการหยุดอาจก่อให้เกิดผลกระทบรุนแรงกว่า ต้องมีแผนฉุกเฉิน มาตรการชดเชย ระยะเวลาสิ้นสุด การติดตามอย่างใกล้ชิด และการทบทวนตามรอบที่ผู้มีอำนาจกำหนด

คะแนนความเสี่ยงเป็นเพียงองค์ประกอบหนึ่งในการพิจารณา ผู้อนุมัติต้องพิจารณาร่วมกับ

- RA/RT และ Risk Capacity
- ข้อจำกัดตามกฎหมายและข้อผูกพัน
- ประสิทธิผลของการควบคุม
- ผลกระทบต่อยุทธศาสตร์และพันธกิจสำคัญ
- ความสัมพันธ์และการกระจุกตัวของความเสี่ยง
- ผลกระทบต่อชีวิต ความปลอดภัย ข้อมูล ชื่อเสียง และผู้มีส่วนได้ส่วนเสีย
- ทางเลือก ต้นทุน ประโยชน์ และผลกระทบจากการไม่ดำเนินการ
- ระยะเวลาที่ต้องคงความเสี่ยงไว้

หลักฐานการยอมรับความเสี่ยง

การยอมรับความเสี่ยงต้องบันทึกอย่างน้อย ดังนี้

1. รายละเอียดความเสี่ยงและวัตถุประสงค์ที่ได้รับผลกระทบ
2. Inherent Risk และ Residual Risk
3. สถานะ RA/RT และเหตุผลที่เสนอให้ยอมรับ
4. การควบคุมที่มีอยู่และผลการประเมินประสิทธิผล
5. ทางเลือกที่พิจารณาและเหตุผลที่ไม่เลือกมาตรการเพิ่มเติม

6. ผลกระทบ ต้นทุน ประโยชน์ และข้อจำกัด
7. KRI เงื่อนไขการติดตาม และ Trigger ในการยกระดับ
8. มาตรการชดเชยหรือแผนฉุกเฉิน หากมี
9. ผู้เสนอ ผู้ให้ความเห็น และผู้อนุมัติ
10. วันที่มีผล ระยะเวลาการยอมรับ และวันที่ทบทวนหรือสิ้นสุด

การยอมรับความเสี่ยงระดับสูงหรือสูงมากต้องมีระยะเวลาสิ้นสุด (Expiry/Sunset Date) และต้องเสนออนุมัติใหม่หากจำเป็นต้องคงความเสี่ยงไว้เกินระยะเวลาที่กำหนด

เหตุ Zero Tolerance ไม่อยู่ในอำนาจการยอมรับตามตารางนี้ มหาวิทยาลัยไม่สามารถอนุมัติให้กระทำการที่ผิดกฎหมาย ทุจริต หรือฝ่าฝืนข้อห้ามที่กำหนดได้ เมื่อพบเหตุหรือข้อสงสัยที่มีมูล ต้องระงับเหตุ รายงาน รักษาหลักฐาน ตรวจสอบข้อเท็จจริง แก้ไข เยียวยา และดำเนินการตามกฎหมายหรือนโยบายที่เกี่ยวข้องโดยไม่ชักช้า ทั้งนี้ Zero Tolerance มิได้หมายความว่าความเป็นไปได้ของการเกิดเหตุเป็นศูนย์ แต่หมายถึงมหาวิทยาลัยไม่ยอมรับการกระทำ การเพิกเฉย หรือการคงเหตุการณ์ดังกล่าวไว้โดยไม่ดำเนินการ

3.10 เกณฑ์การยกระดับความเสี่ยง

การยกระดับความเสี่ยง (Risk Escalation) หมายถึง การส่งต่อข้อมูลความเสี่ยงหรือเหตุการณ์ไปยังผู้มีอำนาจตัดสินใจในระดับสูงขึ้น เมื่อความรุนแรง ความเร่งด่วน ขอบเขตผลกระทบ หรือทรัพยากรที่ต้องใช้เกินอำนาจหรือขีดความสามารถของผู้รับผิดชอบระดับเดิม

ให้ยกระดับเมื่อเข้าเงื่อนไขอย่างน้อยหนึ่งข้อ ดังนี้

1. **ระดับความเสี่ยงสูงหรือสูงมาก:** คะแนนความเสี่ยงอยู่ในระดับสูง 10–15 หรือสูงมาก 16–25
2. **ผลกระทบรุนแรงหรือเข้าเกณฑ์ Override:** ผลกระทบอยู่ในระดับ 5 หรือเข้าเกณฑ์ยกระดับเป็นกรณีพิเศษ โดยไม่คำนึงถึงคะแนนรวมเพียงอย่างเดียว
3. **KRI เข้าใกล้หรือเกิน RT:** KRI เกิน RT อยู่ในช่วงเตือน หรือมีแนวโน้มว่าจะเกินเกณฑ์ภายในรอบการติดตามถัดไปตามแบบจำลองหรือข้อมูลที่เชื่อถือได้
4. **เหตุ Zero Tolerance หรือเหตุการณ์สำคัญ:** เป็นเหตุ Zero Tolerance เหตุวิกฤต หรือเหตุการณ์เกือบเกิดความเสียหาย (Near Miss) ที่หากเกิดขึ้นจริงอาจมีผลกระทบรุนแรง
5. **ผลกระทบข้ามส่วนงานหรือเชิงยุทธศาสตร์:** กระทบหรืออาจกระทบหลายส่วนงาน วัตถุประสงค์เชิงยุทธศาสตร์ พันธกิจสำคัญ หรือภาพรวมความเสี่ยงของมหาวิทยาลัย
6. **การควบคุมหรือมาตรการไม่มีประสิทธิผล:** การควบคุมสำคัญไม่ทำงาน มีข้อบกพร่องที่มีนัยสำคัญ หรือมาตรการล่าช้าจนระดับความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk) ไม่น่าจะบรรลุภายในเวลาที่กำหนด

7. เกินอำนาจหรือขีดความสามารถของ Risk Owner: ต้องใช้ทรัพยากร อำนาจตัดสินใจ การประสานงาน หรือการสื่อสารเกินขอบเขตของ Risk Owner หรือส่วนงาน

8. ผลกระทบต่อมิติสำคัญ: กระทบหรืออาจกระทบชื่อเสียงและความเชื่อมั่น ชีวิตและความปลอดภัย ฐานะการเงิน กฎหมาย ไซเบอร์และ PDPA ความต่อเนื่อง สิ่งแวดล้อม หรือผู้มีส่วนได้ส่วนเสียอย่างมีนัยสำคัญ

9. ความเสี่ยงเกิดใหม่: เป็นความเสี่ยงเกิดใหม่ที่ข้อมูลยังมีจำกัด มีความไม่แน่นอนสูง หรือเปลี่ยนแปลงอย่างรวดเร็ว แต่อาจมีผลกระทบสูง

10. ความสัมพันธ์หรือการกระจุกตัวของความเสี่ยง: ความเสี่ยงหลายรายการมีสาเหตุ แหล่งข้อมูล ระบบ ผู้ให้บริการ ทรัพยากร หรือผลกระทบร่วมกัน ซึ่งอาจทำให้ระดับความเสี่ยงในภาพรวมสูงขึ้น

11. ข้อกำหนดตามกฎหมายหรือหน่วยงานกำกับดูแล: กฎหมาย ระเบียบ สัญญา หรือหน่วยงานกำกับกำหนดให้ต้องแจ้ง รายงาน หรือดำเนินการภายในระยะเวลาที่กำหนด

12. ความเห็นต่างที่ยังไม่ยุติ: มีความเห็นต่างอย่างมีนัยสำคัญเกี่ยวกับระดับความเสี่ยง ประสิทธิผลของการควบคุม การยอมรับความเสี่ยง หรือความเพียงพอของมาตรการ และไม่สามารถยุติได้ในระดับเดิม

หลักการยกระดับ

1. การยกระดับรายงานต้องดำเนินการตามระยะเวลาที่กำหนดใน Reporting and Escalation Matrix โดยเหตุ Zero Tolerance เหตุวิกฤต และความเสี่ยงสูงมากต้องรายงานทันที

2. การรายงานหรือยกระดับไม่ทำให้ Risk Owner พ้นจากหน้าที่ระงับเหตุ บริหารความเสี่ยง ดำเนินมาตรการ และติดตามผล

3. หน่วยบริหารความเสี่ยงทำหน้าที่ประสานและติดตามการยกระดับ แต่ไม่ควรเป็นจุดผ่านที่ทำให้การรายงานเหตุฉุกเฉินต่อผู้มีอำนาจล่าช้า

4. การยกระดับรายงานไม่ทำให้ความเสี่ยงกลายเป็น Enterprise Risk โดยอัตโนมัติ การบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัยต้องผ่านการกลั่นกรองและอนุมัติตามอำนาจที่กำหนด

5. หากกฎหมาย แผนฉุกเฉิน หรือนโยบายเฉพาะด้านกำหนดเวลาและเส้นทางรายงานที่เข้มงวดกว่า ให้ใช้ข้อกำหนดที่เข้มงวดกว่า

ข้อมูลที่ต้องบันทึก

การยกระดับต้องบันทึกในทะเบียนความเสี่ยง (Risk Register) หรือบันทึกการยกระดับเหตุการณ์ (Incident/Escalation Record) อย่างน้อย ดังนี้

- วันที่ เวลา และผู้รายงาน
- เหตุผลหรือเกณฑ์ที่ทำให้ต้องยกระดับ
- ข้อเท็จจริงและแหล่งข้อมูล
- วัตถุประสงค์และผู้มีส่วนได้ส่วนเสียที่ได้รับผลกระทบ
- ระดับความเสี่ยงและสถานะ RA/RT

- การควบคุมและมาตรการที่ดำเนินการแล้ว
- การดำเนินการเร่งด่วนและประเด็นที่ต้องตัดสินใจ
- ผู้รับผิดชอบและทรัพยากรที่ต้องการ
- ผู้มีอำนาจพิจารณาและผลการตัดสินใจ
- รอบรายงานครั้งถัดไปและกำหนดเวลาปิดประเด็น

3.11 การสร้างวัฒนธรรมความเสี่ยงภายใต้โครงสร้างการกำกับดูแล

รายละเอียดองค์ประกอบของวัฒนธรรมความเสี่ยงให้เป็นไปตามข้อ 2.14 โดยในด้านโครงสร้างการกำกับดูแล ผู้กำกับดูแลและฝ่ายบริหารต้องขับเคลื่อนวัฒนธรรมความเสี่ยงผ่านกลไกต่อไปนี้

1. ภาวะผู้นำและพฤติกรรมต้นแบบ (Tone from the Top): ใช้ข้อมูลความเสี่ยงและโอกาสประกอบการตัดสินใจ แสดงความรับผิดชอบต่อผลลัพธ์ และไม่สนับสนุนการปกปิดหรือบิดเบือนข้อมูล

2. ความชัดเจนของความเป็นเจ้าของ (Clear Ownership): กำหนด Risk Owner, Control Owner, Action Owner และ Data Owner พร้อมอำนาจ ทรัพยากร เป้าหมาย และเส้นทางการรายงานที่ชัดเจน

3. การสื่อสารอย่างเปิดเผยและปลอดภัย (Speak-up and Psychological Safety): จัดให้มีช่องทางรายงานที่เข้าถึงได้ รักษาความลับ และคุ้มครองผู้รายงานโดยสุจริตจากการตอบโต้หรือการปฏิบัติที่ไม่เป็นธรรม

4. การท้าทายอย่างสร้างสรรค์ (Constructive Challenge): เปิดโอกาสให้คณะกรรมการ สายงานที่สอง และผู้เกี่ยวข้องตั้งคำถามต่อสมมติฐาน ข้อมูล ระดับความเสี่ยง และความเพียงพอของมาตรการ โดยไม่ถูกมองว่าเป็นการขัดขวางการดำเนินงาน

5. การตัดสินใจโดยคำนึงถึงความเสี่ยง (Risk-informed Decision-making): กำหนดให้ข้อเสนอเชิงนโยบาย โครงการและการลงทุนสำคัญ แสดงความเสี่ยง โอกาส RA/RT ทางเลือก และมาตรการรองรับก่อนอนุมัติ

6. ความรับผิดชอบต่อผลลัพธ์ (Accountability): ติดตามการตัดสินใจ มาตรการ กำหนดเวลา คุณภาพข้อมูล และผลลัพธ์ พร้อมยกระดับเมื่อไม่เป็นไปตามที่กำหนด

7. การเรียนรู้และแก้ไขเชิงระบบ (Risk Learning): วิเคราะห์สาเหตุรากและเรียนรู้จาก Near Miss เหตุการณ์ ข้อร้องเรียน ข้อผิดพลาด และผลการตรวจสอบ เพื่อปรับปรุงกระบวนการและป้องกันการเกิดซ้ำ

8. การพัฒนาความสามารถ (Risk Competency): กำหนดความรู้และทักษะด้านความเสี่ยงตามบทบาท พร้อมพัฒนาผู้กำกับดูแล ผู้บริหาร Risk Owner ผู้ประสานงาน และบุคลากรอย่างต่อเนื่อง

9. การประเมินจากพฤติกรรมและผลลัพธ์: ใช้ข้อมูลหลายแหล่ง เช่น ความรวดเร็วในการรายงาน ความตรงเวลาของมาตรการ เหตุการณ์ซ้ำ คุณภาพ Risk Register ผลการตรวจสอบ และหลักฐานการใช้ข้อมูลความเสี่ยงในการตัดสินใจ โดยไม่ประเมินจากจำนวนผู้เข้าร่วมอบรมเพียงอย่างเดียว

ผลการประเมินวัฒนธรรมความเสี่ยงต้องรายงานต่อฝ่ายบริหารอย่างน้อยปีละหนึ่งครั้ง และใช้ประกอบการกำหนดแผนพัฒนาความสามารถ การสื่อสาร การควบคุม และระดับการพัฒนาระบบบริหารความเสี่ยง

การจัดวาง “ข้อกำหนดก่อนประกาศใช้”

รายการดังกล่าวไม่ควรปรากฏในเนื้อหาฉบับประกาศใช้ ควรจัดเป็น **Checklist สำหรับผู้จัดทำคู่มือ** แยกต่างหาก โดยคงรายการดังนี้

- ตรวจสอบชื่อคณะกรรมการและสายการรายงาน
- ตรวจสอบคำสั่งมอบอำนาจและอำนาจยอมรับความเสี่ยง
- ตรวจสอบ RACI ให้มี A เพียงหนึ่งรายในแต่ละระดับ
- ตรวจสอบแผนภาพโครงสร้างให้กองตรวจสอบภายในเป็นอิสระ
- จัดทำแบบฟอร์ม Incident Brief, Escalation Record และ Risk Acceptance Record
- ทบทวนเมื่อโครงสร้าง กฎหมาย มาตรฐาน หรือการมอบอำนาจเปลี่ยนแปลง

ส่วนที่ 4
กรอบและกระบวนการบริหารความเสี่ยง มหาวิทยาลัยแม่โจ้

4.1 หลักการของกรอบการบริหารความเสี่ยงองค์กร

มหาวิทยาลัยแม่โจ้กำหนดกรอบการบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM) เป็นกรอบกลางสำหรับบริหารความไม่แน่นอนที่อาจส่งผลทั้งด้านลบและด้านบวกต่อการบรรลุวิสัยทัศน์ พันธกิจ วัตถุประสงค์เชิงยุทธศาสตร์ และเป้าหมายของมหาวิทยาลัย โดยบูรณาการการบริหารความเสี่ยงเข้ากับการกำกับดูแล การกำหนดยุทธศาสตร์ การบริหารผลการดำเนินงาน การจัดสรรทรัพยากร การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ และการตัดสินใจทุกระดับ

กรอบนี้ประยุกต์ใช้ ISO 31000:2018, COSO Enterprise Risk Management—Integrating with Strategy and Performance (2017) และหลักเกณฑ์กระทรวงการคลังด้านการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ โดยปรับให้เหมาะสมกับบริบท โครงสร้าง และพันธกิจของมหาวิทยาลัย

รายละเอียดหลักการ ISO 31000:2018 ให้เป็นไปตามข้อ 2.8 โดยมหาวิทยาลัยนำหลักการดังกล่าวมาสู่การออกแบบกรอบการปฏิบัติ ดังนี้

1. เริ่มต้นจากวัตถุประสงค์ (Objective-driven): ความเสี่ยงทุกเรื่องต้องเชื่อมโยงกับวัตถุประสงค์ ผลลัพธ์ ตัวชี้วัด หรือพันธกิจที่ต้องคุ้มครองอย่างชัดเจน

2. ระบบเดียว หลายกรอบอ้างอิง (One Integrated System, Multiple Frameworks): ใช้กระบวนการกลาง คำศัพท์ เกณฑ์ เครื่องมือ ข้อมูล และหลักฐานร่วมเท่าที่เหมาะสม เพื่อสนับสนุน ERM การควบคุมภายใน Compliance, BCM/BCP, EdPEx, ESG และการให้ความเชื่อมั่น โดยไม่สร้างภาระงานซ้ำซ้อน

3. บูรณาการกับการบริหารและการตัดสินใจ (Integrated into Management and Decision-making): เชื่อมโยงความเสี่ยงกับยุทธศาสตร์ แผนงาน งบประมาณ โครงการ การลงทุน การดำเนินงาน และการติดตามผล

4. ใช้มาตรฐานเดียวกันและเหมาะสมตามสัดส่วน (Common Standards and Proportionality): ใช้กระบวนการและเกณฑ์กลางทั่วทั้งมหาวิทยาลัย โดยปรับระดับรายละเอียด ความถี่ และความเข้มข้นให้เหมาะสมกับภารกิจ ขนาด ความซับซ้อน และระดับความเสี่ยงของแต่ละส่วนงาน

5. กำหนดความเป็นเจ้าของและอำนาจตัดสินใจอย่างชัดเจน (Clear Ownership and Decision Rights): กำหนด Objective Owner, Risk Owner, Control Owner, Action Owner และ Data Owner พร้อมอำนาจ ทรัพยากร และเส้นทางการรายงานตามหลัก Three Lines

6. ใช้ข้อมูลและหลักฐานที่เชื่อถือได้ (Evidence-based and Data-driven): ใช้ข้อมูลที่ถูกต้อง ครบถ้วน ทันเวลา และตรวจสอบย้อนกลับได้ พร้อมเปิดเผยข้อจำกัด สมมติฐาน และความไม่แน่นอนของข้อมูล

7. บริหารเชิงรุกและมองไปข้างหน้า (Proactive and Forward-looking): ใช้ KRI สัญญาณเตือนล่วงหน้า การวิเคราะห์แนวโน้ม และการติดตามความเสี่ยงเกิดใหม่ เพื่อเตรียมการก่อนเกิดผลกระทบอย่างมีนัยสำคัญ

8. บริหารทั้งความเสี่ยงและโอกาส (Risk and Opportunity Management): ไม่มุ่งเพียงลดความสูญเสีย แต่พิจารณาทางเลือกและโอกาสในการสร้าง รักษา และเพิ่มคุณค่าภายในกรอบ RA/RT

9. เชื่อมโยงความเสี่ยง–การควบคุม–การให้ความเชื่อมั่น (Risk–Control–Assurance): ประเมินความเสี่ยงควบคู่กับประสิทธิผลของการควบคุมและแหล่งการให้ความเชื่อมั่น เพื่อให้ทราบระดับความเสี่ยงคงเหลืออย่างมีหลักฐาน

10. ทบทวน เรียนรู้ และปรับปรุงอย่างต่อเนื่อง (Learning and Continual Improvement): ใช้ผลการติดตาม เหตุการณ์จริง ข้อร้องเรียน Near Miss ผลการตรวจสอบ และบทเรียนมาปรับปรุงกรอบ กระบวนการ การควบคุม และความสามารถของบุคลากร

การบริหารความเสี่ยงตามกรอบนี้มิใช่กิจกรรมแยกส่วนหรือการจัดทำเอกสารเพื่อรายงานตามรอบเท่านั้น แต่เป็นส่วนหนึ่งของการบริหารงานประจำและการตัดสินใจโดยคำนึงถึงความเสี่ยง (Risk-informed Decision-making)

4.2 วัตถุประสงค์ของกรอบการบริหารความเสี่ยง

กรอบการบริหารความเสี่ยงมีวัตถุประสงค์เพื่อแปลงนโยบายและหลักการกำกับดูแลไปสู่กระบวนการปฏิบัติที่เป็นมาตรฐานเดียวกัน โดยมีวัตถุประสงค์ ดังนี้

1. ถ่ายทอดนโยบายสู่การปฏิบัติ: แปลงนโยบาย กรอบ RA/RT และหลักการกำกับดูแลให้เป็นกระบวนการ เกณฑ์ เครื่องมือ และแนวทางปฏิบัติที่ส่วนงานสามารถนำไปใช้ได้จริง

2. สร้างมาตรฐานเดียวกัน: กำหนดคำศัพท์ วิธีระบุและประเมินความเสี่ยง Risk Matrix แบบฟอร์ม ข้อมูล และแนวทางรายงานที่เป็นมาตรฐานเดียวกันทั่วทั้งมหาวิทยาลัย

3. เชื่อมโยงกับยุทธศาสตร์และผลการดำเนินงาน: ทำให้ความเสี่ยงและโอกาสเชื่อมโยงกับวัตถุประสงค์ KPI โครงการ การลงทุน งบประมาณ และผลลัพธ์ที่มหาวิทยาลัยต้องการบรรลุ

4. สนับสนุนการตัดสินใจบนฐานข้อมูล: จัดให้มีข้อมูลด้านความเสี่ยง โอกาส สมมติฐาน และทางเลือกที่ถูกต้อง ครบถ้วน ทันเวลา และเหมาะสมกับระดับการตัดสินใจ

5. กำหนดความรับผิดชอบและเส้นทางการรายงาน: ทำให้บทบาทของผู้กำกับดูแล ฝ่ายบริหาร ส่วนงาน Risk Owner และหน่วยงานในแต่ละสายตามหลัก Three Lines มีความชัดเจน

6. บริหารความเสี่ยงภายในกรอบ RA/RT: เชื่อมโยงการประเมินความเสี่ยง KRI สัญญาณเตือน การตอบสนอง การยกระดับรายงาน และอำนาจยอมรับความเสี่ยงเข้าด้วยกัน

7. จัดลำดับความสำคัญและจัดสรรทรัพยากร: ใช้ระดับ แนวโน้ม ความเร่งด่วน ความสัมพันธ์ และผลกระทบของความเสี่ยงประกอบการจัดลำดับมาตรการและจัดสรรทรัพยากรอย่างเหมาะสม

8. เชื่อมโยงการควบคุมและการให้ความเชื่อมั่น: สนับสนุนการออกแบบและประเมินการควบคุมภายในการกำหนด Residual Risk และการประสานแหล่งการให้ความเชื่อมั่น

9. เพิ่มความพร้อมและความยืดหยุ่น: สนับสนุนการติดตามความเสี่ยงเกิดใหม่ การเตรียมพร้อมต่อเหตุฉุกเฉิน การบริหารความต่อเนื่อง และการฟื้นตัวจากเหตุหยุดชะงัก

10. สร้างข้อมูลความเสี่ยงสำหรับการกำกับดูแล: จัดทำ Risk Register, Portfolio View, Dashboard และรายงานที่เชื่อถือได้สำหรับ Risk Owner ผู้บริหาร คณะกรรมการ และสภามหาวิทยาลัย

11. สนับสนุนการสร้างคุณค่าและความยั่งยืน: ส่งเสริมการใช้ประโยชน์จากโอกาส นวัตกรรม ความเป็นเลิศ ESG และการพัฒนาอย่างยั่งยืนภายในระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้

12. สนับสนุนการเรียนรู้และปรับปรุงระบบ: ใช้ผลการติดตาม เหตุการณ์จริง ข้อสังเกต และบทเรียนในการพัฒนาระดับความสามารถและประสิทธิผลของระบบบริหารความเสี่ยงอย่างต่อเนื่อง

กรอบการบริหารความเสี่ยงทำหน้าที่เชื่อมโยงวัตถุประสงค์ ความเสี่ยง การควบคุม ข้อมูล การตอบสนอง และการตัดสินใจ เพื่อให้มหาวิทยาลัยบริหารความไม่แน่นอนและสร้างคุณค่าได้อย่างเป็นระบบ

4.3 องค์ประกอบของกรอบการบริหารความเสี่ยง

มหาวิทยาลัยแม่โจ้กำหนดกรอบการบริหารความเสี่ยงองค์กรโดยสังเคราะห์หลักการจาก COSO ERM 2017, ISO 31000:2018 หลักเกณฑ์กระทรวงการคลัง และแนวทางที่เกี่ยวข้อง เป็นองค์ประกอบในการบริหารความเสี่ยงของมหาวิทยาลัยจำนวน 8 องค์ประกอบที่เชื่อมโยงและสนับสนุนกัน ดังนี้

ตารางที่ 4-1 *องค์ประกอบของกรอบการบริหารความเสี่ยงองค์กร มหาวิทยาลัยแม่โจ้*

องค์ประกอบ	สาระสำคัญ	ผลลัพธ์หลัก
1. การกำกับดูแลและวัฒนธรรม (Governance and Culture)	โครงสร้างและบทบาทตามหลัก Three Lines ภาวะผู้นำ ความเป็นเจ้าของความเสี่ยง อำนาจตัดสินใจ ความโปร่งใส และวัฒนธรรมที่เอื้อต่อการรายงาน	โครงสร้าง อำนาจ หน้าที่ สายการรายงาน และพฤติกรรมที่สนับสนุน ERM
2. ยุทธศาสตร์และวัตถุประสงค์ (Strategy and Objectives)	เชื่อมโยงวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ KPI แผนงาน โครงการ และผลลัพธ์ที่ต้องการบรรลุ	วัตถุประสงค์ ตัวชี้วัด สมมติฐาน และผลลัพธ์ที่ชัดเจนและวัดผลได้
3. ความสามารถและระดับการยอมรับความเสี่ยง (Risk Capacity, Appetite and Tolerance)	กำหนดระดับความเสี่ยงสูงสุดที่รองรับได้ ระดับความเสี่ยงที่ยอมรับได้ และขอบเขตความเบี่ยงเบนที่ยอมรับได้	กรอบ RA/RT เกณฑ์การตัดสินใจ อำนาจยอมรับความเสี่ยง และเกณฑ์การยกระดับ
4. การระบุ วิเคราะห์ และประเมินความเสี่ยง (Risk Identification, Analysis and Evaluation)	วิเคราะห์บริบทและผู้มีส่วนได้ส่วนเสีย ระบุสาเหตุ เหตุการณ์ ผลกระทบ การควบคุม โอกาสเกิด และระดับความเสี่ยง	Risk Register, Risk Profile และการจัดลำดับความสำคัญของความเสี่ยง

องค์ประกอบ	สาระสำคัญ	ผลลัพธ์หลัก
5. การตอบสนองและการควบคุม (Risk Response and Control)	เลือกแนวทางหลีกเลี่ยง ลดหรือควบคุม แบ่งปันหรือถ่ายโอน ยอมรับ หรือใช้ประโยชน์จากโอกาส พร้อมออกแบบและดำเนินมาตรการ	Risk Treatment Plan, Control Plan, Action Owner และ Target Residual Risk
6. ข้อมูล ตัวชี้วัด และการรายงาน (Risk Information, Indicators and Reporting)	กำหนด KPI, KRI, KCI และ EWS พร้อมนิยาม สูตร แหล่งข้อมูล เจ้าของข้อมูล ความถี่ Dashboard และรายงานที่เหมาะสมกับระดับการตัดสินใจ	ข้อมูลความเสี่ยงที่ถูกต้อง ครบถ้วน ทันเวลา ตรวจสอบย้อนกลับได้ และพร้อมใช้ตัดสินใจ
7. การติดตาม ทบทวน และการให้ความเชื่อมั่น (Monitoring, Review and Assurance)	ติดตามความเสี่ยงและมาตรการ ประเมินประสิทธิผลของการควบคุม ทบทวน RA/RT และประสานแหล่งการให้ความเชื่อมั่น	รายงานสถานะความเสี่ยง ผลประเมินการควบคุม Assurance Map ข้อค้นพบ และช่องว่างที่ต้องปรับปรุง
8. ความต่อเนื่อง ความยืดหยุ่น และการพัฒนา (Continuity, Resilience and Improvement)	เชื่อมโยง BCM, BCP, DRP การจัดการภาวะวิกฤต การเรียนรู้จากเหตุการณ์ และการปรับปรุงระบบอย่างต่อเนื่อง	ความพร้อมต่อเหตุหยุดชะงัก ความสามารถในการฟื้นตัว และระดับการพัฒนาระบบที่สูงขึ้น

องค์ประกอบทั้ง 8 ประการไม่ใช่ขั้นตอนที่ต้องดำเนินการตามลำดับ แต่เป็นโครงสร้างของระบบที่ต้องทำงานเชื่อมโยงกันตลอดวงจรการบริหารความเสี่ยง

4.3.1 การกำหนดทิศทางจากบนลงล่าง *(Top-down Approach)*

สภามหาวิทยาลัย คณะกรรมการที่เกี่ยวข้อง อธิการบดี และผู้บริหารระดับสูง ทำหน้าที่กำหนดหรือถ่ายทอด

- ทิศทางและวัตถุประสงค์เชิงยุทธศาสตร์
- นโยบายและกรอบการบริหารความเสี่ยง
- Risk Capacity, Risk Appetite และ Risk Tolerance
- ตัวชี้วัดความเสี่ยงระดับมหาวิทยาลัย (University-level KRIs)
- ประเด็นความเสี่ยงและผลลัพธ์สำคัญที่ต้องติดตาม
- อำนาจการยอมรับและเกณฑ์การยกระดับความเสี่ยง
- ลำดับความสำคัญและกรอบการจัดสรรทรัพยากร

ฝ่ายบริหารต้องถ่ายทอดทิศทางดังกล่าวไปสู่ส่วนงาน เจ้าของวัตถุประสงค์ และเจ้าของความเสี่ยง พร้อมกำกับติดตามผลการดำเนินงานและระดับความเสี่ยงอย่างต่อเนื่อง

4.3.2 การบริหารจากล่างขึ้นบน *(Bottom-up Approach)*

ส่วนงานและหน่วยงานต้องระบุและบริหารความเสี่ยงที่เกิดจากวัตถุประสงค์ กระบวนงาน โครงการ ระบบ และการให้บริการในความรับผิดชอบ โดยอย่างน้อยต้อง

1. วิเคราะห์บริบทและกำหนดวัตถุประสงค์ที่ชัดเจน
2. ระบุความเสี่ยงด้วยโครงสร้าง Cause–Event–Impact
3. จัดทำและทบทวน Risk Register
4. ประเมิน Inherent Risk การควบคุม และ Residual Risk
5. กำหนด Risk Owner, Control Owner, Action Owner และ Data Owner
6. กำหนด KRI, RA/RT และ Trigger/Action ที่เกี่ยวข้อง
7. ดำเนินและติดตามมาตรการตอบสนอง
8. รายงานหรือยกระดับความเสี่ยงที่เกินอำนาจ เกิน RT หรือกระทบข้ามส่วนงาน

ข้อมูลจากส่วนงานต้องได้รับการรับรองโดยผู้รับผิดชอบตามสายงานก่อนนำมารวบรวมและวิเคราะห์ในภาพมหาวิทยาลัย

4.3.3 การบูรณาการแนวราบและภาพรวมมหาวิทยาลัย *(Horizontal Integration and Portfolio View)*

หน่วยงานด้านการบริหารความเสี่ยงทำหน้าที่รวบรวม วิเคราะห์ และท้าทายคุณภาพข้อมูลจากกระบวนการ Top-down และ Bottom-up อย่างสร้างสรรค์ โดยประสานกับหน่วยงานด้านยุทธศาสตร์ การเงิน กฎหมาย เทคโนโลยีดิจิทัล ความปลอดภัย BCM/BCP คุณภาพ และหน้าที่กำกับเฉพาะด้าน

การจัดทำภาพรวมความเสี่ยงของมหาวิทยาลัยต้องพิจารณาอย่างน้อย

- ความเชื่อมโยงกับวัตถุประสงค์เชิงยุทธศาสตร์
- ระดับและแนวโน้มของความเสี่ยง
- สถานะ RA/RT และ KRI
- ความสัมพันธ์และการพึ่งพาระหว่างความเสี่ยง
- ผลกระทบร่วมและการกระจุกตัวของความเสี่ยง
- ความเสี่ยงเกิดใหม่และการเปลี่ยนแปลงของบริบท
- ความเพียงพอของการควบคุมและมาตรการ
- ทรัพยากรและประเด็นที่ต้องการการตัดสินใจระดับมหาวิทยาลัย

University Risk Profile และ Portfolio View ต้องผ่านการยืนยันข้อมูลจาก Risk Owner การกลั่นกรองตามโครงสร้างฝ่ายบริหาร และการพิจารณาหรือกำกับดูแลของคณะกรรมการตามอำนาจหน้าที่ มิใช่เพียงการนำรายการความเสี่ยงของส่วนงานมารวมกัน

ภาพที่ 4-1

ภาพแสดงกรอบการบริหารความเสี่ยงองค์กร มหาวิทยาลัยแม่โจ้ (MJU Enterprise Risk Management Framework)

ที่มา: มหาวิทยาลัยแม่โจ้ ประยุกต์จาก COSO ERM 2017, ISO 31000:2018 และหลักเกณฑ์กระทรวงการคลังด้านการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

4.4 กระบวนการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้

มหาวิทยาลัยแม่โจ้กำหนดกระบวนการบริหารความเสี่ยง 8 ขั้นตอน เพื่อให้การบริหารความเสี่ยงระดับมหาวิทยาลัย ระดับส่วนงาน ระดับกระบวนงาน และระดับโครงการเป็นไปในทิศทางและมาตรฐานเดียวกัน โดยประยุกต์จาก ISO 31000:2018, COSO ERM 2017 และหลักเกณฑ์กระทรวงการคลังที่เกี่ยวข้อง

กระบวนการดังกล่าวเป็นวงจรต่อเนื่อง ตั้งแต่การกำหนดบริบทและวัตถุประสงค์ การระบุและประเมินความเสี่ยง การเลือกและดำเนินมาตรการ ตลอดจนการสื่อสาร ติดตาม ทบทวน และปรับปรุงผลการดำเนินงาน

การสื่อสารและปรึกษาหารือ (Communication and Consultation) การติดตามและทบทวน (Monitoring and Review) ตลอดจนการบันทึกและรายงาน (Recording and Reporting) ต้องดำเนินการตลอดทั้ง 8 ขั้นตอน มิใช่ดำเนินการเฉพาะในขั้นตอนท้ายเท่านั้น

ตารางที่ 4-2 *กระบวนการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้ 8 ขั้นตอน*

ขั้นตอน	กระบวนการ	คำถามสำคัญ	ผลลัพธ์ขั้นต่ำ
1	**กำกับดูแลและกำหนดบริบท**	ขอบเขตการประเมินคืออะไร ใครรับผิดชอบ และปัจจัยภายในหรือภายนอกใดอาจส่งผลต่อวัตถุประสงค์	ขอบเขต ระยะเวลา บริบท ผู้มีส่วนได้ส่วนเสีย สมมติฐาน บทบาท และอำนาจตัดสินใจ
2	**กำหนดวัตถุประสงค์และเกณฑ์ความเสี่ยง**	ต้องบรรลุผลลัพธ์ใด ใช้ตัวชี้วัดอะไร และยอมรับความเสี่ยงได้เพียงใด	Objective, KPI, Risk Capacity, RA, RT เกณฑ์ประเมิน และ Trigger
3	**ระบุความเสี่ยงและโอกาส**	เหตุการณ์หรือความไม่แน่นอนใดอาจเกิดขึ้น เกิดจากปัจจัยใด และส่งผลต่อวัตถุประสงค์อย่างไร	Risk Statement, Cause/Risk Driver, Risk Event, Impact, Risk Owner และ Risk Register
4	**วิเคราะห์และประเมินความเสี่ยง**	ระดับความเสี่ยงก่อนและหลังพิจารณาการควบคุมเป็นเท่าใด การควบคุมมีประสิทธิผลหรือไม่ และเกิน RA/RT หรือไม่	Inherent Risk, Control Effectiveness, Residual Risk การจัดลำดับ และประเด็นที่ต้องยกระดับ
5	**ตอบสนองและจัดทำแผนบริหารความเสี่ยง**	จะหลีกเลี่ยง ลดหรือควบคุม แบ่งปันหรือถ่ายโอน ยอมรับ หรือใช้ประโยชน์จากโอกาส ใครรับผิดชอบ และต้องลดความเสี่ยงเหลือเท่าใด	Risk Response, Risk Treatment Plan, Action Owner, ทรัพยากร กำหนดเวลา และ Target Residual Risk
6	**ดำเนินการควบคุมและมาตรการ**	การควบคุมและมาตรการได้รับการดำเนินการจริงหรือไม่ และลดสาเหตุโอกาสเกิด หรือผลกระทบได้เพียงใด	หลักฐานการปฏิบัติ ผลการทดสอบการควบคุม สถานะมาตรการ ข้อบกพร่อง และ Corrective Action
7	**สื่อสาร รายงาน และยกระดับ**	ใครต้องได้รับข้อมูล เมื่อใด ประเด็นใดต้องตัดสินใจ และเข้าเกณฑ์รายงานเร่งด่วนหรือไม่	KRI/EWS, Dashboard, Risk Report, Incident/Escalation Record และ Decision Log
8	**ติดตาม ทบทวน และปรับปรุงอย่างต่อเนื่อง**	บริบทและระดับความเสี่ยงเปลี่ยนแปลงหรือไม่ มาตรการได้ผลตามเป้าหมายหรือไม่ และต้องปรับปรุงเรื่องใด	Updated Risk Register, Risk Profile/Portfolio, Management Review, Lessons Learned และ Improvement Plan

กระบวนการบริหารความเสี่ยง:

กำกับดูแลและบริบท ⟶ วัตถุประสงค์และเกณฑ์ ⟶ ระบุ ⟶ วิเคราะห์และประเมิน ⟶ ตอบสนอง ⟶ ดำเนินการ ⟶ สื่อสารและยกระดับ ⟶ ติดตามและปรับปรุง ⟶ ย้อนกลับสู่บริบทและวัตถุประสงค์

ขั้นตอนที่ 1 กำกับดูแลและกำหนดบริบท *(Governance and Context Setting)*

ขั้นตอนนี้เป็นการกำหนดรากฐานและขอบเขตของการประเมิน เพื่อให้ผู้เกี่ยวข้องมีความเข้าใจตรงกันว่ากำลังบริหารความเสี่ยงของวัตถุประสงค์ กระบวนงาน โครงการ หรือพันธกิจใด ภายในช่วงเวลาและเงื่อนไขใด

1.1 สิ่งที่ต้องกำหนด

1) **ระดับและขอบเขตการประเมิน:** ระดับมหาวิทยาลัย ส่วนงาน กระบวนงาน โครงการ ระบบ หรือกิจกรรม

2) **ช่วงเวลาที่ประเมิน (Time Horizon):** เช่น ปีงบประมาณ ระยะเวลาของแผนยุทธศาสตร์ หรืออายุโครงการ

3) **ผู้รับผิดชอบต่อวัตถุประสงค์:** Objective Owner และผู้มีอำนาจกำกับหรือตัดสินใจ

4) **ผู้มีส่วนได้ส่วนเสีย:** ผู้เรียน บุคลากร ผู้ปกครอง ชุมชน คู่ความร่วมมือ ผู้ให้ทุน หน่วยงานกำกับดูแล และผู้เกี่ยวข้องอื่น

5) **บริบทภายใน:** โครงสร้าง บุคลากร กระบวนการ ระบบข้อมูล เทคโนโลยี การเงิน ทรัพย์สิน วัฒนธรรม และการควบคุมที่เกี่ยวข้อง

6) **บริบทภายนอก:** กฎหมาย นโยบาย เศรษฐกิจ สังคม เทคโนโลยี สิ่งแวดล้อม การแข่งขัน และความคาดหวังของผู้มีส่วนได้ส่วนเสีย

7) **สมมติฐานและข้อจำกัด:** ข้อมูลที่ใช้ สมมติฐานสำคัญ ข้อจำกัดด้านงบประมาณ บุคลากร เวลา เทคโนโลยี และข้อผูกพันตามกฎหมายหรือสัญญา

8) **โครงสร้างการกำกับและการรายงาน:** ผู้มีอำนาจตัดสินใจ อำนาจยอมรับความเสี่ยง เส้นทางรายงาน และเกณฑ์การยกระดับ

1.2 ปัจจัยบริบทที่ควรพิจารณา

ปัจจัยที่นำมาวิเคราะห์ควรครอบคลุมอย่างน้อย

- นโยบายและกฎหมายด้านการอุดมศึกษา
- วิสัยทัศน์และแผนยุทธศาสตร์ของมหาวิทยาลัย
- โครงสร้างประชากรและแนวโน้มจำนวนนักศึกษา
- ความต้องการของผู้เรียนและตลาดแรงงาน
- การแข่งขันด้านการศึกษา การวิจัย และนวัตกรรม
- ปัญญาประดิษฐ์และเทคโนโลยีดิจิทัล
- ความมั่นคงปลอดภัยไซเบอร์และ PDPA
- ฐานะการเงิน รายได้ ต้นทุน และข้อจำกัดด้านงบประมาณ
- สมรรถนะบุคลากรและโครงสร้างองค์กร
- ผู้รับจ้าง ผู้ให้บริการ ระบบหรือบุคคลภายนอกที่พึ่งพา
- การเปลี่ยนแปลงสภาพภูมิอากาศ ESG และความปลอดภัย

- ชื่อเสียง ความเชื่อมั่น และความคาดหวังของผู้มีส่วนได้ส่วนเสีย
- เหตุการณ์ที่ผ่านมา ข้อร้องเรียน Near Miss และข้อสังเกตจากการตรวจสอบ

1.3 ผลลัพธ์ขั้นต่ำ

ผลลัพธ์ของขั้นตอนที่ 1 ต้องประกอบด้วย

- ขอบเขตและช่วงเวลาการประเมิน
- เจ้าของวัตถุประสงค์
- ผู้มีส่วนได้ส่วนเสียสำคัญ
- ปัจจัยบริบทภายในและภายนอก
- สมมติฐานและข้อจำกัด
- โครงสร้างการกำกับและอำนาจตัดสินใจ
- แหล่งข้อมูลที่ต้องใช้
- กำหนดการและผู้ประสานงานการประเมิน

ในขั้นตอนนี้อาจกำหนด Risk Owner เบื้องต้นตามเจ้าของวัตถุประสงค์หรือกระบวนการ แต่ต้องยืนยันอีกครั้งเมื่อระบุความเสี่ยงในขั้นตอนที่ 3 ส่วน Action Owner ให้กำหนดในขั้นตอนที่ 5 หลังจากเลือกมาตรการแล้ว

ขั้นตอนที่ 2 กำหนดวัตถุประสงค์และเกณฑ์ความเสี่ยง *(Objectives and Risk Criteria)*

การระบุความเสี่ยงต้องเริ่มจากวัตถุประสงค์ที่ชัดเจน เนื่องจากความเสี่ยงหมายถึงผลกระทบของความไม่แน่นอนต่อวัตถุประสงค์ หากไม่ทราบว่าต้องบรรลุผลลัพธ์ใด จะไม่สามารถระบุ ประเมิน หรือจัดลำดับความเสี่ยงได้อย่างเหมาะสม

2.1 การกำหนดวัตถุประสงค์

วัตถุประสงค์ควร

- เชื่อมโยงกับวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ หรือภารกิจ
- ระบุผลลัพธ์ที่ต้องการอย่างชัดเจน
- มี KPI และค่าเป้าหมาย
- กำหนดช่วงเวลาและขอบเขต
- ระบุเจ้าของวัตถุประสงค์
- สามารถใช้เป็นฐานในการระบุและประเมินความเสี่ยงได้

2.2 การกำหนดเกณฑ์ความเสี่ยง

มหาวิทยาลัยและส่วนงานต้องกำหนดหรือประยุกต์ใช้เกณฑ์ที่เกี่ยวข้อง ได้แก่

1. ความสามารถในการรองรับความเสี่ยง (Risk Capacity)
2. ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA)
3. ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT)
4. เกณฑ์โอกาสเกิด (Likelihood Criteria)
5. เกณฑ์ผลกระทบ (Impact Criteria)
6. ตารางระดับความเสี่ยง (Risk Matrix)
7. เกณฑ์ยกระดับเป็นกรณีพิเศษ (Override Criteria)
8. จุดเตือนหรือเงื่อนไขการดำเนินการ (Trigger/Action)
9. ผู้มีอำนาจยอมรับและยกระดับความเสี่ยง
10. ความถี่และเส้นทางการติดตามรายงาน

Risk Capacity และ Risk Appetite ระดับมหาวิทยาลัยต้องเป็นไปตามกรอบที่ได้รับอนุมัติ ส่วนงานมีหน้าที่นำกรอบดังกล่าวไปกำหนด RT และ Trigger ที่เหมาะสมกับวัตถุประสงค์ของตน โดยส่วนงานอาจกำหนดเกณฑ์ที่เข้มงวดกว่า แต่ต้องไม่ผ่อนคลายข้อห้ามหรือ Zero Tolerance ของมหาวิทยาลัย

2.3 ความเชื่อมโยงระหว่าง KPI, RA/RT และ KRI

- **KPI** แสดงว่าผลการดำเนินงานบรรลุวัตถุประสงค์หรือไม่
- **KRI** แสดงระดับ แนวโน้ม หรือปัจจัยขับเคลื่อนความเสี่ยง
- **RA** แสดงระดับความเสี่ยงที่มหาวิทยาลัยยินดีรับ
- **RT** แสดงขอบเขตความเบี่ยงเบนที่ต้องเฝ้าระวังหรือดำเนินการ
- **Trigger/Action** กำหนดว่าเมื่อใด ใครต้องดำเนินการ และต้องดำเนินการอย่างไร

ความเชื่อมโยงควรแสดงให้เห็นอย่างน้อยดังนี้

วัตถุประสงค์ ⟶ KPI และเป้าหมาย ⟶ ความเสี่ยง ⟶ KRI ⟶ RA/RT ⟶ Trigger/Action ⟶ ผู้มีอำนาจตัดสินใจ

ขั้นตอนที่ 3 ระบุความเสี่ยงและโอกาส *(Risk and Opportunity Identification)*

เป็นการค้นหาเหตุการณ์หรือความไม่แน่นอนที่อาจส่งผลต่อการบรรลุวัตถุประสงค์ทั้งในด้านลบและด้านบวก โดยต้องระบุให้ชัดเจนว่า ความเสี่ยงนั้นเชื่อมโยงกับวัตถุประสงค์ ผลลัพธ์ หรือ KPI ใด

การเขียนข้อความความเสี่ยง (Risk Statement) ให้ใช้โครงสร้าง

เนื่องจาก [สาเหตุหรือปัจจัยขับเคลื่อน] ⟶ อาจทำให้เกิด [เหตุการณ์หรือความไม่แน่นอน] ⟶ ส่งผลต่อ [วัตถุประสงค์หรือผู้มีส่วนได้ส่วนเสีย]

ตัวอย่าง

เนื่องจากมหาวิทยาลัยยังไม่มีโครงสร้างกำกับดูแล AI และข้อมูลที่เป็นมาตรฐานเดียวกัน อาจทำให้การนำ AI ไปใช้ไม่เหมาะสม ไม่ปลอดภัย หรือไม่ทันต่อการเปลี่ยนแปลง ส่งผลต่อคุณภาพการศึกษา ประสิทธิภาพการดำเนินงาน ความสามารถในการแข่งขัน การคุ้มครองข้อมูล และการปฏิบัติตามกฎหมาย

แหล่งข้อมูลสำหรับการระบุความเสี่ยง

ควรใช้ข้อมูลจากหลายแหล่งเพื่อให้ครอบคลุมและลดอคติ ได้แก่

- แผนยุทธศาสตร์ วัตถุประสงค์ KPI และผลการดำเนินงาน
- KRI สัญญาณเตือนล่วงหน้า และการวิเคราะห์แนวโน้ม
- เหตุการณ์ที่ผ่านมา เหตุการณ์เกือบเกิดความเสียหาย (Near Miss) และบทเรียน
- ข้อร้องเรียน ข้อพิพาท คดี และข้อมูลจากผู้มีส่วนได้ส่วนเสีย
- ผลการประเมินการควบคุมและข้อสังเกตจากการตรวจสอบ
- การเปลี่ยนแปลงกฎหมาย นโยบาย มาตรฐาน และข้อกำหนด
- ข้อมูลคู่เทียบ แนวโน้มอุตสาหกรรม และแนวปฏิบัติของสถาบันอุดมศึกษา
- การวิเคราะห์ข้อมูล สถานการณ์จำลอง และความเห็นของผู้เชี่ยวชาญ
- ความเสี่ยงจากผู้รับจ้าง ผู้ให้บริการ พันธมิตร และบุคคลภายนอก
- ปัจจัย ESG ความปลอดภัย ชื่อเสียง และความต่อเนื่องของพันธกิจ

ข้อกำหนดในการระบุความเสี่ยง

1. ไม่เขียนความเสี่ยงเป็นเพียงปัญหาที่เกิดขึ้นแล้ว เช่น “บุคลากรไม่เพียงพอ” แต่ต้องระบุว่าอาจทำให้เกิดเหตุการณ์ใดและกระทบวัตถุประสงค์อย่างไร
2. ไม่เขียนเป็นเพียงผลกระทบ เช่น “ชื่อเสียงเสียหาย” โดยไม่ระบุสาเหตุและเหตุการณ์ที่อาจนำไปสู่ผลกระทบ
3. แยกความเสี่ยงออกจากการควบคุมหรือมาตรการ เช่น “จัดอบรมไม่ครบ” อาจเป็นข้อบกพร่องของมาตรการ ไม่ใช่เหตุการณ์ความเสี่ยงโดยตัวเอง
4. กำหนดประเภทความเสี่ยงหลักหนึ่งประเภท และระบุประเภทหรือมิติผลกระทบที่เกี่ยวข้องเพิ่มเติมได้
5. กำหนดเจ้าของความเสี่ยงหลัก (Lead Risk Owner) ซึ่งมีอำนาจเพียงพอในการตัดสินใจและประสานการจัดการความเสี่ยง
6. พิจารณาความสัมพันธ์กับความเสี่ยงอื่น ความเสี่ยงเกิดใหม่ และโอกาสที่อาจใช้สร้างคุณค่า

ผลลัพธ์ขั้นต่ำ

- รหัสและชื่อความเสี่ยง
- วัตถุประสงค์ที่ได้รับผลกระทบ
- สาเหตุหรือปัจจัยขับเคลื่อน
- เหตุการณ์ความเสี่ยง

- ผลกระทบที่อาจเกิดขึ้น
- ประเภทความเสี่ยงหลักและมิติผลกระทบร่วม
- Risk Owner และผู้เกี่ยวข้อง
- การควบคุมที่มีอยู่เบื้องต้น
- แหล่งข้อมูลและหลักฐาน
- ความสัมพันธ์กับความเสี่ยงอื่น
- รายการความเสี่ยงใน Risk Register

ขั้นตอนที่ 4 วิเคราะห์และประเมินความเสี่ยง *(Risk Analysis and Evaluation)*

เป็นการทำความเข้าใจลักษณะและระดับของความเสี่ยง เพื่อเปรียบเทียบกับ RA/RT จัดลำดับความสำคัญ เลือกแนวทางตอบสนอง และพิจารณาว่าต้องยกระดับรายงานหรือไม่

มหาวิทยาลัยใช้สูตรพื้นฐาน

คะแนนความเสี่ยง (Risk Score) = โอกาสเกิด (Likelihood) × ผลกระทบ (Impact)

อย่างไรก็ตาม คะแนนเป็นเพียงองค์ประกอบหนึ่งของการพิจารณา ต้องใช้ข้อมูลเชิงคุณภาพ เกณฑ์ Override ความเร่งด่วน ความสัมพันธ์ของความเสี่ยง และข้อจำกัดตามกฎหมายร่วมด้วย

ระดับความเสี่ยงที่ต้องประเมิน

1. **ความเสี่ยงโดยธรรมชาติ (Inherent Risk):** ระดับความเสี่ยงก่อนพิจารณาผลของการควบคุมหรือมาตรการที่มีอยู่
2. **ความเสี่ยงคงเหลือ (Residual Risk):** ระดับความเสี่ยงภายหลังพิจารณาเฉพาะการควบคุมที่มีหลักฐานว่าได้รับการนำไปใช้และทำงานจริง
3. **ความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk):** ระดับความเสี่ยงที่คาดว่าจะเหลือภายหลังดำเนินมาตรการเพิ่มเติมครบถ้วนและมีประสิทธิผลภายในเวลาที่กำหนด

การวิเคราะห์ความเสี่ยง *ต้องพิจารณาอย่างน้อย ดังนี้*

- สาเหตุและปัจจัยขับเคลื่อนความเสี่ยง
- โอกาสเกิดหรือความถี่
- ผลกระทบในแต่ละมิติ
- ความเร็วในการเกิดผลกระทบ (Risk Velocity)
- ระยะเวลาหรือความต่อเนื่องของผลกระทบ
- ความสัมพันธ์และการกระจุกตัวของความเสี่ยง
- ความไม่แน่นอน สมมติฐาน และข้อจำกัดของข้อมูล

- ประสิทธิผลของการควบคุมที่มีอยู่
- ความสามารถในการตรวจพบและตอบสนอง
- ผลกระทบต่อผู้มีส่วนได้ส่วนเสีย

กรณีมีผลกระทบหลายมิติ ให้บันทึกผลกระทบทุกมิติที่เกี่ยวข้อง และใช้ระดับผลกระทบสูงสุดที่มีเหตุผลและหลักฐานรองรับในการคำนวณคะแนน เว้นแต่เกณฑ์เฉพาะด้านกำหนดไว้เป็นอย่างอื่น

การประเมินประสิทธิผลของการควบคุม *ให้ประเมินอย่างน้อย 3 มิติ ได้แก่*

1. ความเหมาะสมของการออกแบบ (Design Adequacy)
2. การนำไปใช้จริง (Implementation)
3. ประสิทธิผลในการปฏิบัติงาน (Operating Effectiveness)

หากการควบคุมยังไม่มีหลักฐาน ไม่ได้ดำเนินการอย่างต่อเนื่อง หรือไม่สามารถยืนยันประสิทธิผลได้ ต้องไม่ลดคะแนน Residual Risk โดยอาศัยการควบคุมนั้น

มาตรการที่ยังเป็นเพียงแผนให้ใช้ประกอบการกำหนด Target Residual Risk เท่านั้น ไม่ให้นำมาลดคะแนน Residual Risk ปัจจุบัน

การประเมินและจัดลำดับความสำคัญ *ภายหลังการวิเคราะห์ ต้องพิจารณา*

- ระดับความเสี่ยงเทียบกับ Risk Matrix
- ความสอดคล้องกับ RA/RT
- KRI และแนวโน้ม
- เกณฑ์ Override
- เหตุ Zero Tolerance
- ความสำคัญเชิงยุทธศาสตร์
- ความเร่งด่วนและความเร็วในการเกิดผลกระทบ
- อำนาจและทรัพยากรที่ต้องใช้
- ความเสี่ยงที่อาจเกิดจากมาตรการตอบสนอง

ผลลัพธ์ขั้นต่ำประกอบด้วย Inherent Risk, ผลการประเมินการควบคุม, Residual Risk, Target Residual Risk เบื้องต้น ลำดับความสำคัญ และข้อเสนอว่าต้องตอบสนอง ยอมรับ หรือต้องยกระดับหรือไม่

ขั้นตอนที่ 5 ตอบสนองและจัดทำแผนบริหารความเสี่ยง *(Risk Response and Treatment Planning)*

Risk Owner ต้องเสนอแนวทางตอบสนองที่เหมาะสม โดยพิจารณาระดับความเสี่ยง RA/RT ข้อจำกัดตามกฎหมาย ต้นทุนและประโยชน์ ความเป็นไปได้ ทรัพยากร ผลกระทบต่อผู้มีส่วนได้ส่วนเสีย และความเสี่ยงที่อาจเกิดขึ้นใหม่จากมาตรการ

การเลือกและยอมรับแนวทางตอบสนองต้องได้รับอนุมัติจากผู้มีอำนาจตามระดับความเสี่ยง

แนวทางตอบสนอง

1. **หลีกเลี่ยง (Avoid):** ยุติ ไม่เริ่ม หรือเปลี่ยนแปลงกิจกรรมที่เป็นแหล่งของความเสี่ยง โดยต้องพิจารณาผลกระทบต่อวัตถุประสงค์และโอกาสที่อาจสูญเสียไปด้วย
2. **ลดหรือควบคุม (Reduce):** ดำเนินมาตรการเพื่อลดโอกาสเกิด ลดผลกระทบ เพิ่มความสามารถในการตรวจพบ หรือเพิ่มความพร้อมในการตอบสนองและฟื้นตัว
3. **แบ่งปันหรือถ่ายโอน (Share/Transfer):** แบ่งภาระหรือผลกระทบกับบุคคลอื่น เช่น การประกันภัย สัญญา การร่วมลงทุน หรือการใช้ผู้ให้บริการ ทั้งนี้ การถ่ายโอนไม่ทำให้มหาวิทยาลัยพ้นจากความรับผิดตามกฎหมายหรือความรับผิดชอบต่อความเสี่ยงคงเหลือ
4. **ยอมรับ (Accept):** ยอมรับความเสี่ยงภายใน RA/RT และอำนาจที่ได้รับมอบหมาย โดยมีเหตุผลหลักฐาน เงื่อนไข KRI และระยะเวลาทบทวนที่ชัดเจน
5. **ใช้ประโยชน์หรือเพิ่มโอกาส (Pursue/Enhance):** ตัดสินใจรับหรือเพิ่มระดับความเสี่ยงอย่างมีข้อมูล เพื่อใช้ประโยชน์จากโอกาส สร้างนวัตกรรม หรือเพิ่มคุณค่า โดยยังอยู่ภายในกรอบการกำกับดูแลและ RA/RT

อาจเลือกใช้หลายแนวทางร่วมกัน หากแนวทางเดียวไม่เพียงพอต่อการจัดการความเสี่ยง

ข้อกำหนดของแผนบริหารความเสี่ยง Risk Treatment Plan ต้องระบุอย่างน้อย

1. ความเสี่ยงและสาเหตุหรือปัจจัยขับเคลื่อนที่ต้องจัดการ
2. วัตถุประสงค์ของมาตรการ
3. มาตรการหรือกิจกรรมที่ต้องดำเนินการ
4. เจ้าของมาตรการ (Action Owner) และผู้ร่วมดำเนินการ
5. ทรัพยากรและงบประมาณ
6. วันที่เริ่มต้น วันที่แล้วเสร็จ และ Milestone
7. ผลผลิตและหลักฐานที่ต้องส่งมอบ
8. KPI, KCI หรือ KRI ที่ใช้ติดตามผล
9. ระดับความเสี่ยงปัจจุบันและ Target Residual Risk
10. ผลที่คาดว่าจะลดโอกาสเกิดหรือผลกระทบ
11. ความสัมพันธ์หรือการพึ่งพามาตรการอื่น
12. ความเสี่ยงใหม่หรือผลข้างเคียงจากการดำเนินมาตรการ
13. Trigger และแนวทางแก้ไขกรณีมาตรการล่าช้าหรือไม่เกิดผล
14. ผู้มีอำนาจอนุมัติและรอบการรายงาน

มาตรการต้องตอบสนองต่อสาเหตุหรือปัจจัยขับเคลื่อนอย่างชัดเจน มิใช่เป็นเพียงกิจกรรมทั่วไปที่ไม่สามารถอธิบายได้ว่าจะช่วยลดความเสี่ยงอย่างไร

ข้อกำหนดตามระดับความเสี่ยง

- **ระดับต่ำ:** อาจยอมรับและติดตามผ่านการควบคุมตามปกติ
- **ระดับปานกลาง:** กำหนดมาตรการตามความเหมาะสมและติดตามโดย Risk Owner
- **ระดับสูง:** ต้องมี Risk Treatment Plan เป็นลายลักษณ์อักษร พร้อมกำหนดเวลาและรายงานฝ่ายบริหาร
- **ระดับสูงมาก:** ต้องยกระดับทันที ดำเนินมาตรการเร่งด่วน และติดตามอย่างใกล้ชิด
- **เหตุ Zero Tolerance:** ไม่สามารถยอมรับเป็นการดำเนินงานตามปกติ ต้องระงับเหตุ รายงาน รักษาหลักฐาน ตรวจสอบ แก้ไข และดำเนินการตามกฎหมายหรือนโยบายที่เกี่ยวข้องโดยไม่ชักช้า

ขั้นตอนที่ 6 ดำเนินการควบคุมและมาตรการ *(Implement Controls and Risk Treatment Actions)*

เป็นขั้นตอนนำแผนบริหารความเสี่ยงไปสู่การปฏิบัติ โดยมีความรับผิดชอบสำคัญ ดังนี้

- **Risk Owner:** รับผิดชอบกำกับภาพรวม ตัดสินใจ แก้ไขอุปสรรค และรับผิดชอบต่อผลการบริหารความเสี่ยง
- **Control Owner:** รับผิดชอบดำเนินการควบคุมที่มีอยู่ให้ทำงานอย่างต่อเนื่องตามรูปแบบและความถี่ที่กำหนด
- **Action Owner:** รับผิดชอบดำเนินมาตรการเพิ่มเติมตามขอบเขต ทรัพยากร Milestone และระยะเวลาที่ได้รับอนุมัติ
- **Data Owner:** รับผิดชอบคุณภาพ ความครบถ้วน และความทันเวลาของข้อมูลที่ใช้ติดตามผล

6.1 การดำเนินการและหลักฐาน

ผู้รับผิดชอบต้องจัดเก็บหลักฐานที่เพียงพอ เหมาะสม และตรวจสอบย้อนกลับได้ เช่น

- คำสั่ง ประกาศ นโยบาย ระเบียบ หรือแนวปฏิบัติ
- เอกสารอนุมัติและหลักฐานการมอบหมายผู้รับผิดชอบ
- รายงานการดำเนินโครงการและผลส่งมอบ
- รายงานผลการทดสอบระบบหรือการควบคุม
- บันทึกเหตุการณ์ (Log) หรือข้อมูลจากระบบสารสนเทศ
- รายงานการสำรองและกู้คืนข้อมูล
- รายงานการซ้อม BCP/DRP และผลการแก้ไขช่องว่าง
- หลักฐานการอบรม ผลการทดสอบ และการประเมินการนำความรู้ไปใช้
- รายงานข้อยกเว้น ข้อบกพร่อง และการแก้ไข
- KCI, KRI หรือข้อมูลผลลัพธ์ที่แสดงถึงประสิทธิผลของมาตรการ
- หลักฐานการสื่อสารและการรับทราบของกลุ่มเป้าหมาย

การมีนโยบาย ระเบียบ คู่มือ ระบบ หรือการจัดกิจกรรมเพียงอย่างเดียวไม่เพียงพอที่จะสรุปว่าการควบคุมมีประสิทธิผล ต้องมีหลักฐานว่าการควบคุมได้รับการนำไปใช้จริง ทำงานอย่างสม่ำเสมอ ครอบคลุมตามขอบเขต และสามารถลดโอกาสเกิดหรือผลกระทบของความเสี่ยงได้ตามวัตถุประสงค์

6.2 การติดตามสถานะมาตรการ

สถานะมาตรการควรจำแนกอย่างน้อย ดังนี้

ตารางที่ 4-3 *สถานะและความหมายในการติดตามการดำเนินงาน*

สถานะ	ความหมาย
ยังไม่เริ่ม (Not Started)	ยังไม่มีการดำเนินงานหรือหลักฐานตามแผน
อยู่ระหว่างดำเนินการ–เป็นไปตามแผน (In Progress–On Track)	ดำเนินการแล้วและมีแนวโน้มแล้วเสร็จตามกำหนด
อยู่ระหว่างดำเนินการ–เสี่ยงล่าช้า (At Risk)	พบอุปสรรคหรือแนวโน้มที่อาจทำให้ไม่บรรลุ Milestone
ล่าช้า (Delayed/Overdue)	ไม่แล้วเสร็จภายในกำหนดและต้องมี Corrective Action
ดำเนินการแล้วเสร็จ (Completed)	ผลผลิตหรือกิจกรรมแล้วเสร็จและมีหลักฐาน แต่ยังอาจต้องประเมินประสิทธิผล
ตรวจสอบแล้วว่ามีประสิทธิผล (Verified Effective)	มีหลักฐานหรือผลการทดสอบยืนยันว่ามาตรการทำงานและลดความเสี่ยงได้ตามเป้าหมาย
ยุติหรือเปลี่ยนแปลง (Closed/Revised)	ได้รับอนุมัติให้ยุติ เปลี่ยน หรือทดแทนมาตรการ พร้อมบันทึกเหตุผล

การรายงานว่า “แล้วเสร็จ” ต้องแยกระหว่างความสำเร็จของกิจกรรม (Completion) กับประสิทธิผลในการลดความเสี่ยง (Effectiveness)

6.3 การปรับระดับความเสี่ยง

ห้ามลดระดับ Residual Risk เพียงเพราะมาตรการมีสถานะดำเนินการแล้วเสร็จ การปรับลดต้องมีหลักฐานอย่างน้อยว่า

1. มาตรการได้รับการนำไปใช้ครบถ้วน
2. การควบคุมทำงานจริงตามระยะเวลาที่เพียงพอ
3. KCI หรือผลการทดสอบเป็นไปตามเกณฑ์
4. KRI หรือระดับความเสี่ยงมีแนวโน้มดีขึ้น
5. ไม่มีข้อยกเว้นหรือผลข้างเคียงที่มีนัยสำคัญ

6. Risk Owner ได้ทบทวนและรับรองผลการประเมิน

หากมาตรการล่าช้า ไม่เพียงพอ หรือก่อให้เกิดความเสี่ยงใหม่ ต้องกำหนด Corrective Action และยกระดับตามเกณฑ์ที่กำหนด

ขั้นตอนที่ 7 สื่อสาร รายงาน และยกระดับ *(Communicate, Report and Escalate)*

การสื่อสารและรายงานเป็นกิจกรรมที่ต้องดำเนินการตลอดกระบวนการบริหารความเสี่ยง เพื่อให้ผู้เกี่ยวข้องได้รับข้อมูลที่เหมาะสมกับบทบาทและสามารถตัดสินใจได้อย่างทันเวลา

7.1 สาระขั้นต่ำของรายงาน

รายงานความเสี่ยงควรแสดงอย่างน้อย

1. วัตถุประสงค์หรือผลลัพธ์ที่ได้รับผลกระทบ
2. ระดับความเสี่ยงปัจจุบันและการเปลี่ยนแปลงจากรอบก่อน
3. Inherent Risk, Residual Risk และ Target Residual Risk
4. ผลและแนวโน้ม KRI เทียบกับ RA/RT
5. สัญญาณเตือนล่วงหน้าและการคาดการณ์
6. ประสิทธิผลของการควบคุมและข้อบกพร่องสำคัญ
7. ความก้าวหน้า ประสิทธิผล และสถานะของมาตรการ
8. เหตุการณ์ Near Miss ข้อร้องเรียน และความเสียหายที่เกิดขึ้น
9. ความเสี่ยงเกิดใหม่ ความสัมพันธ์ และผลกระทบข้ามส่วนงาน
10. ประเด็นที่เกินอำนาจหรือทรัพยากรของ Risk Owner
11. ทางเลือก ข้อเสนอ และประเด็นที่ต้องการการตัดสินใจ
12. ผู้รับผิดชอบ กำหนดเวลา และรอบติดตามครั้งถัดไป

รายงานต้องแยกให้ชัดระหว่างข้อเท็จจริง ข้อมูลประมาณการ สมมติฐาน และความเห็นของผู้ประเมิน พร้อมระบุข้อจำกัดด้านคุณภาพข้อมูลตามความเหมาะสม

7.2 ระดับและรูปแบบการรายงาน

รูปแบบและรายละเอียดของรายงานให้เหมาะสมกับผู้รับ ดังนี้

- **ระดับปฏิบัติการ:** เน้นสถานะการควบคุม มาตรการ ข้อยกเว้น และงานที่ต้องดำเนินการ
- **ระดับส่วนงาน:** เน้น Risk Register, KRI, RA/RT ทรัพยากร และประเด็นที่ต้องตัดสินใจ
- **ระดับฝ่ายบริหาร:** เน้นแนวโน้ม ความเสี่ยงสำคัญ Portfolio View ความสัมพันธ์ และทางเลือกเชิงบริหาร
- **ระดับผู้กำกับดูแล:** เน้นความเสี่ยงเชิงยุทธศาสตร์ ความเสี่ยงเกิน RA เหตุสำคัญ ความเพียงพอของระบบ และผลการให้ความเชื่อมั่น

ข้อมูลที่มีความอ่อนไหว เช่น ข้อมูลส่วนบุคคล เหตุทุจริต เหตุคุกคามทางเพศ หรือเหตุการณ์ไซเบอร์ ต้องจำกัดการเข้าถึงและเปิดเผยเท่าที่จำเป็นตามกฎหมายและอำนาจหน้าที่

7.3 ระยะเวลาและการยกระดับ

ระยะเวลา เส้นทาง และสาระขั้นต่ำของการรายงานให้เป็นไปตาม ***ตารางการรายงานและการยกระดับ (Reporting and Escalation Matrix) ในข้อ 3.6*** *ซึ่งเป็นเกณฑ์อ้างอิงหลัก* สรุประยะเวลา ได้แก่

ตารางที่ 4-5 *องค์ประกอบและตัวอย่างการกำหนดเกณฑ์ความเสี่ยง*

เงื่อนไข	ระยะเวลารายงาน
Zero Tolerance เหตุวิกฤต หรือผลกระทบระดับ 5	แจ้งทันที และรายงานเบื้องต้นไม่เกิน 24 ชั่วโมง
ความเสี่ยงสูงมาก 16–25	ทันทีและไม่เกิน 24 ชั่วโมง
ความเสี่ยงสูง 10–15 หรือ KRI เกิน RT	ภายใน 3 วันทำการ หรือเร็วกว่าตาม Trigger
ความเสี่ยงปานกลาง 5–9	อย่างน้อยรายไตรมาส
ความเสี่ยงต่ำ 1–4	ตามรอบการบริหารงานปกติ

การรายงานไม่ทดแทนการระงับเหตุหรือการดำเนินการเร่งด่วนเพื่อคุ้มครองชีวิต สุขภาพ ข้อมูล ระบบ ทรัพย์สิน สิ่งแวดล้อม และความต่อเนื่องของพันธกิจ

การตัดสินใจที่เกิดจากการรายงานต้องบันทึกใน Decision Log โดยระบุผู้ตัดสินใจ วันที่ ข้อมูลที่ใช้ ทางเลือก เหตุผล เงื่อนไข ผู้รับผิดชอบ และกำหนดเวลาทบทวน

ขั้นตอนที่ 8 ติดตาม ทบทวน และปรับปรุงอย่างต่อเนื่อง *(Monitor, Review and Continually Improve)*

การติดตามและทบทวนมีวัตถุประสงค์เพื่อประเมินว่า

- บริบท สมมติฐาน หรือวัตถุประสงค์เปลี่ยนแปลงหรือไม่
- ระดับและแนวโน้มของความเสี่ยงเปลี่ยนแปลงอย่างไร
- การควบคุมและมาตรการดำเนินการครบถ้วนและมีประสิทธิผลหรือไม่
- Target Residual Risk ยังมีความเหมาะสมและสามารถบรรลุได้หรือไม่
- มีความเสี่ยงใหม่ ความสัมพันธ์ หรือผลกระทบข้ามส่วนงานเกิดขึ้นหรือไม่
- ต้องปรับการตัดสินใจ การจัดสรรทรัพยากร หรือการยกระดับหรือไม่

8.1 การติดตามตามรอบ

Risk Owner ต้องติดตามตามความถี่ที่กำหนดใน Risk Register โดยพิจารณาระดับความเสี่ยง ความเร็วในการเปลี่ยนแปลง KRI ความสำคัญของการควบคุม และความเร่งด่วนของมาตรการ

8.2 เหตุที่ต้องทบทวนนอกเหนือจากรอบปกติ

ต้องทบทวนเมื่อเกิดกรณีอย่างน้อยหนึ่งข้อ ดังนี้

1. KRI เข้าใกล้หรือเกิน RT หรือมีแนวโน้มเสื่อมลง
2. เกิดเหตุการณ์หรือ Near Miss ที่มีนัยสำคัญ
3. การควบคุมสำคัญไม่ทำงานหรือพบข้อยกเว้นเพิ่มขึ้น
4. มาตรการล่าช้าหรือไม่น่าบรรลุ Target Residual Risk
5. ยุทธศาสตร์ วัตถุประสงค์ KPI โครงสร้าง หรือทรัพยากรเปลี่ยนแปลง
6. มีกฎหมาย นโยบาย มาตรฐาน หรือข้อกำหนดใหม่
7. ผลการตรวจสอบหรือการประเมินพบข้อบกพร่องที่มีนัยสำคัญ
8. เกิดความเสี่ยงใหม่หรือความเสี่ยงข้ามส่วนงาน
9. มีการเปลี่ยนแปลงระบบ เทคโนโลยี ผู้ให้บริการ หรือคู่สัญญาสำคัญ
10. เกิดเหตุฉุกเฉิน ภาวะวิกฤต หรือมีผลการทดสอบ BCM/BCP/DRP ที่ไม่เป็นไปตามเป้าหมาย

8.3 ผลลัพธ์ของการทบทวน

ผลการทบทวนต้องนำไปใช้ในการ

- ปรับข้อมูลและระดับความเสี่ยงใน Risk Register
- ปรับ KRI, KCI และสัญญาณเตือนล่วงหน้า
- เสนอปรับ RA/RT ต่อผู้มีอำนาจ หากมีเหตุผลรองรับ
- ปรับปรุงหรือเพิ่มการควบคุมและมาตรการ
- ปรับ Action Owner ทรัพยากร Milestone หรือกำหนดเวลา
- ยกระดับหรือปรับสถานะความเสี่ยงระดับมหาวิทยาลัย
- ปรับ Risk Profile และ Portfolio View
- จัดทำ Lessons Learned และ Root Cause Analysis
- จัดทำและติดตาม Improvement Plan
- ปรับยุทธศาสตร์ แผนงาน งบประมาณ หรือการจัดสรรทรัพยากรตามความจำเป็น

RA/RT จะเปลี่ยนแปลงได้ต่อเมื่อได้รับอนุมัติจากผู้มีอำนาจ ไม่ควรปรับเกณฑ์เพื่อให้ผลการดำเนินงานที่ไม่เป็นไปตามเป้าหมายกลับมาอยู่ในระดับยอมรับได้โดยไม่มีเหตุผลเชิงยุทธศาสตร์และหลักฐานรองรับ

8.4 การปิดความเสี่ยงหรือมาตรการ

การปิดความเสี่ยงหรือมาตรการต้องได้รับการพิจารณาจากผู้มีอำนาจตามระดับความเสี่ยง โดยมีหลักฐานว่า

- วัตถุประสงค์หรือเหตุผลของมาตรการได้รับการตอบสนองแล้ว
- การควบคุมได้รับการนำไปใช้และมีประสิทธิผล
- ระดับ Residual Risk อยู่ภายใน RA/RT
- ไม่มีประเด็นสำคัญที่ยังค้างดำเนินการ
- มีการกำหนดการติดตามตามปกติหรือการเฝ้าระวังต่อเนื่อง
- มีการบันทึกบทเรียนและผู้อนุมัติการปิด

ภาพที่ 4-2

ภาพแสดงกระบวนการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้ 8 ขั้นตอน (MJU 8-Step Risk Management Process)

ที่มา: มหาวิทยาลัยแม่โจ้ ประยุกต์จาก ISO 31000:2018, COSO ERM 2017 และหลักเกณฑ์กระทรวงการคลังด้านการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

กระบวนการทั้ง 8 ขั้นตอนเป็นวงจรต่อเนื่อง โดยการสื่อสารและปรึกษาหารือ การติดตามและทบทวน รวมทั้งการบันทึกและรายงาน เป็นกิจกรรมที่ดำเนินการตลอดทั้งกระบวนการ และสามารถย้อนกลับไปทบทวนขั้นตอนก่อนหน้าได้เมื่อบริบท วัตถุประสงค์ ข้อมูล หรือระดับความเสี่ยงเปลี่ยนแปลง

4.5 ขั้นตอนที่ 1 การกำกับดูแลและกำหนดบริบท *(Governance and Context Setting)*

การกำกับดูแลและกำหนดบริบทเป็นการวางรากฐานของการประเมินความเสี่ยง เพื่อให้ผู้เกี่ยวข้องเข้าใจตรงกันเกี่ยวกับวัตถุประสงค์ ขอบเขต ช่วงเวลา สมมติฐาน ผู้รับผิดชอบ ผู้มีส่วนได้ส่วนเสีย และปัจจัยที่อาจส่งผลต่อการบรรลุวัตถุประสงค์

ข้อมูลที่ใช้ต้องมีความเหมาะสมกับระดับและวัตถุประสงค์ของการประเมิน โดยไม่จำเป็นต้องจัดทำเอกสารแยกหลายชุด หากสามารถบันทึกไว้ในเอกสารกำหนดขอบเขตหรือ Risk Register ได้อย่างครบถ้วน

4.5.1 การกำหนดขอบเขต *(Scope Definition)*

ก่อนประเมินความเสี่ยง ต้องกำหนดขอบเขตให้ชัดเจนอย่างน้อย ดังนี้

1. **ระดับการประเมิน:** ระดับมหาวิทยาลัย ส่วนงาน กระบวนงาน โครงการ ระบบสารสนเทศ หรือกิจกรรม
2. **วัตถุประสงค์ของการประเมิน:** ระบุว่าการประเมินจัดทำขึ้นเพื่อสนับสนุนการตัดสินใจ การจัดทำแผน การอนุมัติโครงการ การปรับปรุงการควบคุม หรือวัตถุประสงค์อื่นใด
3. **ขอบเขตภารกิจและกระบวนงาน:** ระบุกิจกรรม หน่วยงาน ระบบ พื้นที่ หรือกลุ่มผู้มีส่วนได้ส่วนเสียที่อยู่ภายในและภายนอกขอบเขต
4. **ช่วงเวลาที่ประเมิน (Time Horizon):** เช่น ปีงบประมาณ ระยะเวลาแผนยุทธศาสตร์ อายุโครงการ หรือช่วงเวลาการเปลี่ยนแปลงที่สำคัญ
5. **ขอบเขตผลกระทบ:** พิจารณาผลกระทบต่อยุทธศาสตร์ การเงิน การดำเนินงาน กฎหมาย ชื่อเสียง ความปลอดภัย สิ่งแวดล้อม และผู้มีส่วนได้ส่วนเสีย
6. **ความสัมพันธ์และการพึ่งพา:** ระบุส่วนงาน ระบบ ผู้รับจ้าง ผู้ให้บริการ คู่สัญญา หรือทรัพยากรที่การดำเนินงานต้องพึ่งพา
7. **ผู้มีอำนาจตัดสินใจ:** ระบุเจ้าของวัตถุประสงค์ ผู้กำกับดูแล ผู้อนุมัติ และผู้มีอำนาจยอมรับหรือยกระดับความเสี่ยง
8. **ทรัพยากรและข้อจำกัด:** ระบุข้อจำกัดด้านงบประมาณ บุคลากร เวลา ข้อมูล เทคโนโลยี กฎหมาย และข้อผูกพัน
9. **สมมติฐานและข้อยกเว้น:** ระบุสมมติฐานที่ใช้ ขอบเขตที่ไม่นำมาประเมิน และเหตุผลประกอบอย่างชัดเจน

การเปลี่ยนแปลงขอบเขตภายหลังเริ่มประเมินต้องได้รับความเห็นชอบจากเจ้าของวัตถุประสงค์หรือผู้มีอำนาจ และบันทึกเหตุผลไว้เพื่อให้ตรวจสอบย้อนกลับได้

4.5.2 การวิเคราะห์บริบทภายนอก *(External Context Analysis)*

ให้พิจารณาปัจจัยภายนอกที่อาจส่งผลต่อวัตถุประสงค์ ทั้งในลักษณะของความเสี่ยงและโอกาส โดยครอบคลุมอย่างน้อย

- นโยบายของรัฐและนโยบายด้านการอุดมศึกษา
- กฎหมาย ระเบียบ มาตรฐาน และข้อกำหนดของหน่วยงานกำกับ
- ภาวะเศรษฐกิจ การเงิน เงินเฟ้อ และแหล่งงบประมาณ
- โครงสร้างประชากร จำนวนนักศึกษา และพฤติกรรมของผู้เรียน
- ความต้องการของตลาดแรงงาน ผู้ใช้บัณฑิต และภาคอุตสาหกรรม
- การแข่งขันและความร่วมมือด้านการศึกษา การวิจัย และนวัตกรรม
- ปัญญาประดิษฐ์ เทคโนโลยีดิจิทัล และภัยคุกคามไซเบอร์
- การเปลี่ยนแปลงสภาพภูมิอากาศ ภัยพิบัติ ทรัพยากรธรรมชาติ และความหลากหลายทางชีวภาพ
- สถานการณ์ทางสังคม การเมือง และภูมิรัฐศาสตร์
- ความคาดหวังของผู้เรียน ผู้ปกครอง ชุมชน คู่ความร่วมมือ และผู้มีส่วนได้ส่วนเสีย
- ความเสี่ยงและโอกาสเกิดใหม่

เครื่องมือที่อาจนำมาใช้ ได้แก่

- PESTLE Analysis
- Scenario Analysis
- Horizon Scanning
- Environmental Scanning
- Benchmarking
- Stakeholder Consultation
- Trend and Data Analysis

การเลือกใช้เครื่องมือให้เหมาะสมกับวัตถุประสงค์และระดับความซับซ้อนของการประเมิน ไม่จำเป็นต้องใช้ทุกเครื่องมือในทุกกรณี

4.5.3 การวิเคราะห์บริบทภายใน *(Internal Context Analysis)*

ให้พิจารณาปัจจัยภายในที่อาจสนับสนุนหรือเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ โดยครอบคลุมอย่างน้อย

- วิสัยทัศน์ พันธกิจ ยุทธศาสตร์ และเป้าหมาย
- โครงสร้างการกำกับดูแลและอำนาจตัดสินใจ
- นโยบาย ระเบียบ กระบวนงาน และระบบควบคุมภายใน
- จำนวน โครงสร้าง สมรรถนะ และความพร้อมของบุคลากร

- งบประมาณ รายได้ ต้นทุน สภาพคล่อง และฐานะการเงิน
- ระบบข้อมูล คุณภาพข้อมูล เทคโนโลยี และความมั่นคงปลอดภัย
- อาคาร สถานที่ ทรัพย์สิน เครื่องมือ และโครงสร้างพื้นฐาน
- ผู้รับจ้าง ผู้ให้บริการ และการพึ่งพาบุคคลภายนอก
- วัฒนธรรมองค์กร พฤติกรรม แรงจูงใจ และการสื่อสาร
- ผลการดำเนินงานและแนวโน้ม KPI/KRI
- เหตุการณ์ Near Miss ข้อร้องเรียน ข้อพิพาท และคดี
- ผลการประเมินการควบคุม การตรวจสอบ และการประกันคุณภาพ
- ความพร้อมด้าน BCM/BCP/DRP และผลการทดสอบแผน
- บทเรียนและประเด็นที่เกิดซ้ำจากรอบก่อน

เครื่องมือที่อาจนำมาใช้ ได้แก่ SWOT Analysis, Process Mapping, Value Chain Analysis, Data Analysis, Control Self-assessment, Interviews, Workshops และ Lessons Learned

SWOT ควรใช้เป็นข้อมูลสนับสนุนการวิเคราะห์บริบท ไม่ควรนำรายการจุดอ่อนหรืออุปสรรคไปใช้เป็นข้อความความเสี่ยงโดยตรงโดยยังไม่ได้วิเคราะห์ Cause–Event–Impact

4.5.4 การวิเคราะห์ผู้มีส่วนได้ส่วนเสีย *(Stakeholder Analysis)*

ให้ระบุผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับวัตถุประสงค์หรือขอบเขตการประเมิน และพิจารณาอย่างน้อย

1. บทบาทและความสัมพันธ์กับมหาวิทยาลัย
2. ความต้องการและความคาดหวัง
3. สิทธิ ข้อผูกพัน และข้อกำหนดตามกฎหมายหรือสัญญา
4. ระดับอิทธิพลและระดับผลกระทบที่อาจได้รับ
5. ความเปราะบางหรือความต้องการการคุ้มครองเป็นพิเศษ
6. ผลกระทบที่ไม่สามารถยอมรับได้
7. ช่องทางและความถี่ในการสื่อสารหรือปรึกษาหารือ
8. ข้อมูลหรือมุมมองที่ต้องนำมาใช้ในการประเมินความเสี่ยง

ความคาดหวังของผู้มีส่วนได้ส่วนเสียไม่ถือเป็นข้อผูกพันทั้งหมดโดยอัตโนมัติ ต้องพิจารณาร่วมกับกฎหมาย นโยบาย ยุทธศาสตร์ ทรัพยากร และอำนาจหน้าที่ของมหาวิทยาลัย

4.5.5 การกำหนดบทบาทและโครงสร้างการตัดสินใจ *(Governance Roles and Decision Structure)*

ก่อนเริ่มประเมิน ต้องกำหนดอย่างน้อย

- เจ้าของวัตถุประสงค์ (Objective Owner)
- ผู้รับผิดชอบนำการประเมิน

- ผู้เข้าร่วมและผู้เชี่ยวชาญที่ต้องให้ข้อมูล
- ผู้ตรวจสอบหรือท้าทายคุณภาพการประเมิน
- ผู้มีอำนาจอนุมัติผลการประเมิน
- ผู้มีอำนาจยอมรับและยกระดับความเสี่ยง
- เส้นทางและระยะเวลาการรายงาน
- ผู้ประสานงานและผู้จัดเก็บข้อมูล
- วิธีจัดการผลประโยชน์ทับซ้อน

อาจกำหนด Risk Owner เบื้องต้นตามเจ้าของวัตถุประสงค์หรือกระบวนงาน และยืนยันอย่างเป็นทางการเมื่อระบุความเสี่ยงในขั้นตอนที่ 3 ส่วน Action Owner ให้กำหนดหลังเลือกมาตรการในขั้นตอนที่ 5

4.5.6 ข้อมูลสำหรับกำหนดเกณฑ์ความเสี่ยง

ในขั้นตอนนี้ให้รวบรวมข้อมูลที่จำเป็นต่อการกำหนดเกณฑ์ เช่น

- ผลกระทบที่ผู้มีส่วนได้ส่วนเสียหรือมหาวิทยาลัยไม่สามารถยอมรับได้
- ข้อจำกัดตามกฎหมายและเหตุ Zero Tolerance
- เป้าหมายและค่าความเบี่ยงเบนของ KPI
- ข้อมูลเหตุการณ์และความเสียหายในอดีต
- ขีดความสามารถด้านการเงิน บุคลากร เทคโนโลยี และการตอบสนอง
- เกณฑ์หรือข้อกำหนดเฉพาะด้าน

การกำหนดและอนุมัติ Likelihood, Impact, Risk Matrix, RA/RT, Override และเกณฑ์ยกระดับ ให้ดำเนินการในขั้นตอนที่ 2 ตามข้อ 4.6 เพื่อป้องกันการปรับเกณฑ์ภายหลังให้สอดคล้องกับคะแนนที่ต้องการ

ผลลัพธ์ขั้นต่ำของขั้นตอนที่ 1 (Minimum Outputs of Step 1)

- เอกสารกำหนดขอบเขตและวัตถุประสงค์การประเมิน (Risk Assessment Scope and Objectives)
- การวิเคราะห์บริบท (Context Analysis)
- แผนที่ผู้มีส่วนได้ส่วนเสีย (Stakeholder Map)
- กรอบระยะเวลาที่ใช้ในการประเมิน (Time Horizon)
- สมมติฐานและข้อจำกัด (Assumptions and Constraints)
- การพึ่งพาและจุดเชื่อมโยงกับระบบหรือหน่วยงานอื่น (Dependencies and Interfaces)
- โครงสร้างบทบาทและอำนาจตัดสินใจ (Roles and Decision Authority Structure)
- แหล่งข้อมูลและผู้รับผิดชอบข้อมูลเบื้องต้น (Preliminary Data Sources and Data Owners)
- ข้อมูลพื้นฐานสำหรับกำหนดเกณฑ์ความเสี่ยง (Baseline Information for Risk Criteria)
- กำหนดการประเมินและการรายงาน (Assessment and Reporting Schedule)

ผลลัพธ์ดังกล่าวอาจบันทึกรวมในแบบฟอร์มกำหนดบริบทและขอบเขตความเสี่ยง (Risk Context and Scope Record) ฉบับเดียว เพื่อลดความซ้ำซ้อนของเอกสารและใช้เป็นข้อมูลตั้งต้นสำหรับขั้นตอนต่อไป

4.6 ขั้นตอนที่ 2 การกำหนดวัตถุประสงค์และเกณฑ์ความเสี่ยง *(Objectives and Risk Criteria)*

การบริหารความเสี่ยงต้องเริ่มจากวัตถุประสงค์ที่ชัดเจน เนื่องจากความเสี่ยงหมายถึงผลกระทบของความไม่แน่นอนต่อวัตถุประสงค์ การระบุความเสี่ยงโดยไม่มีวัตถุประสงค์อ้างอิงอาจทำให้ได้เพียงรายการปัญหาทั่วไป ซึ่งไม่สามารถประเมิน จัดลำดับ กำหนดเจ้าของ หรือนำไปใช้ตัดสินใจได้อย่างเหมาะสม

วัตถุประสงค์ควรมีลักษณะดังนี้

- เฉพาะเจาะจงและเข้าใจตรงกัน *(Specific)*
- สามารถวัดผลหรือตรวจสอบความสำเร็จได้ *(Measurable)*
- มีความเป็นไปได้ภายใต้ทรัพยากรและข้อจำกัด *(Achievable)*
- เชื่อมโยงกับยุทธศาสตร์ พันธกิจ หรือภารกิจ *(Relevant)*
- มีกรอบระยะเวลาที่ชัดเจน *(Time-bound)*
- มีเจ้าของวัตถุประสงค์ที่รับผิดชอบต่อผลลัพธ์ *(Objective Owner)*

4.6.1 องค์ประกอบที่ต้องกำหนด

ตารางที่ 4-5 *องค์ประกอบและตัวอย่างการกำหนดเกณฑ์ความเสี่ยง*

องค์ประกอบ	ความหมาย	คำถามสำคัญ
1. **วัตถุประสงค์ (Objective)**	ผลลัพธ์ที่ต้องการบรรลุภายในช่วงเวลาที่กำหนด	ต้องการบรรลุอะไร ภายในเมื่อใด และใครรับผิดชอบ
2. **ตัวชี้วัดและเป้าหมาย (KPI/Target)**	ตัววัดความสำเร็จของวัตถุประสงค์และค่าเป้าหมาย	จะทราบได้อย่างไรว่าบรรลุวัตถุประสงค์แล้ว
3. **ความสามารถในการรองรับความเสี่ยง (Risk Capacity)**	ระดับความเสี่ยงสูงสุดที่มหาวิทยาลัยสามารถรองรับได้ก่อนกระทบต่อข้อจำกัดสำคัญ ความอยู่รอด หรือพันธกิจ	จุดใดที่มหาวิทยาลัยไม่สามารถรองรับผลกระทบต่อไปได้
4. **ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA)**	ประเภทและระดับความเสี่ยงที่มหาวิทยาลัยยินดีรับในการดำเนินยุทธศาสตร์และบรรลุวัตถุประสงค์	มหาวิทยาลัยยินดีรับความเสี่ยงได้เพียงใด
5. **ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT)**	ขอบเขตความเบี่ยงเบนที่วัดได้จาก RA เป้าหมาย หรือผลการดำเนินงาน ซึ่งยังสามารถบริหารจัดการได้ภายใต้เงื่อนไขที่กำหนด	ผลการดำเนินงานสามารถเบี่ยงเบนจากเป้าหมายได้เท่าใดก่อนต้องยกระดับ
6. **จุดแจ้งเตือนหรือเงื่อนไขดำเนินการ (Trigger)**	ค่า เหตุการณ์ หรือแนวโน้มที่กำหนดให้ต้องเฝ้าระวัง ดำเนินมาตรการ หรือยกระดับรายงาน	เมื่อใดต้องเริ่มดำเนินการ และต้องทำอะไร

องค์ประกอบ	ความหมาย	คำถามสำคัญ
7. **อำนาจตัดสินใจ (Decision Authority)**	ผู้มีอำนาจยอมรับ ตอบสนอง จัดสรรทรัพยากร หรือยกระดับความเสี่ยง	ใครมีอำนาจตัดสินใจในแต่ละระดับ
8. **เจ้าของข้อมูล (Data Owner)**	ผู้รับผิดชอบคุณภาพ ความครบถ้วน และความทันเวลาของข้อมูล	ใครรับรองข้อมูลที่ใช้ติดตามและตัดสินใจ

4.6.2 หลักการกำหนด RA/RT

1. RA และ RT ต้องเชื่อมโยงกับวัตถุประสงค์ KPI และความเสี่ยงที่เกี่ยวข้อง
2. ควรกำหนดข้อความเชิงคุณภาพควบคู่กับค่าเชิงปริมาณเมื่อมีข้อมูลเพียงพอ
3. ค่าเชิงปริมาณต้องระบุนิยาม สูตร หน่วยวัด แหล่งข้อมูล ความถี่ และเจ้าของข้อมูล
4. Trigger อาจกำหนดไว้ก่อนถึง RT เพื่อให้มีเวลาเตรียมการและดำเนินมาตรการเชิงป้องกัน
5. เมื่อเกิน RT ต้องดำเนินมาตรการและยกระดับตามเกณฑ์ ไม่ควรรอให้กระทบ Risk Capacity
6. ส่วนงานอาจกำหนด RT ที่เข้มงวดกว่ากรอบมหาวิทยาลัย แต่ต้องไม่ผ่อนคลาย RA ข้อห้าม หรือ Zero Tolerance โดยไม่ได้รับอนุมัติ
7. ห้ามปรับ RA/RT ภายหลังเพื่อให้ผลการดำเนินงานที่ไม่บรรลุเป้าหมายกลับมาอยู่ในระดับยอมรับได้โดยไม่มีเหตุผลและหลักฐานรองรับ
8. RA/RT ต้องไม่ขัดต่อกฎหมาย ข้อบังคับ จริยธรรม ข้อผูกพัน และนโยบาย Zero Tolerance

4.6.3 ตัวอย่างการกำหนด Objective–KPI–RA/RT

ตัวอย่างที่ 1 ความมั่นคงและความยั่งยืนทางการเงิน *(Financial Sustainability)*

ตารางที่ 4-6 *ตัวอย่างข้อความความเสี่ยงที่ไม่เหมาะสมและข้อความที่ปรับปรุงแล้ว*

องค์ประกอบ	ตัวอย่างการกำหนด
วัตถุประสงค์ (Objective)	รักษาสภาพคล่องให้เพียงพอต่อการดำเนินพันธกิจสำคัญของมหาวิทยาลัยอย่างต่อเนื่องตลอดปีงบประมาณ พ.ศ. 2570
เจ้าของวัตถุประสงค์ (Objective Owner)	รองอธิการบดีหรือผู้บริหารที่กำกับด้านการเงิน
KPI/Target	จำนวนวันที่มหาวิทยาลัยสามารถดำเนินงานได้ด้วยเงินสดที่มีอยู่ (Days Cash on Hand: DCOH) ไม่น้อยกว่า 180 วัน
ความเสี่ยง (Risk)	เนื่องจากรายได้ค่าเล่าเรียนและรายได้จากแหล่งอื่นอาจต่ำกว่าแผน ขณะที่ค่าใช้จ่ายคงที่อยู่ในระดับสูง อาจทำให้กระแสเงินสดและสภาพคล่องลดลง ส่งผลต่อความสามารถในการดำเนินพันธกิจและชำระภาระผูกพัน
Risk Capacity	DCOH ต่ำกว่า 90 วัน ถือว่าเข้าใกล้ขีดจำกัดที่อาจกระทบต่อความต่อเนื่องของพันธกิจสำคัญ

องค์ประกอบ	ตัวอย่างการกำหนด
Risk Appetite: RA	มหาวิทยาลัยมีความเสี่ยงที่ยอมรับได้ในระดับต่ำต่อการขาดสภาพคล่อง โดยกำหนด DCOH ไม่น้อยกว่า 180 วัน
Risk Tolerance: RT	ยอมให้ DCOH อยู่ในช่วง 120–ต่ำกว่า 180 วันได้เป็นการชั่วคราว โดยต้องมีแผนแก้ไขและติดตามอย่างใกล้ชิด
Trigger/Early Warning	ประมาณการ DCOH ต่ำกว่า 150 วัน หรือมีแนวโน้มลดลงต่อเนื่อง 3 เดือน ให้ทบทวนประมาณการกระแสเงินสดและจัดทำแผนสภาพคล่อง
เกิน RT	DCOH ต่ำกว่า 120 วัน ให้ยกระดับต่ออธิการบดีหรือคณะกรรมการที่เกี่ยวข้องและดำเนิน Liquidity Action Plan
เข้าใกล้ Capacity	DCOH ต่ำกว่า 90 วัน ให้ยกระดับเร่งด่วนและพิจารณามาตรการรักษาพันธกิจสำคัญ
Data Owner	กองคลัง
Decision Authority	ตามตารางอำนาจยอมรับและยกระดับความเสี่ยงของมหาวิทยาลัย

การแสดงสถานะสามารถสรุปได้ดังนี้

สถานะ	DCOH	แนวทางดำเนินการ
อยู่ภายใน RA	≥ 180 วัน	ควบคุมและติดตามตามรอบ
เฝ้าระวัง	150–<180 วัน	วิเคราะห์แนวโน้มและเตรียมมาตรการ
อยู่ในช่วง RT	120–<150 วัน	ดำเนินแผนแก้ไขและติดตามใกล้ชิด
เกิน RT	90–<120 วัน	ยกระดับรายงานและเร่งแก้ไข
เกิน Risk Capacity	<90 วัน	ดำเนินมาตรการฉุกเฉินและคุ้มครองพันธกิจสำคัญ

ตัวอย่างที่ 2 ความเสี่ยงแบบ Zero Tolerance

องค์ประกอบ	ตัวอย่างการกำหนด
วัตถุประสงค์ (Objective)	ดำเนินงานด้วยความโปร่งใส ถูกต้องตามกฎหมาย และปราศจากการทุจริต
KPI/Target	จำนวนกรณีทุจริตที่ได้รับการยืนยันข้อเท็จจริงเท่ากับ 0 กรณี
Risk Appetite: RA	ไม่ยอมรับการทุจริต การรับสินบน หรือการใช้ทรัพย์สินของมหาวิทยาลัยโดยมิชอบ (Zero Appetite)
Risk Tolerance: RT	ไม่มีช่วงความเบี่ยงเบนที่ยอมรับได้
Trigger	พบเหตุ ข้อร้องเรียน หรือข้อมูลที่มีมูลเกี่ยวกับการทุจริตตั้งแต่ 1 กรณีขึ้นไป
Action	ระงับหรือจำกัดความเสียหาย รักษาพยานหลักฐาน รายงาน และตรวจสอบข้อเท็จจริงทันที
Decision Authority	ผู้มีอำนาจตามกฎหมาย ระเบียบ และเส้นทางรายงานเหตุ Zero Tolerance

การรายงานข้อสงสัยหรือการเริ่มตรวจสอบไม่ถือเป็นข้อยุติว่าบุคคลใดกระทำความผิด การวินิจฉัยต้องเป็นไปตามกระบวนการตรวจสอบข้อเท็จจริงและหลักความเป็นธรรม

ผลลัพธ์ขั้นต่ำของขั้นตอนที่ 2 *(Minimum Outputs of Step 2)*

- ความเชื่อมโยงระหว่างวัตถุประสงค์ KPI และความเสี่ยง *(Objective–KPI–Risk Linkage)*
- วัตถุประสงค์และค่าเป้าหมายที่ได้รับการยืนยัน *(Approved Objectives and Targets)*
- กรอบ Risk Capacity, Risk Appetite และ Risk Tolerance
- เกณฑ์โอกาสเกิดและผลกระทบ *(Likelihood and Impact Criteria)*
- ตารางระดับความเสี่ยง *(Risk Matrix)*
- เกณฑ์ Override และ Zero Tolerance
- จุดแจ้งเตือนและเงื่อนไขดำเนินการ *(Trigger and Action)*
- เจ้าของข้อมูลและแหล่งข้อมูล *(Data Owners and Data Sources)*
- ผู้มีอำนาจยอมรับ ตอบสนอง และยกระดับความเสี่ยง *(Decision and Escalation Authorities)*

เนื้อหาครบถ้วนและเหมาะสมกับกรอบความเสี่ยง 4 ประเภทของมหาวิทยาลัย ควรใช้คำว่า “ความเสี่ยงด้านยุทธศาสตร์” ให้สอดคล้องกับแผนยุทธศาสตร์ เพิ่มตัวอย่างการจำแนกความเสี่ยง และจัดองค์ประกอบ Risk Register เป็นหมวดเพื่อให้ส่วนงานนำไปใช้ได้ง่าย ดังนี้

4.7 ขั้นตอนที่ 3 การระบุความเสี่ยง *(Risk Identification)*

การระบุความเสี่ยงเป็นกระบวนการค้นหาและอธิบายเหตุการณ์หรือความไม่แน่นอนที่อาจส่งผลต่อการบรรลุวัตถุประสงค์ ทั้งในด้านผลกระทบเชิงลบและโอกาสในการสร้างคุณค่า โดยต้องพิจารณาสาเหตุ เหตุการณ์ ผลกระทบ การควบคุม และความสัมพันธ์กับความเสี่ยงอื่นอย่างเป็นระบบ

4.7.1 รูปแบบการเขียนข้อความความเสี่ยง *(Risk Statement)*

ให้เขียนข้อความความเสี่ยงด้วยโครงสร้าง

เนื่องจาก [สาเหตุหรือปัจจัยขับเคลื่อน (Cause/Risk Driver)] ⟶ อาจทำให้เกิด [เหตุการณ์ความเสี่ยง (Risk Event)] ⟶ ส่งผลต่อ [วัตถุประสงค์หรือผู้มีส่วนได้ส่วนเสีย (Impact)]

ตัวอย่าง

เนื่องจากข้อมูลนักศึกษาและข้อมูลตลาดแรงงานยังไม่เชื่อมโยงกันอย่างเพียงพอ **(Cause)** อาจทำให้มหาวิทยาลัยปรับหลักสูตรและแผนรับนักศึกษาไม่ทันต่อความต้องการ **(Event)** ส่งผลให้จำนวนผู้สมัคร รายได้ และความสามารถในการแข่งขันต่ำกว่าเป้าหมาย **(Impact)**

หลักการเขียนข้อความความเสี่ยง

1. ต้องเชื่อมโยงกับวัตถุประสงค์ ผลลัพธ์ หรือ KPI ที่ชัดเจน
2. หลีกเลี่ยงการเขียนเป็นหัวข้อกว้าง เช่น “บุคลากร” “งบประมาณ” หรือ “เทคโนโลยี”
3. หลีกเลี่ยงการเขียนเป็นเพียงปัญหาหรือสาเหตุ เช่น “บุคลากรไม่เพียงพอ” หรือ “งบประมาณไม่เพียงพอ” โดยไม่ระบุเหตุการณ์และผลกระทบ

4. ไม่เขียนเป็นเพียงผลกระทบ เช่น “มหาวิทยาลัยเสียชื่อเสียง” โดยไม่ระบุสาเหตุและเหตุการณ์ที่นำไปสู่ผลกระทบ

5. ไม่เขียนมาตรการเป็นความเสี่ยง เช่น “ไม่ได้จัดอบรม” หรือ “ไม่มีการประชุมติดตาม”

6. เหตุการณ์ที่เกิดขึ้นแล้วให้บันทึกเป็น Issue หรือ Incident และนำสาเหตุหรือบทเรียนมาใช้ทบทวนความเสี่ยง

7. ข้อความควรกระชับ เฉพาะเจาะจง และสามารถนำไปกำหนด Risk Owner, KRI และมาตรการได้

ตัวอย่างการปรับข้อความ

ข้อความที่ไม่เหมาะสม	ข้อความความเสี่ยงที่ปรับปรุง
งบประมาณไม่เพียงพอ	เนื่องจากรายได้ค่าเล่าเรียนอาจต่ำกว่าแผนและต้นทุนคงที่อยู่ในระดับสูง อาจทำให้สภาพคล่องลดลง ส่งผลต่อความสามารถในการดำเนินพันธกิจและชำระภาระผูกพัน
บุคลากรขาดทักษะ	เนื่องจากการพัฒนาทักษะยังไม่สอดคล้องกับสมรรถนะที่ยุทธศาสตร์ต้องการ อาจทำให้บุคลากรไม่สามารถนำ AI และเทคโนโลยีดิจิทัลมาใช้ได้อย่างมีประสิทธิผล ส่งผลให้การขับเคลื่อนยุทธศาสตร์ล่าช้า
ความเสี่ยงด้านไซเบอร์	เนื่องจากระบบสำคัญยังมีช่องโหว่และการควบคุมสิทธิไม่เพียงพอ อาจเกิดการเข้าถึงหรือทำลายข้อมูลโดยมิชอบ ส่งผลให้บริการหยุดชะงัก ข้อมูลรั่วไหล และมหาวิทยาลัยไม่ปฏิบัติตามกฎหมาย
ชื่อเสียงเสียหาย	เนื่องจากกระบวนการติดตามและตอบสนองต่อข้อมูลข่าวสารยังไม่ทันเวลา อาจทำให้ข้อมูลที่ไม่ถูกต้องแพร่กระจายในวงกว้าง ส่งผลต่อความเชื่อมั่นของนักศึกษา ผู้ปกครอง และสาธารณชน

4.7.2 แหล่งข้อมูลและเทคนิคการระบุความเสี่ยง *(Risk Identification Sources and Techniques)*

การระบุความเสี่ยงต้องใช้ข้อมูลหลายแหล่งเพื่อให้ครอบคลุมและลดอคติ เช่น

- วัตถุประสงค์ แผนยุทธศาสตร์ KPI และ KRI
- แนวโน้มผลการดำเนินงานและข้อมูลคาดการณ์
- เหตุการณ์ Incident และ Near Miss
- ข้อร้องเรียน ข้อพิพาท คดี และความคิดเห็นของผู้มีส่วนได้ส่วนเสีย
- ผลการตรวจสอบและการประเมินการควบคุม
- การเปลี่ยนแปลงกฎหมาย นโยบาย และมาตรฐาน
- ข้อมูลคู่เทียบและแนวโน้มของสถาบันอุดมศึกษา
- ข้อมูลจากผู้รับจ้าง ผู้ให้บริการ และคู่ความร่วมมือ
- ความเสี่ยงเกิดใหม่และการเปลี่ยนแปลงของบริบท

เทคนิคที่อาจนำมาใช้ ได้แก่

- การประชุมเชิงปฏิบัติการ *(Risk Workshop)*
- การสัมภาษณ์ *(Interview)*
- การวิเคราะห์กระบวนงาน *(Process Mapping)*
- การวิเคราะห์สาเหตุและผลกระทบ *(Cause and Effect/Fishbone)*
- การวิเคราะห์แบบโบว์ไท *(Bow-tie Analysis)*
- การวิเคราะห์สาเหตุราก *(Root Cause Analysis)*
- การวิเคราะห์สถานการณ์จำลอง *(Scenario Analysis)*
- การกวาดสัญญาณอนาคต *(Horizon Scanning)*
- PESTLE และ SWOT Analysis
- การวิเคราะห์ข้อมูลและแนวโน้ม *(Data and Trend Analysis)*

การเลือกเทคนิคให้เหมาะสมกับวัตถุประสงค์ ความซับซ้อน และระดับความเสี่ยง โดยไม่จำเป็นต้องใช้ทุกเทคนิคในทุกกรณี

4.7.3 ประเภทความเสี่ยง (Risk Categories)

ตั้งแต่ปีงบประมาณ พ.ศ. 2570 มหาวิทยาลัยกำหนดประเภทความเสี่ยงหลัก **5 ประเภท** เพื่อใช้เป็นกรอบมาตรฐานเดียวกันในการระบุ วิเคราะห์ ประเมิน จัดลำดับ และรายงานความเสี่ยงทั่วทั้งมหาวิทยาลัย ดังนี้

ตารางที่ 4-7 *ประเภทความเสี่ยง ขอบเขต และตัวอย่าง*

ลำดับ	ประเภทความเสี่ยง	ขอบเขตและตัวอย่าง
1	**ความเสี่ยงด้านยุทธศาสตร์ (Strategic Risk: S)**	ความเสี่ยงที่อาจส่งผลต่อการบรรลุวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ เป้าประสงค์ และตัวชี้วัดสำคัญของมหาวิทยาลัย ครอบคลุมความสามารถในการแข่งขันด้านการศึกษา การเปลี่ยนแปลงจำนวนและความต้องการของผู้เรียน คุณภาพและความทันสมัยของหลักสูตร การวิจัยและนวัตกรรม ความร่วมมือระดับชาติและนานาชาติ การจัดอันดับมหาวิทยาลัย การเปลี่ยนแปลงของระบบอุดมศึกษา ตลอดจนความสามารถในการปรับตัวและใช้ประโยชน์จากการเปลี่ยนแปลงทางเศรษฐกิจ สังคม และเทคโนโลยีเพื่อขับเคลื่อนยุทธศาสตร์
2	**ความเสี่ยงด้านการดำเนินงาน (Operational Risk: O)**	ความเสี่ยงที่เกิดจากบุคลากร กระบวนการปฏิบัติงาน ระบบงาน การให้บริการ ทรัพย์สิน อาคารสถานที่ ผู้รับจ้าง หรือการควบคุมที่ไม่เพียงพอ ซึ่งอาจส่งผลต่อคุณภาพ ประสิทธิภาพ ประสิทธิผล ความปลอดภัย และความต่อเนื่องในการดำเนินงาน ครอบคลุมช่องว่างด้านสมรรถนะ ความผิดพลาดในการปฏิบัติงาน การหยุดชะงักของกระบวนงาน อุบัติเหตุ ภัยพิบัติ การบริหารคู่สัญญา และการบริหารความต่อเนื่องทางธุรกิจ (BCM/BCP)

ลำดับ	ประเภทความเสี่ยง	ขอบเขตและตัวอย่าง
3	**ความเสี่ยงด้านการเงิน (Financial Risk: F)**	ความเสี่ยงที่อาจส่งผลต่อความมั่นคง ความสามารถในการชำระภาระผูกพัน และความยั่งยืนทางการเงินของมหาวิทยาลัย ครอบคลุมโครงสร้างและความหลากหลายของรายได้ การพึ่งพารายได้จากค่าเล่าเรียน สภาพคล่อง กระแสเงินสด งบประมาณ ต้นทุนคงที่ การจัดสรรทรัพยากร การลงทุน การบริหารทรัพย์สิน ภาระผูกพัน ความผันผวนทางเศรษฐกิจ ตลอดจนความคุ้มค่าและความเป็นไปได้ของโครงการหรือกิจกรรมสร้างรายได้
4	**ความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (Compliance and Governance Risk: C)**	ความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ ประกาศ มติ สัญญา มาตรฐานวิชาชีพ จริยธรรม หรือข้อกำหนดของหน่วยงานกำกับ รวมถึงข้อบกพร่องด้านโครงสร้างการกำกับดูแล อำนาจหน้าที่ การแบ่งแยกหน้าที่ การควบคุมภายใน ความโปร่งใส และความรับผิดชอบ ครอบคลุมการทุจริต การรับสินบน ผลประโยชน์ทับซ้อน การจัดซื้อจัดจ้าง การเงินและบัญชี การละเมิดข้อมูลส่วนบุคคล การประพฤติมิชอบทางการวิจัย การรายงานข้อมูลที่ไม่ถูกต้อง และการไม่แก้ไขข้อบกพร่องหรือข้อสั่งการที่มีนัยสำคัญ
5	**ความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Technology Risk: D)**	ความเสี่ยงที่มีสาเหตุหลักจากเทคโนโลยีดิจิทัล ระบบสารสนเทศ โครงสร้างพื้นฐานดิจิทัล ข้อมูล AI หรือการพึ่งพาเทคโนโลยี ซึ่งอาจส่งผลต่อความพร้อมใช้ ความมั่นคงปลอดภัย ความถูกต้อง ความครบถ้วน และความลับของข้อมูลและระบบ ครอบคลุมภัยคุกคามทางไซเบอร์ การเข้าถึงโดยไม่ได้รับอนุญาต ช่องโหว่ของระบบ ความล้มเหลวของโครงสร้างพื้นฐานหรือระบบสำคัญ การสูญหายหรือเสียหายของข้อมูล การสำรองและกู้คืนข้อมูล ความเสี่ยงจากผู้ให้บริการภายนอก ระบบ Cloud การใช้ AI ที่ไม่เหมาะสมหรือไม่สามารถควบคุมได้ ความล้าสมัยของเทคโนโลยี และความเสี่ยงจากการเปลี่ยนผ่านสู่ดิจิทัล

ประเภทความเสี่ยงดังกล่าวมีวัตถุประสงค์เพื่อช่วยให้การระบุและบริหารความเสี่ยงมีความครบถ้วนและเป็นระบบ **มิได้มีวัตถุประสงค์เพื่อแบ่งการบริหารความเสี่ยงออกเป็นส่วนแยกจากกัน (Silo)** เนื่องจากความเสี่ยงหนึ่งรายการอาจมีสาเหตุ ผลกระทบ หรือความเชื่อมโยงกับความเสี่ยงมากกว่าหนึ่งประเภท

หลักการจำแนกประเภทความเสี่ยง

1. **พิจารณาจากวัตถุประสงค์ที่ได้รับผลกระทบและสาเหตุหลักของเหตุการณ์ความเสี่ยง** เป็นสำคัญ โดยไม่จำแนกจากผลกระทบปลายทางเพียงอย่างเดียว
2. **กำหนดประเภทหลัก (Primary Risk Category) เพียงหนึ่งประเภท** สำหรับความเสี่ยงแต่ละรายการ เพื่อให้การกำหนดเจ้าของความเสี่ยง (Risk Owner) ความรับผิดชอบ และสายการรายงานมีความชัดเจน ทั้งนี้ สามารถระบุประเภทความเสี่ยงหรือมิติผลกระทบที่เกี่ยวข้องเพิ่มเติมได้
3. **ความเสี่ยงด้าน AI และเทคโนโลยีดิจิทัล** ให้จำแนกตามสาเหตุหลักและวัตถุประสงค์ที่ได้รับผลกระทบ ดังนี้

- **Strategic Risk (S):** เมื่อประเด็นหลักเกี่ยวข้องกับความสามารถในการปรับตัว การกำหนดทิศทาง การลงทุน การนำเทคโนโลยีมาใช้สร้างคุณค่า หรือการขับเคลื่อนยุทธศาสตร์
- **Operational Risk (O):** เมื่อประเด็นหลักเกิดจากบุคลากร กระบวนงาน หรือวิธีการนำเทคโนโลยีไปใช้ในการปฏิบัติงาน
- **Compliance and Governance Risk (C):** เมื่อประเด็นหลักเกี่ยวข้องกับการไม่ปฏิบัติตามกฎหมาย จริยธรรม ความโปร่งใส สิทธิของผู้มีส่วนได้ส่วนเสีย หรือธรรมาภิบาลด้าน AI
- **Digital Technology Risk (D):** เมื่อสาเหตุหลักเกิดจากระบบสารสนเทศ โครงสร้างพื้นฐานดิจิทัล ข้อมูล AI แบบจำลอง ระบบอัตโนมัติ ภัยคุกคามทางไซเบอร์ หรือความล้มเหลวของเทคโนโลยีโดยตรง

4. **ความเสี่ยงด้านไซเบอร์และข้อมูลส่วนบุคคล (PDPA)** ให้พิจารณาจากสาเหตุหลัก ดังนี้
   - จัดเป็น **Digital Technology Risk (D)** เมื่อสาเหตุหลักเกิดจากช่องโหว่ การโจมตีทางไซเบอร์ ระบบหรือโครงสร้างพื้นฐาน การกำหนดสิทธิ์ การสำรองข้อมูล หรือกลไกทางเทคนิค
   - จัดเป็น **Operational Risk (O)** เมื่อสาเหตุหลักเกิดจากกระบวนงานหรือการปฏิบัติงานของบุคลากร
   - จัดเป็น **Compliance and Governance Risk (C)** เมื่อประเด็นหลักเป็นการไม่ปฏิบัติตามกฎหมายหรือข้อกำหนดด้านข้อมูลส่วนบุคคล
5. **ชื่อเสียงและความเชื่อมั่น ความปลอดภัย สิ่งแวดล้อมและ ESG** ตลอดจนผลกระทบต่อคุณภาพการศึกษา การวิจัย และวิชาการ ให้พิจารณาเป็น มิติผลกระทบร่วม (Cross-cutting Impact Dimensions) ซึ่งอาจเกิดจากความเสี่ยงประเภทใดประเภทหนึ่งหรือหลายประเภท
6. **หากมิติผลกระทบร่วมมีนัยสำคัญต่อการบรรลุวัตถุประสงค์ของมหาวิทยาลัย** ต้องกำหนดตัวชี้วัดความเสี่ยง (KRI) ระดับความเสี่ยงที่ยอมรับได้ มาตรการจัดการความเสี่ยง และหลักเกณฑ์การรายงานหรือยกระดับ (Escalation) ให้เหมาะสม แม้มิได้กำหนดเป็นประเภทความเสี่ยงหลักแยกต่างหาก
7. **ต้องพิจารณา ความสัมพันธ์ระหว่างความเสี่ยง (Risk Interdependency)** ผลกระทบร่วม (Cumulative Impact) และการกระจุกตัวของความเสี่ยง (Risk Concentration) ในระดับส่วนงานและระดับมหาวิทยาลัย เพื่อป้องกันการประเมินความเสี่ยงแต่ละรายการแบบแยกส่วน

ตารางที่ 4-8 *ตัวอย่างการจำแนกประเภทความเสี่ยงหลักและมิติผลกระทบร่วม*

ตัวอย่างการจำแนกประเภทความเสี่ยง

ตัวอย่างความเสี่ยง	ประเภทหลัก	ประเภท/มิติที่เกี่ยวข้อง
มหาวิทยาลัยไม่สามารถปรับตัวและใช้ประโยชน์จาก AI และเทคโนโลยีดิจิทัลเพื่อขับเคลื่อนยุทธศาสตร์ได้ทันต่อการเปลี่ยนแปลง	S	D, O, C, ชื่อเสียง
ระบบสารสนเทศสำคัญหยุดชะงักจากช่องโหว่หรือการโจมตีทางไซเบอร์	D	O, C, ความต่อเนื่อง, ชื่อเสียง
การประมวลผลข้อมูลส่วนบุคคลไม่เป็นไปตามกฎหมาย	C	D, O, ชื่อเสียง
ระบบฐานข้อมูลสูญหายหรือไม่สามารถกู้คืนได้ตามระยะเวลาที่กำหนด	D	O, ความต่อเนื่อง, ชื่อเสียง
รายได้ไม่เพียงพอและสภาพคล่องลดลงต่ำกว่าเกณฑ์ที่กำหนด	F	S, ความต่อเนื่อง
หลักสูตรไม่สอดคล้องกับความต้องการของผู้เรียนและตลาดแรงงาน	S	O, F, ชื่อเสียง
บุคลากรขาดสมรรถนะที่จำเป็นต่อการดำเนินงานและการเปลี่ยนแปลงในอนาคต	O	S, D, ความต่อเนื่อง
เกิดอุบัติเหตุจากกระบวนการปฏิบัติงานหรือการควบคุมด้านความปลอดภัยไม่เพียงพอ	O	C, Safety, ชื่อเสียง
เกิดการทุจริต การรับสินบน หรือการจัดซื้อจัดจ้างโดยมิชอบ	C	F, ชื่อเสียง
การนำ AI มาใช้ให้ผลลัพธ์คลาดเคลื่อนจากข้อมูลหรือแบบจำลองที่ไม่มีคุณภาพ	D	O, C, ชื่อเสียง

4.7.4 องค์ประกอบขั้นต่ำของทะเบียนความเสี่ยง *(Minimum Risk Register Requirements)*

ทะเบียนความเสี่ยงต้องมีข้อมูลอย่างน้อย ดังนี้

ก. ข้อมูลอ้างอิงและวัตถุประสงค์

- รหัสและชื่อความเสี่ยง
- ระดับการบริหารหรือส่วนงาน
- วัตถุประสงค์และ KPI ที่เกี่ยวข้อง
- ประเภทความเสี่ยงหลัก
- ประเภทที่เกี่ยวข้องและ Cross-cutting Impact
- วันที่ระบุและวันที่ทบทวนล่าสุด

ข. รายละเอียดความเสี่ยง

- Risk Statement
- สาเหตุหรือปัจจัยขับเคลื่อน
- เหตุการณ์ความเสี่ยง
- ผลกระทบ
- ความสัมพันธ์กับความเสี่ยงอื่น

- Risk Owner

ค. การประเมินและการควบคุม

- Inherent Risk
- การควบคุมที่มีอยู่
- Control Owner
- หลักฐานของการควบคุม
- Control Effectiveness
- Residual Risk
- สถานะเทียบกับ RA/RT
- เกณฑ์ Override หรือ Zero Tolerance ที่เกี่ยวข้อง

ง. ตัวชี้วัดและข้อมูล

- KPI, KRI หรือ KCI ที่เกี่ยวข้อง
- นิยามและสูตรคำนวณ
- ค่า RA/RT และ Trigger
- แหล่งข้อมูล
- Data Owner
- ความถี่ในการติดตาม

จ. การตอบสนองและมาตรการ

- Risk Response
- Risk Treatment Plan
- Action Owner และผู้ร่วมดำเนินการ
- ทรัพยากรและงบประมาณ
- Milestone และกำหนดแล้วเสร็จ
- หลักฐานหรือผลส่งมอบ
- Target Residual Risk
- ผู้มีอำนาจอนุมัติหรือยอมรับความเสี่ยง

ฉ. การติดตามและรายงาน

- สถานะและร้อยละความก้าวหน้า
- แนวโน้มความเสี่ยง
- เหตุการณ์และ Near Miss
- ปัญหาและอุปสรรค
- Corrective Action
- ประเด็นที่ต้องยกระดับ

- ผลการตัดสินใจและ Decision Log
- วันที่ติดตามและรอบติดตามครั้งถัดไป

ตารางที่ 4-9 *ตัวอย่างทะเบียนความเสี่ยงแบบย่อ*

รายการ	ตัวอย่าง
รหัสความเสี่ยง	S1
วัตถุประสงค์	ยกระดับความสามารถของมหาวิทยาลัยในการใช้ AI และเทคโนโลยีดิจิทัลเพื่อขับเคลื่อนยุทธศาสตร์ภายในปีงบประมาณ พ.ศ. 2570
Risk Statement	เนื่องจากโครงสร้างกำกับดูแล AI สมรรถนะบุคลากร และการเชื่อมโยงข้อมูลยังไม่เพียงพอ อาจทำให้มหาวิทยาลัยนำ AI มาใช้ไม่ทันหรือไม่เหมาะสม ส่งผลต่อคุณภาพการศึกษา ประสิทธิภาพ ความสามารถในการแข่งขัน และการปฏิบัติตามกฎหมาย
ประเภทหลัก	ความเสี่ยงด้านยุทธศาสตร์ (Strategic Risk: S)
ประเภท/มิติที่เกี่ยวข้อง	O, C, ชื่อเสียง การวิจัย และ ESG
Risk Owner	ผู้บริหารที่ได้รับมอบหมายให้กำกับด้านยุทธศาสตร์ AI และดิจิทัล
การควบคุมที่มีอยู่	นโยบายเทคโนโลยีดิจิทัล การอบรมบุคลากร ระบบสารสนเทศ และคณะทำงานที่เกี่ยวข้อง
Inherent Risk	L = 4, I = 4, คะแนน 16 ระดับสูงมาก (E)
Control Effectiveness	มีการควบคุมบางส่วน แต่ยังไม่ครอบคลุมและยังไม่สามารถยืนยันประสิทธิผลได้ทั้งหมด
Residual Risk	L = 4, I = 3, คะแนน 12 ระดับสูง (H)
ตัวอย่าง KRI	ร้อยละบุคลากรที่ผ่านเกณฑ์ AI/Digital Literacy
RA	≥80%
RT	70–<80%
Trigger	ต่ำกว่า 70% หรือแนวโน้มไม่บรรลุเป้าหมายตามรอบที่กำหนด
Risk Response	ลดความเสี่ยงและใช้ประโยชน์จากโอกาส (Reduce and Pursue)
มาตรการสำคัญ	จัดทำ AI Governance Framework พัฒนาสมรรถนะบุคลากร และดำเนินโครงการ AI Use Cases ที่ผ่านการประเมิน
Action Owner	หน่วยงานด้านยุทธศาสตร์ ทรัพยากรบุคคล และเทคโนโลยีดิจิทัลตามมาตรการ
Target Residual Risk	L = 2, I = 2, คะแนน 4 ระดับต่ำ (L)
กำหนดเวลา	ภายในปีงบประมาณ พ.ศ. 2570
สถานะ/แนวโน้ม	บันทึกตามผลการติดตามจริงในแต่ละรอบ
ประเด็นยกระดับ	เสนอผู้บริหารเมื่อ KRI เกิน RT มาตรการสำคัญล่าช้า หรือจำเป็นต้องใช้ทรัพยากรเกินอำนาจ Risk Owner

ผลลัพธ์ขั้นต่ำของขั้นตอนที่ 3 *(Minimum Outputs of Step 3)*

- ทะเบียนความเสี่ยงที่ผ่านการยืนยันจาก Risk Owner *(Validated Risk Register)*
- รายการความเสี่ยงและโอกาสที่เชื่อมโยงกับวัตถุประสงค์
- การกำหนดประเภทความเสี่ยงหลักและมิติผลกระทบร่วม
- รายชื่อ Risk Owner และผู้เกี่ยวข้อง
- รายการความสัมพันธ์และการกระจุกตัวของความเสี่ยง
- รายการความเสี่ยงที่ต้องยกระดับหรือเสนอพิจารณาในระดับมหาวิทยาลัย
- หลักฐานและแหล่งข้อมูลที่ใช้ในการระบุความเสี่ยง

4.8 ขั้นตอนที่ 4 การวิเคราะห์และประเมินความเสี่ยง *(Risk Analysis and Evaluation)*

การวิเคราะห์และประเมินความเสี่ยงมีวัตถุประสงค์เพื่อทำความเข้าใจลักษณะ สาเหตุ โอกาสเกิด ผลกระทบ ประสิทธิผลของการควบคุม และระดับความเสี่ยง เพื่อเปรียบเทียบกับ RA/RT จัดลำดับความสำคัญ เลือกแนวทางตอบสนอง และพิจารณาการยกระดับ

คะแนนความเสี่ยงเป็นข้อมูลประกอบการตัดสินใจ มิใช่ข้อยุติเพียงอย่างเดียว ต้องพิจารณาแนวโน้มความเร็วในการเกิดผลกระทบ ความสัมพันธ์ของความเสี่ยง คุณภาพข้อมูล เกณฑ์ Override และข้อจำกัดตามกฎหมายร่วมด้วย

4.8.1 ระดับความเสี่ยงที่ต้องประเมิน

1. **ความเสี่ยงโดยธรรมชาติ (Inherent Risk):** ระดับความเสี่ยงก่อนพิจารณาผลของการควบคุมหรือมาตรการที่มีอยู่
2. **ความเสี่ยงคงเหลือ (Residual Risk):** ระดับความเสี่ยงภายหลังพิจารณาเฉพาะการควบคุมที่มีหลักฐานว่าได้รับการนำไปใช้และทำงานจริง ณ วันที่ประเมิน
3. **ความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk):** ระดับความเสี่ยงที่คาดว่าจะเหลือภายหลังดำเนินมาตรการเพิ่มเติมครบถ้วนและมีประสิทธิผลภายในระยะเวลาที่กำหนด

ห้ามใช้ Target Residual Risk แทน Residual Risk และห้ามลดคะแนน Residual Risk เพียงเพราะมีแผนหรือกำลังดำเนินมาตรการ หากยังไม่มีหลักฐานเพียงพอว่ามาตรการได้รับการนำไปใช้และมีประสิทธิผล

4.8.2 เกณฑ์โอกาสเกิด *(Likelihood Criteria)*

ต้องกำหนดช่วงเวลาที่ใช้ประเมิน (Time Horizon) ให้ชัดเจน โดยทั่วไปใช้หนึ่งปีงบประมาณ หรือใช้ช่วงเวลาของยุทธศาสตร์ โครงการ สัญญา หรืออายุระบบตามความเหมาะสม

ตารางที่ 4-10 *เกณฑ์การประเมินโอกาสเกิด (Likelihood)*

คะแนน	ระดับ	แนวทางเชิงคุณภาพ	ตัวอย่างความถี่
1	**น้อยมาก (Rare)**	มีโอกาสเกิดน้อยมาก ไม่เคยเกิด หรือเกิดเฉพาะในสถานการณ์ผิดปกติอย่างยิ่ง	ไม่เกิน 1 ครั้งใน 5 ปี
2	**น้อย (Unlikely)**	อาจเกิดขึ้นได้ แต่ไม่คาดว่าจะเกิดในสภาวะปกติ	ประมาณ 1 ครั้งใน 2–4 ปี
3	**ปานกลาง (Possible)**	มีโอกาสเกิดในสภาวะปกติ หรือเคยเกิดเป็นครั้งคราว	ประมาณ 1 ครั้งต่อปี
4	**มาก (Likely)**	มีแนวโน้มเกิดหลายครั้ง หรือมีปัจจัยขับเคลื่อนปรากฏอย่างต่อเนื่อง	ประมาณ 2–6 ครั้งต่อปี
5	**สูงมาก (Almost Certain)**	เกือบแน่นอน เกิดเป็นประจำ หรือเกิดซ้ำอย่างต่อเนื่อง	มากกว่า 6 ครั้งต่อปี หรือเกิดเกือบทุกเดือน

ตัวอย่างความถี่เป็นแนวทางประกอบ มิใช่เกณฑ์ตายตัว หากข้อมูลเชิงสถิติและดุลยพินิจเชิงคุณภาพให้ผลต่างกัน ต้องบันทึกเหตุผลและหลักฐานที่ใช้ตัดสิน

กรณีความเสี่ยงเชิงยุทธศาสตร์หรือความเสี่ยงเกิดใหม่ที่ไม่สามารถวัดเป็นความถี่ได้ ให้พิจารณาจาก

- ความน่าจะเป็นภายในช่วงเวลาที่กำหนด
- แนวโน้มและปัจจัยขับเคลื่อน
- ความเปราะบางและระดับการเปิดรับความเสี่ยง
- สมมติฐานเชิงยุทธศาสตร์
- ข้อมูลคู่เทียบและความเห็นผู้เชี่ยวชาญ
- Scenario Analysis และ Horizon Scanning
- ความเชื่อมั่นและข้อจำกัดของข้อมูล

4.8.3 เกณฑ์ผลกระทบ *(Impact Criteria)*

ให้ประเมินผลกระทบทุกมิติที่เกี่ยวข้องและบันทึกคะแนนแยกตามมิติ โดยใช้คะแนนสูงสุดที่มีเหตุผลและหลักฐานรองรับเป็น Impact Score ไม่เฉลี่ยคะแนนข้ามมิติ เพราะอาจทำให้ผลกระทบรุนแรงบางด้านถูกลดทอน

ตารางที่ 4-11 เกณฑ์การประเมินผลกระทบ (Impact)

คะแนน	ระดับ	คำอธิบายกลาง
1	**น้อยมาก (Insignificant)**	ผลกระทบเล็กน้อย แก้ไขได้ในงานประจำ ไม่กระทบเป้าหมายหรือผู้มีส่วนได้ส่วนเสียอย่างมีนัยสำคัญ
2	**น้อย (Minor)**	ผลกระทบจำกัดภายในหน่วยงาน แก้ไขได้ด้วยทรัพยากรและอำนาจที่มี
3	**ปานกลาง (Moderate)**	กระทบเป้าหมาย บริการ หรือผู้มีส่วนได้ส่วนเสียอย่างมีนัยสำคัญ ต้องให้ผู้บริหารกำกับและจัดสรรทรัพยากรเพิ่มเติม
4	**มาก (Major)**	กระทบหลายส่วนงาน วัตถุประสงค์เชิงยุทธศาสตร์ ชื่อเสียง หรือความต่อเนื่อง ต้องใช้การตัดสินใจหรือทรัพยากรระดับมหาวิทยาลัย
5	**สูงมาก (Severe/Catastrophic)**	กระทบรุนแรงต่อชีวิต กฎหมาย ความอยู่รอด พันธกิจหลัก ระบบสำคัญ หรือความเชื่อมั่นในวงกว้าง และอาจฟื้นฟูได้ยาก

มิติผลกระทบที่ต้องพิจารณาอย่างน้อย ได้แก่

- ยุทธศาสตร์และผลการดำเนินงาน
- การดำเนินงานและคุณภาพบริการ
- การเงินและทรัพย์สิน
- กฎหมาย จริยธรรม และธรรมาภิบาล
- ชื่อเสียงและความเชื่อมั่น
- บุคลากร นักศึกษา สุขภาพ และความปลอดภัย
- ข้อมูล เทคโนโลยี และความมั่นคงปลอดภัยไซเบอร์
- ความต่อเนื่องและความสามารถในการฟื้นตัว
- สิ่งแวดล้อม สังคม และ ESG
- การศึกษา การวิจัย นวัตกรรม และความซื่อสัตย์ทางวิชาการ

เกณฑ์เชิงปริมาณเฉพาะแต่ละมิติให้กำหนดในภาคผนวก และทบทวนตามฐานะการเงิน ขนาดโครงการ กฎหมาย บริบท และระดับผลกระทบที่มหาวิทยาลัยสามารถรองรับได้

4.8.4 การประเมินประสิทธิผลของการควบคุม *(Control Effectiveness Assessment)*

ต้องประเมินความเหมาะสมของการออกแบบ การนำไปใช้ และประสิทธิผลในการปฏิบัติงาน โดยมีเกณฑ์สรุปดังนี้

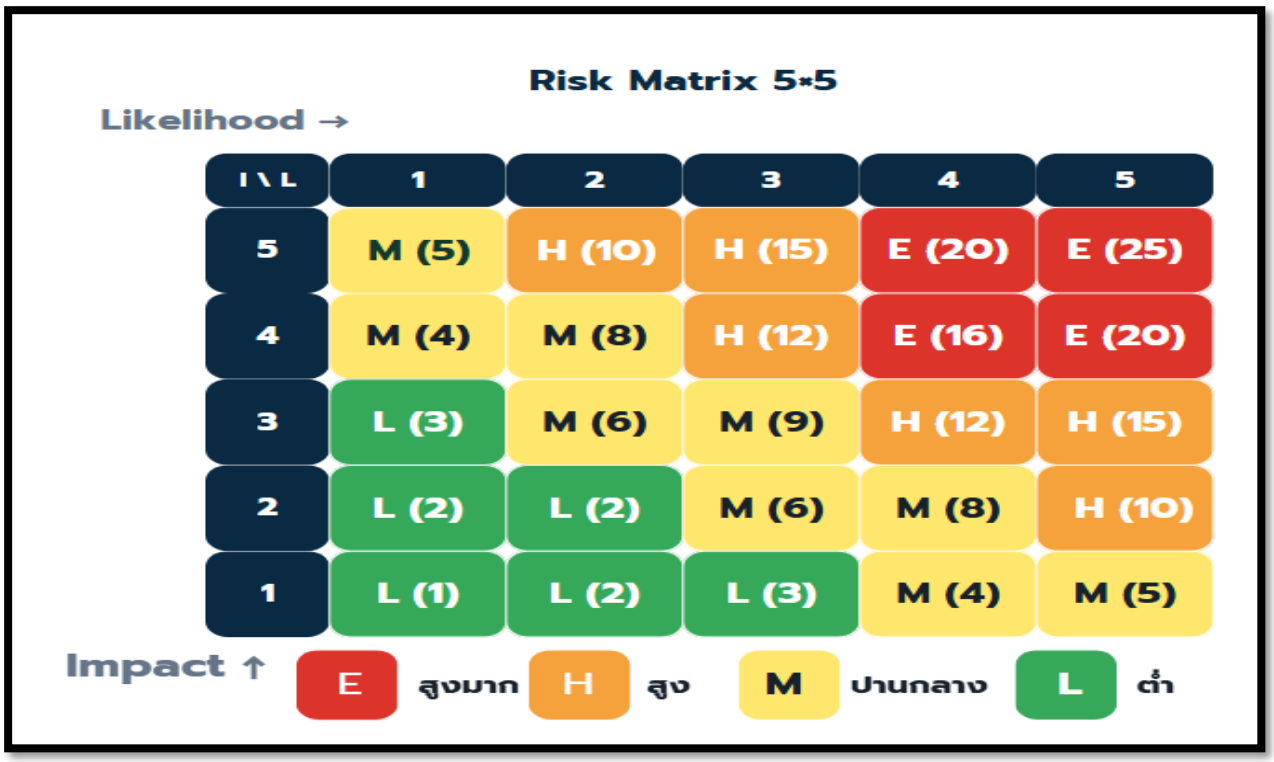
ตารางที่ 4-12 เกณฑ์การพิจารณาระดับผลกระทบ

ระดับ	ข้อพิจารณา
มีประสิทธิผล (Effective)	ออกแบบตอบสนองต่อสาเหตุหรือผลกระทบ มี Control Owner นำไปใช้ครบถ้วน ปฏิบัติสม่ำเสมอ มีหลักฐาน และมีผลการทดสอบสนับสนุน
มีประสิทธิผลบางส่วน (Partially Effective)	มีการควบคุมและนำไปใช้บางส่วน แต่ยังมีช่องว่าง ขอบเขตไม่ครบ ปฏิบัติไม่สม่ำเสมอ พบข้อยกเว้น หรือหลักฐานยังไม่เพียงพอ
ไม่มีประสิทธิผลหรือไม่มีการควบคุม (Ineffective/No Control)	การออกแบบไม่ตอบสนองต่อสาเหตุสำคัญ ไม่ได้นำไปใช้ ไม่ทำงานจริง หรือไม่มีหลักฐานให้ตรวจสอบ

Control Effectiveness ใช้ประกอบดุลยพินิจในการกำหนด Residual Likelihood และ Residual Impact ไม่ควรนำคะแนนการควบคุมไปหักออกจาก Risk Score โดยตรง เว้นแต่มหาวิทยาลัยอนุมัติวิธีคำนวณที่มีหลักการชัดเจน ผ่านการทดสอบ และใช้เป็นมาตรฐานเดียวกันแล้ว

4.8.5 การคำนวณและตารางระดับความเสี่ยง *(Risk Score and Risk Matrix)* ใช้สูตร

คะแนนความเสี่ยง (Risk Score) = โอกาสเกิด (Likelihood) × ผลกระทบ (Impact)



ระดับความเสี่ยงกำหนดทั้งการตอบสนองและอำนาจตัดสินใจ

ตารางจัดระดับและแนวทางดำเนินการ (Risk Level & Response) | ปีงบประมาณ พ.ศ. 2570

Risk Score = Likelihood × Impact

คะแนน	ระดับความเสี่ยง	แนวทางบริหารขั้นต่ำ	ผู้รับผิดชอบและการรายงาน
16–25	E สูงมาก Extreme	**ยกระดับทันทีและเร่งดำเนินมาตรการ** ไม่ยอมรับเป็นงานปกติ · จัดทำแผนเร่งด่วน · กำหนด Target Residual Risk	**ผู้บริหารระดับมหาวิทยาลัย / ผู้กำกับดูแล** แจ้งทันที · รายงานเบื้องต้นไม่เกิน 24 ชม. · ติดตามอย่างใกล้ชิด
10–15	H สูง High	**จัดทำแผนลดความเสี่ยงเป็นลายลักษณ์อักษร** กำหนด Action Owner · ทรัพยากร · กำหนดเวลา · มาตรการแก้ไข	**Risk Owner + ฝ่ายบริหารที่กำกับ** รายงานภายใน 3 วันทำการเมื่อเกิด/เปลี่ยนระดับ หรือ KRI เกิน RT
5–9	M ปานกลาง Medium	**กำหนดมาตรการตามความเหมาะสม** ควบคุมให้อยู่ภายใน RA/RT · ติดตาม KRI และประสิทธิผลการควบคุม	**Risk Owner / หัวหน้าส่วนงาน** ติดตามอย่างน้อยรายไตรมาส หรือตาม Trigger ที่กำหนด
1–4	L ต่ำ Low	**ยอมรับภายในอำนาจและติดตามตามรอบปกติ** คงการควบคุมที่จำเป็น · เฝ้าระวังการเปลี่ยนแปลงของบริบทและ KRI	**Risk Owner** รายงานตามรอบการบริหารงานปกติ และทบทวนเมื่อมีการเปลี่ยนแปลง

เกณฑ์ยกระดับเป็นกรณีพิเศษ (Override)

- Impact = 5 อย่างน้อยระดับ H
- Zero Tolerance ยกระดับทันทีเทียบเท่า E
- KRI เกิน RT / กระทบหลายส่วนงานหรือยุทธศาสตร์ ยกระดับเสนอพิจารณา — ไม่เป็น Enterprise Risk โดยอัตโนมัติ

คะแนนเป็นจุดเริ่มต้นของการพิจารณา ต้องใช้ RA/RT · ประสิทธิผลการควบคุม · หลักฐาน · ความเร่งด่วน และอำนาจตัดสินใจร่วมด้วย

คู่มือการบริหารความเสี่ยงองค์กร มหาวิทยาลัยแม่โจ้ ฉบับปรับปรุง พ.ศ. 2570

Risk · Value · Resilience

เมื่อเกณฑ์นี้ได้รับอนุมัติ คะแนน 4 × 4 = 16 ต้องแสดงเป็นระดับสูงมาก (E) อย่างสม่ำเสมอใน Risk Register, Dashboard, รายงาน และแบบฟอร์มทุกฉบับ

4.8.6 เกณฑ์ยกระดับเป็นกรณีพิเศษ *(Override Criteria)*

1. ผลกระทบระดับ 5 ให้จัดการอย่างน้อยตามแนวทางของความเสี่ยงระดับสูง แม้คะแนนรวมต่ำกว่า 10

2. เหตุ Zero Tolerance ให้ยกระดับรายงานและตอบสนองเทียบเท่าระดับสูงมากทันที โดยไม่รอคะแนนรวม ทั้งนี้ ไม่จำเป็นต้องแก้คะแนน LxI ให้เป็น 16–25 หากคะแนนตามข้อเท็จจริงเป็นอย่างอื่น

3. KRI เกิน RT ความเสี่ยงกระทบหลายส่วนงาน เกินอำนาจของ Risk Owner หรือกระทบวัตถุประสงค์เชิงยุทธศาสตร์ ให้ยกระดับรายงานและเสนอพิจารณาว่าควรเป็น Enterprise Risk หรือไม่ โดยไม่ถือเป็น Enterprise Risk โดยอัตโนมัติ

4. ความเสี่ยงที่มีความเร็วสูง ข้อมูลไม่แน่นอนมาก การควบคุมสำคัญไม่ทำงาน หรืออาจเกิดผลกระทบที่ไม่สามารถฟื้นฟูได้ ให้พิจารณายกระดับเพิ่มเติม

5. หากกฎหมาย แผนฉุกเฉิน หรือนโยบายเฉพาะด้านกำหนดเกณฑ์เข้มงวดกว่า ให้ใช้เกณฑ์ที่เข้มงวดกว่า

การใช้ Override ต้องบันทึกเหตุผล หลักฐาน ผู้เสนอ ผู้พิจารณา วันที่ตัดสินใจ และแนวทางดำเนินการไว้ใน Risk Register หรือ Escalation Record

ตารางที่ 4-13 *ตัวอย่างการวิเคราะห์และประเมินความเสี่ยง*

รายการ	ตัวอย่าง S1: การปรับตัวและใช้ประโยชน์จาก AI
Inherent Likelihood	4 เนื่องจากเทคโนโลยีเปลี่ยนแปลงรวดเร็วและช่องว่างด้านสมรรถนะยังมีอยู่
Inherent Impact	4 เนื่องจากอาจกระทบยุทธศาสตร์ การศึกษา การวิจัย ประสิทธิภาพ และความสามารถในการแข่งขัน
Inherent Risk	4 × 4 = 16 ระดับสูงมาก (E)
การควบคุมที่มีอยู่	นโยบายดิจิทัล การอบรม ระบบสารสนเทศ และคณะทำงานที่เกี่ยวข้อง
Control Effectiveness	มีประสิทธิผลบางส่วน เนื่องจากยังไม่ครอบคลุม AI Governance และการใช้งานทุกส่วนงาน
Residual Likelihood	4
Residual Impact	3
Residual Risk	4 × 3 = 12 ระดับสูง (H)
Target Residual Risk	2 × 2 = 4 ระดับต่ำ (L) หลังดำเนินมาตรการครบถ้วนและยืนยันประสิทธิผล
สถานะเทียบ RA/RT	เกินระดับที่กำหนด ต้องจัดทำแผนลดความเสี่ยงและติดตาม KRI
ประเด็นยกระดับ	ต้องใช้ทรัพยากรและการตัดสินใจระดับมหาวิทยาลัย

ผลลัพธ์ขั้นต่ำของขั้นตอนที่ 4 *(Minimum Outputs of Step 4)*

- คะแนนและเหตุผลของ Inherent Risk
- ผลการประเมิน Control Effectiveness
- คะแนนและเหตุผลของ Residual Risk
- Target Residual Risk และสมมติฐาน
- ผลการเปรียบเทียบกับ RA/RT
- ลำดับความสำคัญของความเสี่ยง
- เกณฑ์ Override ที่เกี่ยวข้อง
- รายการความเสี่ยงที่ต้องยกระดับ
- ข้อมูลและหลักฐานประกอบการประเมิน

4.9 ขั้นตอนที่ 5 การตอบสนองและจัดทำแผนบริหารความเสี่ยง *(Risk Response and Treatment Planning)*

4.9.1 ทางเลือกการตอบสนอง

ตารางที่ 4-14 *ทางเลือกการตอบสนองต่อความเสี่ยง (Risk Response)*

ทางเลือก	ความหมาย	ตัวอย่างการใช้
หลีกเลี่ยง (Avoid)	ยุติ ไม่เริ่ม หรือเปลี่ยนกิจกรรมที่เป็นแหล่งความเสี่ยง	ยุติโครงการที่ผิดกฎหมาย เกิน Risk Capacity หรือไม่มีมาตรการลดความเสี่ยงที่เพียงพอ
ลดหรือควบคุม (Reduce)	ลดโอกาสเกิด ผลกระทบ หรือเพิ่มความสามารถในการตรวจพบ ตอบสนอง และฟื้นตัว	ปรับกระบวนงาน แบ่งแยกหน้าที่ เพิ่มการตรวจสอบ สำรองระบบ หรือพัฒนาสมรรถนะ
แบ่งปันหรือถ่ายโอน (Share/Transfer)	แบ่งภาระทางการเงินหรือการดำเนินงานกับบุคคลอื่น โดยมหาวิทยาลัยยังคงกำกับและรับผิดชอบต่อความเสี่ยงคงเหลือ	ประกันภัย สัญญา พันธมิตร หรือ Outsource พร้อม SLA และการกำกับผู้ให้บริการ
ยอมรับ (Accept)	คงความเสี่ยงไว้ภายใน RA/RT และอำนาจที่ได้รับมอบหมาย โดยติดตามตามเงื่อนไข	ไม่เพิ่มมาตรการเมื่อความเสี่ยงอยู่ในเกณฑ์และต้นทุนมาตรการไม่คุ้มกับประโยชน์
ใช้ประโยชน์หรือเพิ่มโอกาส (Pursue/Enhance)	ตัดสินใจรับหรือเพิ่มความเสี่ยงอย่างมีข้อมูลเพื่อสร้างคุณค่า	ทดลองนวัตกรรมแบบ Pilot หรือ Sandbox พร้อม Guardrails, Stop Criteria และการติดตาม

การเลือกแนวทางต้องพิจารณา

- ความสอดคล้องกับ RA/RT และ Risk Capacity
- กฎหมาย ข้อกำหนด และ Zero Tolerance
- ผลดี ผลเสีย และผลกระทบต่อวัตถุประสงค์
- ต้นทุนเทียบกับประโยชน์
- ความเป็นไปได้และระยะเวลาดำเนินการ
- ทรัพยากรและความสามารถของผู้รับผิดชอบ
- ผลกระทบต่อผู้มีส่วนได้ส่วนเสีย
- ความเสี่ยงใหม่หรือผลข้างเคียงจากมาตรการ
- ความเสี่ยงคงเหลือภายหลังดำเนินมาตรการ

อาจใช้หลายทางเลือกร่วมกันได้ หากทางเลือกเดียวไม่เพียงพอ

4.9.2 องค์ประกอบของแผนบริหารความเสี่ยง *(Risk Treatment Plan)*

แผนต้องระบุอย่างน้อย

1. ความเสี่ยง สาเหตุ และปัจจัยขับเคลื่อนที่มาตรการต้องตอบสนอง
2. วัตถุประสงค์และผลลัพธ์ที่ต้องการ
3. Residual Risk ปัจจุบันและ Target Residual Risk
4. มาตรการ กิจกรรม และผลส่งมอบที่ตรวจสอบได้
5. Action Owner, Control Owner และหน่วยงานร่วม
6. วันที่เริ่มต้น วันที่สิ้นสุด และ Milestone
7. ทรัพยากรและงบประมาณ
8. KPI ของมาตรการ KCI ของการควบคุม และ KRI ของความเสี่ยง
9. นิยาม สูตร แหล่งข้อมูล ความถี่ และ Data Owner
10. หลักฐานที่ต้องส่งมอบ
11. ความเสี่ยงหรือผลข้างเคียงจากการดำเนินมาตรการ
12. แผนสำรองหรือมาตรการชดเชย
13. Trigger และ Corrective Action เมื่อมาตรการล่าช้าหรือไม่ได้ผล
14. รอบการติดตามและเกณฑ์การยกระดับ
15. ผู้พิจารณาและผู้อนุมัติ

ความเสี่ยงระดับสูงและสูงมากต้องมีแผนเป็นลายลักษณ์อักษร การยอมรับความเสี่ยงต้องได้รับอนุมัติจากผู้มีอำนาจ พร้อมบันทึกเหตุผล เงื่อนไข ระยะเวลาที่อนุมัติ และวันที่ทบทวน

เหตุ Zero Tolerance ไม่สามารถยอมรับเป็นการดำเนินงานตามปกติ ต้องระงับเหตุ รายงาน รักษาหลักฐาน ตรวจสอบ และดำเนินการตามกฎหมายหรือนโยบายที่เกี่ยวข้อง

ตารางที่ 4-15 *องค์ประกอบและตัวอย่างแผนบริหารความเสี่ยง (Risk Treatment Plan)*

ตัวอย่าง Risk Treatment Plan แบบย่อ

ความเสี่ยง: S1 มหาวิทยาลัยอาจปรับตัวและใช้ประโยชน์จาก AI และเทคโนโลยีดิจิทัลไม่ทันต่อการเปลี่ยนแปลง

องค์ประกอบ	ตัวอย่าง
Residual Risk	4 × 3 = 12 ระดับสูง (H)
Target Residual Risk	2 × 2 = 4 ระดับต่ำ (L) ภายในสิ้นปีงบประมาณ พ.ศ. 2570
Response	ลดความเสี่ยงและใช้ประโยชน์จากโอกาส (Reduce and Pursue)
มาตรการ 1	จัดทำ AI Governance Framework ครอบคลุมนโยบาย บทบาท มาตรฐานข้อมูล จริยธรรม ความปลอดภัย และการอนุมัติ Use Case
Deliverable	นโยบายและแนวปฏิบัติ AI ที่ได้รับอนุมัติ พร้อมแบบประเมินความเสี่ยง AI
Action Owner	ผู้บริหารและหน่วยงานที่กำกับด้านยุทธศาสตร์ ดิจิทัล และกฎหมาย

Milestone	ร่างกรอบ ⟶ รับฟังความคิดเห็น ⟶ ทดลองใช้ ⟶ อนุมัติและประกาศใช้
มาตรการ 2	พัฒนาสมรรถนะ AI/Digital Literacy ตามกลุ่มบุคลากรและเชื่อมโยงกับ IDP
KRI	ร้อยละบุคลากรที่ผ่านเกณฑ์ AI/Digital Literacy
RA/RT	RA ≥80%; RT 70–<80%; ต่ำกว่า 70% ให้เร่งรัดและยกระดับ
มาตรการ 3	ดำเนินโครงการ AI Use Cases แบบ Pilot/Sandbox พร้อม Guardrails และการประเมินก่อนขยายผล
หลักฐาน	กรอบที่อนุมัติ ผลการประเมินบุคลากร รายงาน Pilot ผลการประเมินความเสี่ยง และ Decision Log
Trigger	Milestone ล่าช้าเกิน 30 วัน KRI ต่ำกว่า RT หรือพบเหตุด้านกฎหมาย/ข้อมูลที่มีนัยสำคัญ
Corrective Action	เสนอปรับทรัพยากร แผน และผู้รับผิดชอบต่อฝ่ายบริหารภายในรอบที่กำหนด
ผู้อนุมัติ	ผู้มีอำนาจตามระดับความเสี่ยงและโครงสร้างการกำกับของมหาวิทยาลัย

ผลลัพธ์ขั้นต่ำของขั้นตอนที่ 5 *(Minimum Outputs of Step 5)*

- ผลการตัดสินใจเลือกแนวทางตอบสนอง *(Risk Response Decision)*
- แผนบริหารความเสี่ยง *(Risk Treatment Plan)*
- Action Owner, Control Owner และหน่วยงานร่วม
- ทรัพยากรและงบประมาณที่ได้รับอนุมัติ
- Milestone และกำหนดแล้วเสร็จ
- KPI, KCI, KRI และ Data Owner
- Target Residual Risk
- Trigger, Corrective Action และเกณฑ์ยกระดับ
- ผู้พิจารณาและผู้อนุมัติ
- บันทึกการยอมรับความเสี่ยง หากเลือก Accept *(Risk Acceptance Record)*

4.10 ขั้นตอนที่ 6 การดำเนินการควบคุมและมาตรการ *(Implement Controls and Risk Treatment Actions)*

Risk Owner รับผิดชอบกำกับให้การควบคุมและมาตรการตอบสนองความเสี่ยงได้รับการดำเนินการอย่างเหมาะสม ขณะที่ Control Owner รับผิดชอบดำเนินการควบคุมที่มีอยู่ และ Action Owner รับผิดชอบดำเนินมาตรการเพิ่มเติมตามแผนบริหารความเสี่ยง โดยต้องจัดเก็บหลักฐานที่ตรวจสอบย้อนกลับได้และแสดงให้เห็นทั้งความเหมาะสมของการออกแบบ การนำไปใช้ และการทำงานจริงของการควบคุม

การควบคุมอาจจำแนกตามวัตถุประสงค์ได้ดังนี้

1. **การควบคุมเชิงป้องกัน (Preventive Control):** ป้องกันหรือลดโอกาสเกิดเหตุการณ์ก่อนเกิดความเสียหาย เช่น การแบ่งแยกหน้าที่ การอนุมัติตามลำดับอำนาจ การกำหนดสิทธิ์เข้าถึงระบบ การตรวจสอบคุณสมบัติก่อนรับบุคลากร และการสำรองข้อมูลตามรอบ

2. **การควบคุมเชิงตรวจจับ (Detective Control):** ตรวจพบข้อผิดพลาด เหตุผิดปกติ หรือการไม่ปฏิบัติตามข้อกำหนดภายหลังหรือระหว่างการดำเนินงาน เช่น การกระทบยอดบัญชี รายงานข้อยกเว้น การติดตาม Log ระบบ การตรวจนับทรัพย์สิน และการติดตามสัญญาณเตือนความมั่นคงปลอดภัยไซเบอร์

3. **การควบคุมเชิงแก้ไข (Corrective Control):** แก้ไข ฟื้นฟู และป้องกันการเกิดซ้ำภายหลังพบเหตุหรือข้อบกพร่อง เช่น การตอบสนองต่อเหตุการณ์ แผนปฏิบัติการแก้ไขและป้องกัน (Corrective and Preventive Action: CAPA) การกู้คืนข้อมูลจากระบบสำรอง และการดำเนินการตามแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP)

4. **การควบคุมเชิงกำกับหรือชี้นำ (Directive Control):** กำหนดทิศทาง พฤติกรรม และวิธีปฏิบัติที่คาดหวัง เช่น นโยบาย ระเบียบ คู่มือ มาตรฐานการปฏิบัติงาน การอบรม และประมวลจริยธรรม (Code of Conduct)

การควบคุมแต่ละรายการต้องกำหนดอย่างน้อย ดังนี้

- วัตถุประสงค์ของการควบคุม (Control Objective)
- ความเสี่ยงหรือสาเหตุที่การควบคุมต้องตอบสนอง
- เจ้าของการควบคุม (Control Owner)
- วิธีดำเนินการและความถี่
- หลักฐานที่ต้องจัดเก็บ
- เกณฑ์ผ่าน–ไม่ผ่าน
- วิธีทดสอบหรือประเมินประสิทธิผล
- ผู้รับผิดชอบและระยะเวลาแก้ไขข้อบกพร่อง
- เส้นทางรายงานเมื่อการควบคุมไม่ทำงาน

การมีนโยบาย ระเบียบ คู่มือ หรือคำสั่งเพียงอย่างเดียวไม่เพียงพอที่จะสรุปว่าการควบคุมมีประสิทธิผล ต้องมีหลักฐานว่าการควบคุมได้รับการนำไปใช้จริง ปฏิบัติอย่างสม่ำเสมอ ครอบคลุมกลุ่มเป้าหมาย และสามารถลดโอกาสเกิดหรือผลกระทบของความเสี่ยงได้ตามวัตถุประสงค์

ตารางที่ 4-16 *ตัวอย่างการดำเนินการควบคุม: ความเสี่ยงด้าน Cybersecurity และ PDPA*

ประเภทการควบคุม	ตัวอย่างการควบคุม	เจ้าของการควบคุม	ความถี่/หลักฐาน	เกณฑ์ผ่าน
Preventive ป้องกันก่อนเกิดเหตุ	ติดตั้ง Security Patch สำหรับระบบสำคัญภายในระยะเวลาที่กำหนด	ผู้ดูแลระบบ	รายเดือน; Patch Report และ System Log	ระบบสำคัญได้รับ Patch ตาม SLA ไม่น้อยกว่าร้อยละ 95

ประเภทการควบคุม	ตัวอย่างการควบคุม	เจ้าของการควบคุม	ความถี่/หลักฐาน	เกณฑ์ผ่าน
Detective ตรวจพบความผิดปกติ	ติดตามเหตุผิดปกติจาก Firewall/SIEM และตรวจสอบ Failed Login	ศูนย์เฝ้าระวังความปลอดภัย	ต่อเนื่อง; Alert Log และ Incident Ticket	Alert ระดับรุนแรงได้รับการตรวจสอบภายในเวลาที่กำหนด
Corrective แก้ไขและฟื้นฟู	ระงับบัญชีที่ถูกโจมตี กู้คืนระบบ และวิเคราะห์สาเหตุราก	Incident Response Team	เมื่อเกิดเหตุ; Incident Report และ RCA	ควบคุมเหตุและฟื้นคืนระบบภายใน RTO
Directive กำหนดทิศทาง	กำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์และอบรมบุคลากร	หน่วยงานด้านดิจิทัล/ทรัพยากรบุคคล	อย่างน้อยปีละครั้ง; รายชื่อและผลทดสอบ	บุคลากรกลุ่มเป้าหมายผ่านการอบรมไม่น้อยกว่าร้อยละ 90

หากผลการตรวจสอบพบว่าการติดตั้ง Security Patch ครอบคลุมเพียงร้อยละ 88 แม้มหาวิทยาลัยจะมีนโยบายและขั้นตอนปฏิบัติครบถ้วน ให้ประเมินว่าการควบคุม “มีประสิทธิผลบางส่วน” และจัดทำ Corrective Action โดยไม่ลดคะแนน Residual Risk จนกว่าจะมีหลักฐานว่าการแก้ไขดำเนินการแล้วและการควบคุมทำงานได้ตามเกณฑ์

ผลลัพธ์ขั้นต่ำ (Minimum Outputs): หลักฐานการดำเนินงาน ผลการทดสอบการควบคุม รายการข้อบกพร่อง แผนแก้ไขข้อบกพร่อง (Corrective Action) ผู้รับผิดชอบ กำหนดแล้วเสร็จ และผลการติดตาม

4.11 ขั้นตอนที่ 7 การสื่อสาร การรายงาน และการยกระดับ *(Communication, Reporting and Escalation)*

4.11.1 หลักการของข้อมูลความเสี่ยง

ข้อมูลความเสี่ยงต้องถูกต้อง ครบถ้วน ทันเวลา สอดคล้องกัน ตรวจสอบย้อนกลับได้ มีเจ้าของข้อมูล และได้รับการคุ้มครองตามระดับชั้นความลับและกฎหมายที่เกี่ยวข้อง

การรายงานต้องมุ่งแสดงแนวโน้ม สาเหตุ ผลกระทบ ระดับความเสี่ยง ประสิทธิผลของการควบคุม ประเด็นที่เข้าใกล้หรือเกิน RA/RT และการตัดสินใจหรือทรัพยากรที่ต้องการ ไม่ควรรายงานเฉพาะจำนวนกิจกรรมหรือร้อยละความสำเร็จของแผน โดยไม่แสดงว่าระดับความเสี่ยงลดลงหรือไม่

4.11.2 การกำหนดตัวชี้วัดความเสี่ยงที่สำคัญ

ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ต้องเชื่อมโยงกับสาเหตุ ปัจจัยขับเคลื่อนเหตุการณ์ หรือการเปลี่ยนแปลงของระดับความเสี่ยง และต้องกำหนดองค์ประกอบอย่างน้อย ดังนี้

1. ชื่อและนิยามตัวชี้วัด
2. วัตถุประสงค์หรือความเสี่ยงที่เชื่อมโยง
3. สูตรคำนวณและหน่วยวัด
4. แหล่งข้อมูลและเจ้าของข้อมูล (Data Owner)

5. ความถี่ในการจัดเก็บและรายงาน
6. ค่าฐาน (Baseline) และแนวโน้ม
7. ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA)
8. ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT)
9. จุดกระตุ้นการดำเนินการ (Trigger)
10. การดำเนินการเมื่อเข้าใกล้หรือเกินเกณฑ์
11. ผู้รับรายงานและผู้มีอำนาจตัดสินใจ

ควรกำหนดทั้ง

- **ตัวชี้วัดนำ (Leading Indicator):** สะท้อนปัจจัยที่อาจทำให้ความเสี่ยงเพิ่มขึ้นก่อนเกิดผลกระทบ เช่น อัตราการติดตั้ง Patch การผ่านการอบรม หรือจำนวน Alert ที่ยังไม่ได้ตรวจสอบ
- **ตัวชี้วัดตาม (Lagging Indicator):** สะท้อนเหตุการณ์หรือผลกระทบที่เกิดขึ้นแล้ว เช่น จำนวนเหตุข้อมูลรั่วไหล ระยะเวลาระบบหยุดชะงัก หรือมูลค่าความเสียหาย

ตารางที่ 4-17 *ตัวอย่างการกำหนดตัวชี้วัดความเสี่ยงที่สำคัญ (KRI)*

รายการ	ตัวอย่าง
ความเสี่ยง	ระบบสารสนเทศสำคัญอาจถูกโจมตีหรือหยุดชะงัก ส่งผลต่อข้อมูลและความต่อเนื่องของพันธกิจ
Leading KRI	ร้อยละของระบบสำคัญที่ติดตั้ง Security Patch ภายใน SLA
สูตร	จำนวนระบบสำคัญที่ติดตั้ง Patch ภายใน SLA ÷ จำนวนระบบสำคัญทั้งหมด × 100
Data Owner	หน่วยงานด้านเทคโนโลยีดิจิทัล
ความถี่	รายเดือน
ภายใน RA	ตั้งแต่ร้อยละ 95 ขึ้นไป
ช่วงเฝ้าระวัง RT	ตั้งแต่ร้อยละ 90 แต่ต่ำกว่าร้อยละ 95
เกิน RT	ต่ำกว่าร้อยละ 90
Trigger/Action	ต่ำกว่าร้อยละ 95 ให้จัดทำแผนเร่งรัด; ต่ำกว่าร้อยละ 90 ให้รายงานและยกระดับภายใน 3 วันทำการ
Lagging KRI	จำนวนเหตุข้อมูลรั่วไหลที่มีผลกระทบรุนแรง และระยะเวลาหยุดชะงักของระบบสำคัญ

4.11.3 องค์ประกอบขั้นต่ำของรายงาน

รายงานความเสี่ยงควรประกอบด้วยอย่างน้อย

- ภาพรวมความเสี่ยงระดับมหาวิทยาลัยหรือส่วนงาน (University/Unit Risk Profile)
- Inherent Risk, Residual Risk และ Target Residual Risk
- แนวโน้มความเสี่ยงและการเปลี่ยนแปลงจากรอบก่อน
- ผล KRI เปรียบเทียบกับ RA/RT
- ประสิทธิผลและข้อบกพร่องของการควบคุม

- ความก้าวหน้าของมาตรการและมาตรการที่ล่าช้า
- เหตุการณ์ ความเสียหาย และ Near Miss
- ความเสี่ยงเกิดใหม่ (Emerging Risk)
- ความสัมพันธ์ การกระจุกตัว และผลกระทบร่วมระหว่างความเสี่ยง
- ประเด็นที่ต้องการการตัดสินใจ อำนาจ หรือทรัพยากร
- ความเชื่อมั่นและข้อจำกัดของข้อมูลที่รายงาน

4.11.4 เกณฑ์เวลาในการรายงาน

ตารางที่ 4-18 *เกณฑ์และระยะเวลาการรายงาน/ยกระดับความเสี่ยง*

เหตุหรือระดับความเสี่ยง	เวลารายงานขั้นต่ำ
เหตุ Zero Tolerance เหตุวิกฤต Impact ระดับ 5 หรือภัยคุกคามต่อชีวิต หรือข้อมูลสำคัญ	รายงานทันที และจัดทำรายงานเบื้องต้นไม่เกิน 24 ชั่วโมง
ระดับสูงมาก 16–25	ยกระดับทันที และรายงานไม่เกิน 24 ชั่วโมง
ระดับสูง 10–15, KRI เกิน RT หรือมาตรการสำคัญล่าช้า	รายงานภายใน 3 วันทำการ
ระดับปานกลาง 5–9	อย่างน้อยรายไตรมาส หรือตามรอบที่กำหนด
ระดับต่ำ 1–4	รายงานตามรอบปกติ

หากกฎหมาย แผนฉุกเฉิน แผนสื่อสารภาวะวิกฤต หรือนโยบายเฉพาะกำหนดระยะเวลาที่สั้นกว่าหรือเคร่งครัดกว่า ให้ใช้ข้อกำหนดที่เคร่งครัดกว่า

การรายงานไม่ทดแทนการระงับเหตุ ผู้รับผิดชอบต้องดำเนินการคุ้มครองชีวิต ข้อมูล ทรัพย์สิน ความต่อเนื่อง และหลักฐานควบคู่กับการรายงาน

ตัวอย่างการรายงานและยกระดับ

ผลการติดตามพบว่าอัตราการติดตั้ง Security Patch ของระบบสำคัญลดลงจากร้อยละ 97 เป็นร้อยละ 93 และร้อยละ 88 ติดต่อกันสามเดือน จึงถือว่า KRI เกิน RT หน่วยงานต้องดำเนินการดังนี้

1. Data Owner ยืนยันความถูกต้องและสาเหตุของข้อมูล
2. Control Owner เร่งแก้ไขระบบที่ยังไม่ได้ติดตั้ง Patch
3. Risk Owner ประเมิน Residual Risk และผลกระทบต่อระบบสำคัญ
4. จัดทำ Corrective Action พร้อมผู้รับผิดชอบและกำหนดเสร็จ
5. รายงานหน่วยบริหารความเสี่ยงและผู้บริหารที่กำกับภายใน 3 วันทำการ
6. หากพบการโจมตีหรือข้อมูลสำคัญรั่วไหล ให้ยกระดับทันทีตามเกณฑ์เหตุวิกฤตหรือ Zero Tolerance

ผลลัพธ์ขั้นต่ำ (Minimum Outputs): KRI Dashboard, Risk Report, Incident/Escalation Record, Corrective Action และบันทึกการตัดสินใจ (Decision Log)

4.12 ขั้นตอนที่ 8 การติดตาม ทบทวน และปรับปรุงอย่างต่อเนื่อง *(Monitoring, Review and Continual Improvement)*

การติดตามและทบทวนมีวัตถุประสงค์เพื่อประเมินว่าระดับความเสี่ยง บริบท และประสิทธิผลของการควบคุมเปลี่ยนแปลงไปอย่างไร มาตรการดำเนินการได้ตามแผนและสามารถลดความเสี่ยงได้จริงหรือไม่ รวมทั้งนำผลที่ได้รับไปปรับปรุงระบบอย่างต่อเนื่อง

การดำเนินมาตรการครบถ้วนตามจำนวนกิจกรรมไม่ถือว่าความเสี่ยงลดลงโดยอัตโนมัติ การเปลี่ยนระดับ Residual Risk ต้องมีข้อมูลและหลักฐานยืนยันว่าการควบคุมหรือมาตรการได้รับการนำไปใช้และมีประสิทธิผลจริง

4.12.1 การติดตามโดยฝ่ายบริหาร *(Management Monitoring)*

Risk Owner ต้องติดตามอย่างน้อยในประเด็นต่อไปนี้

1. ระดับและแนวโน้มของ Inherent Risk, Residual Risk และ Target Residual Risk
2. ผล KRI เปรียบเทียบกับ Risk Appetite (RA) และ Risk Tolerance (RT)
3. ประสิทธิผลและข้อบกพร่องของการควบคุมสำคัญ
4. ความก้าวหน้า คุณภาพ และความล่าช้าของมาตรการ
5. เหตุการณ์ Near Miss ข้อร้องเรียน และความเสียหายที่เกิดขึ้น
6. การเปลี่ยนแปลงของบริบท สมมติฐาน กฎหมาย เทคโนโลยี และผู้มีส่วนได้ส่วนเสีย
7. ความเสี่ยงเกิดใหม่และความสัมพันธ์กับความเสี่ยงอื่น
8. ประเด็นที่ต้องการอำนาจตัดสินใจหรือทรัพยากรเพิ่มเติม

ตารางที่ 4-19 *ความถี่ขั้นต่ำในการติดตามตามระดับความเสี่ยง*

ระดับความเสี่ยง	ความถี่ขั้นต่ำ	แนวทางดำเนินการ
สูงมาก 16–25	อย่างน้อยรายเดือน หรือทันทีเมื่อเกิด Trigger	เร่งดำเนินมาตรการและรายงานผู้บริหารระดับสูง
สูง 10–15	อย่างน้อยรายไตรมาส หรือถี่กว่าตาม KRI และเหตุการณ์	ติดตามแผนลดความเสี่ยงและประเด็นเกิน RA/RT
ปานกลาง 5–9	อย่างน้อยรายไตรมาสหรือตามรอบที่กำหนด	ติดตามโดย Risk Owner และปรับมาตรการตามความจำเป็น
ต่ำ 1–4	ตามรอบการบริหารงานปกติ	ยอมรับและเฝ้าระวังการเปลี่ยนแปลง

หาก KRI เกิน RT เกิดเหตุ Zero Tolerance การควบคุมสำคัญล้มเหลว หรือบริบทเปลี่ยนแปลงอย่างมีนัยสำคัญ ต้องดำเนินการและยกระดับตามเกณฑ์ทันทีโดยไม่รอรอบรายงานปกติ

ตัวอย่าง: ผล KRI ด้านการติดตั้ง Security Patch ของระบบสำคัญลดลงจากร้อยละ 97 เป็นร้อยละ 93 และร้อยละ 88 ติดต่อกันสามเดือน โดยเกณฑ์ภายใน RA เท่ากับไม่น้อยกว่าร้อยละ 95 และเกิน RT เมื่อต่ำกว่าร้อยละ 90 Risk Owner ต้องสั่งการแก้ไข ประเมิน Residual Risk ใหม่ และรายงานผู้บริหารภายในระยะเวลาที่กำหนด

4.12.2 การทบทวนทะเบียนความเสี่ยง *(Risk Register Review)*

Risk Register ต้องได้รับการทบทวนเมื่อสิ้นรอบรายงาน และเมื่อเกิดเงื่อนไขกระตุ้น (Trigger) อย่างน้อยกรณีต่อไปนี้

- วัตถุประสงค์ ยุทธศาสตร์ KPI หรือค่าเป้าหมายเปลี่ยนแปลง
- มีกฎหมาย นโยบาย มาตรฐาน หรือข้อกำหนดใหม่
- เกิดเหตุการณ์ Near Miss ข้อร้องเรียน หรือความเสียหายสำคัญ
- การควบคุมสำคัญล้มเหลวหรือไม่ทำงานตามที่ออกแบบ
- KRI เข้าใกล้หรือเกิน RT
- โครงการ การลงทุน ระบบงาน หรือโครงสร้างองค์กรเปลี่ยนแปลง
- เกิดความเสี่ยงใหม่หรือความเสี่ยงที่กระทบหลายส่วนงาน
- ผลการตรวจสอบหรือการให้ความเชื่อมั่นพบข้อบกพร่องสำคัญ
- สมมติฐานที่ใช้ประเมินความเสี่ยงไม่เป็นจริง

การทบทวนต้องบันทึกอย่างน้อย

1. วันที่และช่วงเวลาที่ประเมิน
2. ข้อมูล หลักฐาน และสมมติฐานที่ใช้
3. ผู้ประเมิน Risk Owner และผู้อนุมัติ
4. การเปลี่ยนแปลงของสาเหตุ เหตุการณ์ และผลกระทบ
5. คะแนนเดิม คะแนนใหม่ และเหตุผลของการเปลี่ยนคะแนน
6. ผลการประเมินประสิทธิผลของการควบคุม
7. สถานะ KRI และมาตรการ
8. การตัดสินใจ การยอมรับ หรือการยกระดับความเสี่ยง
9. รอบการติดตามครั้งถัดไป

ห้ามลดคะแนน Residual Risk จากมาตรการที่ยังไม่แล้วเสร็จ หรือมาตรการที่ยังไม่มีหลักฐานยืนยันการทำงานจริง ส่วนระดับความเสี่ยงที่คาดว่าจะเหลือภายหลังดำเนินมาตรการให้บันทึกเป็น Target Residual Risk แยกต่างหาก

ตัวอย่าง: ระบบสำคัญมี Inherent Risk เท่ากับ 20 คะแนน และ Residual Risk เท่ากับ 15 คะแนน แม้ส่วนงานจะอนุมัติโครงการปรับปรุงระบบสำรองแล้ว แต่ยังไม่ติดตั้งและทดสอบ จึงต้องคง Residual Risk ไว้ที่ 15 คะแนน ส่วนระดับที่คาดว่าจะลดลงเหลือ 8 คะแนนให้บันทึกเป็น Target Residual Risk จนกว่าจะมีหลักฐานการดำเนินงานและผลทดสอบที่เพียงพอ

4.12.3 การให้ความเชื่อมั่น *(Assurance)*

การติดตามและการให้ความเชื่อมั่นให้ดำเนินการตามหลัก Three Lines ดังนี้

1. **บทบาทแนวที่หนึ่ง (First Line):** Risk Owner, Control Owner และ Action Owner ติดตามการควบคุม การดำเนินมาตรการ และผลลัพธ์ในงานที่รับผิดชอบ
2. **บทบาทแนวที่สอง (Second Line):** หน่วยงานบริหารความเสี่ยง การควบคุมภายใน กฎหมาย Compliance ไซเบอร์ PDPA ความปลอดภัย และหน้าที่กำกับเฉพาะด้าน ให้คำปรึกษา กำหนดมาตรฐาน ติดตาม ท้าทายคุณภาพข้อมูล และรายงานภาพรวม โดยไม่รับผิดชอบแทน Risk Owner
3. **บทบาทแนวที่สาม (Third Line):** กองตรวจสอบภายในให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระต่อความเพียงพอและประสิทธิผลของการกำกับดูแล การบริหารความเสี่ยง และการควบคุม โดยไม่ออกแบบหรือดำเนินการควบคุมแทนฝ่ายบริหาร
4. **ผู้ให้ความเชื่อมั่นอื่น (Other Assurance Providers):** ผู้สอบบัญชี ผู้ประเมินภายนอก หน่วยรับรอง และหน่วยงานกำกับดูแลให้ความเชื่อมั่นตามขอบเขต อำนาจหน้าที่ และความเชี่ยวชาญของแต่ละหน่วยงาน

มหาวิทยาลัยควรจัดทำแผนที่การให้ความเชื่อมั่น (Assurance Map) เพื่อแสดงว่าความเสี่ยงสำคัญได้รับการประเมินจากแหล่งใด มีความถี่และระดับความเป็นอิสระเพียงใด รวมทั้งระบุความซ้ำซ้อนและช่องว่างที่ยังไม่ได้รับความเชื่อมั่น

ตัวอย่าง: Risk Owner รายงานว่าการสำรองข้อมูลดำเนินการครบถ้วนทุกวัน หน่วยงานแนวที่สองตรวจสอบ Backup Log และพบว่ามีการสำรองจริง แต่กองตรวจสอบภายในทดสอบการกู้คืนแล้วพบว่าบางระบบไม่สามารถกู้คืนภายใน RTO ได้ จึงยังไม่ควรสรุปว่าการควบคุมมีประสิทธิผลครบถ้วน และต้องจัดทำ Corrective Action พร้อมติดตามผลการทดสอบซ้ำ

4.12.4 ความต่อเนื่องและความยืดหยุ่นขององค์กร *(Business Continuity and Organizational Resilience)*

ความเสี่ยงที่อาจทำให้พันธกิจสำคัญหยุดชะงักต้องเชื่อมโยงกับ

- การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)
- การบริหารความต่อเนื่อง (Business Continuity Management: BCM)
- แผนความต่อเนื่องในการดำเนินงาน (Business Continuity Plan: BCP)
- การสื่อสารภาวะวิกฤต (Crisis Communication)

- การตอบสนองต่อเหตุการณ์ (Incident Response)
- แผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP)
- เป้าหมายระยะเวลาการกู้คืน (Recovery Time Objective: RTO)
- เป้าหมายจุดการกู้คืนข้อมูล (Recovery Point Objective: RPO)

ส่วนงานต้องกำหนดภารกิจสำคัญ ทรัพยากรขั้นต่ำ ผู้รับผิดชอบ วิธีดำเนินงานทดแทน การติดต่อสื่อสาร และลำดับการกู้คืน พร้อมทดสอบแผนตามรอบที่กำหนด วิเคราะห์ช่องว่าง และติดตามการแก้ไขจนแล้วเสร็จ

การมีเอกสาร BCP หรือ DRP โดยไม่มีการทดสอบ ไม่เพียงพอที่จะสรุปว่ามหาวิทยาลัยมีความพร้อมต่อเหตุหยุดชะงัก

ตัวอย่าง: มหาวิทยาลัยกำหนดให้ระบบทะเบียนนักศึกษามี RTO ไม่เกิน 4 ชั่วโมง และ RPO ไม่เกิน 1 ชั่วโมง แต่ผลการทดสอบพบว่าใช้เวลากู้คืน 7 ชั่วโมง และข้อมูลล่าสุดที่กู้คืนได้ย้อนหลัง 3 ชั่วโมง จึงถือว่ายังไม่ผ่านเกณฑ์ ต้องวิเคราะห์สาเหตุ ปรับระบบสำรอง และทดสอบซ้ำจนบรรลุ RTO/RPO ที่กำหนด

4.12.5 การเรียนรู้และปรับปรุง *(Learning and Improvement)*

มหาวิทยาลัยต้องนำข้อมูลจากเหตุการณ์ Near Miss ข้อร้องเรียน ผลการตรวจสอบ การทดสอบแผน ข้อมูลคู่เทียบ และบทเรียนจากการดำเนินงานมาวิเคราะห์สาเหตุราก (Root Cause Analysis) และใช้ปรับปรุงอย่างน้อยในเรื่องต่อไปนี้

- นโยบายและกระบวนงาน
- การควบคุมและมาตรการ
- KRI, RA, RT และ Trigger
- ระบบข้อมูลและคุณภาพข้อมูล
- สมรรถนะของบุคลากร
- BCM, BCP และ DRP
- วัฒนธรรมความเสี่ยง (Risk Culture)
- โครงสร้างบทบาทและอำนาจตัดสินใจ

การปิดประเด็นต้องแสดงให้เห็นว่ามาตรการสามารถแก้ไขสาเหตุราก ลดระดับความเสี่ยง หรือเพิ่มความพร้อมได้จริง มิใช่พิจารณาเพียงว่ากิจกรรมดำเนินการครบถ้วนแล้ว

ตัวอย่าง: ภายหลังเกิดเหตุส่งอีเมลข้อมูลส่วนบุคคลผิดผู้รับ การแก้ไขไม่ควรจำกัดเพียงการตักเตือนหรืออบรมซ้ำ แต่ต้องวิเคราะห์สาเหตุราก เช่น สิทธิ์เข้าถึงข้อมูล ขั้นตอนตรวจสอบก่อนส่ง การตั้งชื่อไฟล์ และข้อจำกัดของระบบ แล้วพิจารณาเพิ่ม Data Loss Prevention, การเข้ารหัสไฟล์ และการอนุมัติก่อนส่งข้อมูลสำคัญ พร้อมติดตามว่าเหตุลักษณะเดียวกันลดลงจริงหรือไม่

ผลลัพธ์ขั้นต่ำ (Minimum Outputs):

- ทะเบียนความเสี่ยงฉบับปรับปรุง (Updated Risk Register)
- รายงานการทบทวนโดยฝ่ายบริหาร (Management Review)
- ข้อค้นพบจากการให้ความเชื่อมั่น (Assurance Findings)
- บทเรียนที่ได้รับ (Lessons Learned)
- แผนปรับปรุงระบบ (System Improvement Plan)

4.13 การควบคุมคุณภาพข้อมูลและเอกสารความเสี่ยง *(Risk Data and Documentation Quality Control)*

ก่อนเสนอ Risk Register รายงานผล หรือแผนบริหารความเสี่ยงต่อผู้บริหารหรือคณะกรรมการ หน่วยงานผู้จัดทำและหน่วยงานบริหารความเสี่ยงต้องตรวจสอบคุณภาพอย่างน้อย ดังนี้

ตารางที่ 4-20 *เกณฑ์การควบคุมคุณภาพข้อมูลและเอกสารความเสี่ยง*

ประเด็นตรวจสอบ	เกณฑ์คุณภาพ	ตัวอย่างสิ่งที่ต้องตรวจพบ
1. **ความเชื่อมโยงกับวัตถุประสงค์**	ระบุ Objective/KPI และ Risk Owner ชัดเจน	ความเสี่ยงเชื่อมกับเป้าหมายความพร้อมใช้ของระบบสารสนเทศ
2. **Risk Statement**	แยก Cause–Event–Impact ชัดเจน	ไม่ใช้คำว่า “ระบบล่ม” เพียงอย่างเดียว
3. **คะแนนความเสี่ยง**	มีเหตุผล ข้อมูล และหลักฐานรองรับ	ระบุสถิติเหตุการณ์ ช่องโหว่ และผลทดสอบระบบ
4. **Impact และ Override**	ใช้คะแนนสูงสุดของมิติที่เกี่ยวข้องและตรวจ Override	ข้อมูลสำคัญรั่วไหลอาจเข้าเกณฑ์รายงานทันที
5. **KRI**	มีนิยาม สูตร แหล่งข้อมูล Data Owner ความถี่ RA/RT และ Trigger	Patch Compliance มีสูตรและรายงานรายเดือน
6. **มาตรการ**	ตอบสาเหตุสำคัญ มี Deliverable ผู้รับผิดชอบ ทรัพยากร และกำหนดเวลา	ติดตั้งระบบสำรองพร้อมผลทดสอบ ไม่ใช้ข้อความว่า “เฝ้าระวัง” อย่างเดียว
7. **ระดับความเสี่ยง**	แยก Residual Risk และ Target Residual Risk	ไม่ลด Residual Risk จากมาตรการที่ยังเป็นแผน
8. **การยกระดับ**	ความเสี่ยงเกิน RA/RT มีหลักฐานการรายงานและตัดสินใจ	มี Escalation Record และ Decision Log
9. **Portfolio View**	ใช้รหัส นิยาม และประเภทมาตรฐาน ลดรายการซ้ำซ้อน	รวมความเสี่ยงไซเบอร์ที่กระทบหลายส่วนงานเป็นภาพรวม
10. **การควบคุมเอกสาร**	มี Version วันที่ประเมิน ผู้จัดทำ ผู้ตรวจสอบ ผู้อนุมัติ และหลักฐานอ้างอิง	สามารถตรวจสอบย้อนหลังได้ว่าใครเปลี่ยนคะแนนและเพราะเหตุใด

ตัวอย่างการตรวจสอบคุณภาพ Risk Register

ข้อความเดิมที่ยังไม่เพียงพอ: “ความเสี่ยงด้านเทคโนโลยี: ระบบอาจมีปัญหา จึงจัดอบรมบุคลากรและสำรองข้อมูล”

ข้อความที่ปรับปรุงแล้ว:

“เนื่องจากระบบสำคัญบางส่วนยังติดตั้ง Security Patch ไม่ครบถ้วนและการทดสอบกู้คืนระบบยังไม่เป็นไปตาม RTO/RPO (Cause) อาจทำให้ระบบถูกโจมตีหรือไม่สามารถกู้คืนได้ภายในเวลาที่กำหนด (Event) ส่งผลให้การให้บริการหยุดชะงัก ข้อมูลสำคัญเสียหาย และมหาวิทยาลัยอาจไม่สามารถปฏิบัติตามกฎหมายหรือรักษาความเชื่อมั่นของผู้มีส่วนได้ส่วนเสียได้ (Impact)”

ข้อมูลประกอบต้องระบุเพิ่มเติม เช่น Risk Owner, Control Owner, Inherent Risk, Residual Risk, RA/RT, KRI, Action Owner, กำหนดเวลา และหลักฐานผลทดสอบ

หากพบข้อบกพร่องด้านข้อมูลที่มีนัยสำคัญ ต้องส่งคืนให้ Risk Owner หรือ Data Owner แก้ไขก่อนเสนอผู้มีอำนาจพิจารณา และต้องไม่ใช้ข้อมูลที่ยังไม่ได้รับการยืนยันเป็นฐานลดระดับความเสี่ยง

4.14 ผลลัพธ์ของกรอบการบริหารความเสี่ยง *(Outcomes of the Risk Management Framework)*

เมื่อดำเนินการตามกรอบนี้อย่างมีประสิทธิผล มหาวิทยาลัยต้องสามารถแสดงให้เห็นผลลัพธ์และหลักฐานอย่างน้อยดังนี้

ตารางที่ 4-21 *ผลลัพธ์ที่คาดหวังของกรอบการบริหารความเสี่ยงและตัวอย่างหลักฐาน*

ผลลัพธ์ที่คาดหวัง	ตัวอย่างหลักฐาน
1. **ความเสี่ยงสำคัญเชื่อมโยงกับยุทธศาสตร์และผลการดำเนินงาน**	Risk Register ระบุ Objective, KPI และผลลัพธ์เชิงยุทธศาสตร์ที่ได้รับผลกระทบ
2. **ผู้มีอำนาจได้รับข้อมูลเพียงพอและทันเวลา**	Dashboard รายงานแนวโน้ม KRI ประเด็นเกิน RT และเรื่องที่ต้องตัดสินใจ
3. **ความเสี่ยงเกิน RA/RT ได้รับการยกระดับและตอบสนอง**	Escalation Record, Decision Log และมติหรือข้อสั่งการ
4. **การควบคุมและมาตรการมีหลักฐานยืนยันประสิทธิผล**	Control Test, System Log, Sample Testing และผลทดสอบ BCP/DRP
5. **การจัดสรรทรัพยากรสอดคล้องกับระดับความเสี่ยง**	การอนุมัติงบประมาณหรือบุคลากรให้ความเสี่ยงสูงและสูงมากก่อน
6. **มหาวิทยาลัยเรียนรู้จากเหตุการณ์และพร้อมต่อภาวะหยุดชะงัก**	Lessons Learned, Root Cause Analysis และผลทดสอบแผนที่ดีขึ้น

ผลลัพธ์ที่คาดหวัง	ตัวอย่างหลักฐาน
7. **วัฒนธรรมความเสี่ยงและระดับการพัฒนาของระบบดีขึ้นต่อเนื่อง**	บุคลากรรายงานเหตุได้ทันเวลา มาตรการล่าช้าลดลง และคุณภาพ Risk Register ดีขึ้น
8. **มหาวิทยาลัยสามารถสร้าง รักษา และเพิ่มคุณค่า**	การใช้ข้อมูลความเสี่ยงสนับสนุนยุทธศาสตร์ โครงการ การลงทุน และการใช้ประโยชน์จากโอกาส

ผลลัพธ์ของระบบไม่ควรประเมินจากจำนวนแบบฟอร์ม การประชุม หรือกิจกรรมที่ดำเนินการเพียงอย่างเดียว แต่ต้องพิจารณาคุณภาพการตัดสินใจ การเปลี่ยนแปลงของระดับความเสี่ยง ประสิทธิผลของการควบคุม ความพร้อมต่อเหตุหยุดชะงัก และความสามารถในการบรรลุวัตถุประสงค์ของมหาวิทยาลัย

ตัวอย่างภาพรวมผลลัพธ์

เดิมมหาวิทยาลัยมีความเสี่ยงด้านความต่อเนื่องของระบบสารสนเทศอยู่ในระดับสูง 15 คะแนน และพบว่า KRI การติดตั้ง Patch ต่ำกว่า RT ภายหลังฝ่ายบริหารอนุมัติทรัพยากร กำหนด Control Owner ปรับปรุงระบบสำรอง และทดสอบ DRP แล้ว พบว่า

- Patch Compliance เพิ่มจากร้อยละ 88 เป็นร้อยละ 97
- ระบบสำคัญสามารถกู้คืนได้ภายใน RTO/RPO
- ไม่พบข้อบกพร่องสำคัญจากการทดสอบซ้ำ
- Residual Risk ลดลงจาก 15 เป็น 8 คะแนนโดยมีหลักฐานรองรับ
- Dashboard และ Decision Log แสดงการยกระดับและการตัดสินใจครบถ้วน

กรณีดังกล่าวแสดงให้เห็นว่าระบบบริหารความเสี่ยงสร้างผลลัพธ์เชิงบริหาร มิใช่เพียงดำเนินกิจกรรมหรือจัดทำรายงานครบตามรอบ

ข้อกำหนดก่อนประกาศใช้

1. Risk Matrix เกณฑ์ Override, RA/RT อำนาจการยอมรับความเสี่ยง และระยะเวลาการรายงาน (Reporting SLA) ต้องได้รับอนุมัติเป็นเกณฑ์กลางของมหาวิทยาลัย

2. เกณฑ์ Impact เชิงปริมาณเฉพาะมิติต้องตรวจสอบให้สอดคล้องกับฐานะการเงิน กฎหมาย แผนฉุกเฉิน ข้อมูลผลการดำเนินงาน และบริบทปัจจุบันก่อนประกาศใช้

3. ชื่อคณะกรรมการ สายการรายงาน อำนาจอนุมัติ และอำนาจตัดสินใจต้องตรงกับข้อบังคับ กฎบัตร คำสั่งแต่งตั้ง และคำสั่งมอบอำนาจที่มีผลใช้บังคับ

4. คำศัพท์ รหัสประเภทความเสี่ยง ระดับคะแนน แบบฟอร์ม และรอบรายงานต้องสอดคล้องกันทั้งคู่มือและภาคผนวก

5. หากข้อความในส่วนนี้ขัดหรือแย้งกับกฎหมายหรือข้อกำหนดเฉพาะ ให้ใช้กฎหมายหรือข้อกำหนดที่เคร่งครัดกว่า และเสนอปรับปรุงคู่มือโดยเร็ว

6. ให้ทบทวนกรอบอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อยุทธศาสตร์ โครงสร้าง กฎหมาย มาตรฐาน ระบบงาน หรือบริบทความเสี่ยงเปลี่ยนแปลงอย่างมีนัยสำคัญ

7. ก่อนประกาศใช้ ต้องกำหนดเจ้าของเอกสาร เลขที่เอกสาร Version วันที่อนุมัติ วันที่มีผลใช้บังคับ รอบทบทวน ผู้อนุมัติ และประวัติการแก้ไขให้ครบถ้วน

ส่วนที่ 5
การกำหนดระดับความเสี่ยงที่ยอมรับได้ ตัวชี้วัดความเสี่ยง และเกณฑ์การตัดสินใจ

(Risk Appetite, Risk Tolerance, Key Risk Indicators and Decision Criteria)

ส่วนนี้กำหนดกรอบเพื่อให้มหาวิทยาลัย ส่วนงาน/หน่วยงานสามารถตอบคำถามสำคัญได้อย่างชัดเจนว่า “มหาวิทยาลัยยอมรับความเสี่ยงได้เพียงใด ใช้ข้อมูลใดเป็นสัญญาณเตือน ใครต้องดำเนินการ และเมื่อใดต้องรายงานหรือยกระดับความเสี่ยง”

5.1 หลักการและวัตถุประสงค์

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) และตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) เป็นเครื่องมือเชื่อมโยงระหว่าง

ยุทธศาสตร์ ⟶ วัตถุประสงค์ ⟶ ความเสี่ยง ⟶ การตัดสินใจ ⟶ การติดตามผล

มหาวิทยาลัยใช้เครื่องมือดังกล่าวเพื่อ

1. กำหนดประเภทและขอบเขตความเสี่ยงที่มหาวิทยาลัยยินดีรับในการบรรลุวัตถุประสงค์
2. สนับสนุนการตัดสินใจ การลงทุน การอนุมัติโครงการ และการจัดสรรทรัพยากร
3. กำหนดสัญญาณเตือนก่อนความเสี่ยงส่งผลกระทบต่อเป้าหมายอย่างมีนัยสำคัญ
4. กำหนดเกณฑ์การตอบสนอง การรายงาน และการยกระดับให้เป็นมาตรฐานเดียวกัน
5. ป้องกันการยอมรับความเสี่ยงเกินอำนาจ เกินความสามารถในการรองรับ หรือขัดต่อกฎหมาย
6. ทำให้ผู้บริหารสามารถพิจารณาความเสี่ยงและโอกาสประกอบการตัดสินใจบนฐานข้อมูล
7. ส่งเสริมความรับผิดชอบของ Risk Owner, Action Owner และ Data Owner
8. สนับสนุนการบริหารพอร์ตความเสี่ยงในภาพรวม โดยพิจารณาความสัมพันธ์และการกระจุกตัวของความเสี่ยง

RA/RT ต้องนำไปใช้ในการตัดสินใจจริง มิใช่กำหนดไว้เพียงเพื่อประกอบเอกสารหรือรายงานตามรอบเวลา

5.2 คำศัพท์และความสัมพันธ์

ตารางที่ 5-1 *คำศัพท์และความหมายเกี่ยวกับ Risk Capacity, RA, RT, Risk Limit, KRI และ Trigger*

คำศัพท์	*ความหมายในการใช้งาน*
ความสามารถในการรองรับความเสี่ยง (Risk Capacity)	ระดับความเสี่ยงสูงสุดที่มหาวิทยาลัยสามารถรองรับได้โดยไม่กระทบต่อความอยู่รอด พันธกิจหลัก ข้อจำกัดทางกฎหมาย หรือความสามารถในการดำเนินงาน
ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA)	ประเภทและระดับความเสี่ยงโดยรวมที่มหาวิทยาลัยยินดีรับในการดำเนินยุทธศาสตร์และบรรลุวัตถุประสงค์

คำศัพท์	*ความหมายในการใช้งาน*
ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT)	ขอบเขตความเบี่ยงเบนเชิงปฏิบัติจากระดับหรือเป้าหมายที่กำหนด ซึ่งยังสามารถบริหารจัดการได้ภายในอำนาจและระยะเวลาที่กำหนด
ขีดจำกัดความเสี่ยง (Risk Limit)	ขีดจำกัดเชิงปฏิบัติที่ห้ามเกิน หรือเกินได้เฉพาะเมื่อได้รับอนุมัติเป็นกรณีพิเศษ โดยต้องไม่เกิน Risk Capacity
ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI)	ตัวชี้วัดที่สะท้อนระดับ แนวโน้ม สาเหตุ หรือปัจจัยขับเคลื่อนของความเสี่ยง
จุดกระตุ้นการดำเนินการ (Trigger)	ค่า เหตุการณ์ หรือเงื่อนไขที่กำหนดให้ต้องแจ้งเตือน วิเคราะห์ ตอบสนอง หรือยกระดับ
ความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk)	ระดับความเสี่ยงที่คาดว่าจะเหลือภายหลังดำเนินมาตรการเพิ่มเติมครบถ้วนและมีประสิทธิผล
เหตุที่ไม่ยอมรับ (Zero Tolerance Event)	เหตุการณ์หรือพฤติกรรมที่มหาวิทยาลัยไม่ยอมรับและต้องระงับ รายงาน สอบสวน แก้ไข หรือยกระดับทันที

ความสัมพันธ์ของเครื่องมือดังกล่าวสรุปได้ดังนี้

- Risk Capacity เป็นเพดานสูงสุดของความสามารถในการรองรับความเสี่ยง
- RA กำหนดท่าทีและขอบเขตความเสี่ยงที่มหาวิทยาลัยยินดีรับ
- RT แปลง RA ไปสู่ช่วงเฝ้าระวังที่วัดและบริหารได้
- Risk Limit เป็นขีดจำกัดที่ไม่ควรเกินในการดำเนินงาน
- KRI ใช้ติดตามว่าความเสี่ยงกำลังเคลื่อนเข้าใกล้หรือเกินเกณฑ์หรือไม่
- Trigger กำหนดว่าเมื่อใด ใครต้องดำเนินการ และต้องรายงานต่อใคร

ทั้งนี้

- RA ไม่ใช่ค่าเป้าหมายผลการดำเนินงานหรือ KPI
- RT ไม่ใช่ค่าที่มหาวิทยาลัยยอมให้ผลการดำเนินงานต่ำกว่ามาตรฐานได้โดยไม่ต้องดำเนินการ
- ค่า KRI ที่แสดง “ภายใน RA” เป็นเกณฑ์เชิงปฏิบัติที่ถ่ายทอดมาจากถ้อยแถลง RA
- Target Residual Risk ไม่ใช่ระดับความเสี่ยงปัจจุบัน และใช้แทน Residual Risk ไม่ได้

5.3 หลักการกำหนด Risk Capacity

การกำหนด Risk Capacity ต้องพิจารณาข้อจำกัดสูงสุดที่มหาวิทยาลัยสามารถรองรับได้ โดยอย่างน้อยครอบคลุม

- ความสามารถด้านการเงิน สภาพคล่อง และภาระผูกพัน
- ความปลอดภัยของนักศึกษา บุคลากร ผู้รับบริการ และประชาชน
- ความต่อเนื่องของพันธกิจด้านการศึกษา การวิจัย และการบริการ
- ข้อจำกัดตามกฎหมาย ข้อบังคับ และเงื่อนไขของหน่วยงานกำกับดูแล
- ความสามารถและความพร้อมของระบบเทคโนโลยี ข้อมูล และโครงสร้างพื้นฐาน

- จำนวน สมรรถนะ และความพร้อมของบุคลากร
- ชื่อเสียง ความเชื่อมั่น และความชอบธรรมของมหาวิทยาลัย
- ข้อผูกพันต่อนักศึกษา ผู้ให้ทุน คู่สัญญา ชุมชน และผู้มีส่วนได้ส่วนเสีย
- ความสามารถในการฟื้นตัวจากภาวะวิกฤตหรือเหตุหยุดชะงัก

Risk Capacity ต้องกำหนดจากข้อมูล ข้อจำกัด และสถานการณ์ที่เป็นจริง มิใช่กำหนดจากระดับความเสี่ยงที่ผู้บริหารประสงค์จะรับ และต้องไม่ใช้แทน RA

ตัวอย่าง: หากมหาวิทยาลัยต้องมีเงินสดขั้นต่ำเพื่อรองรับเงินเดือน ภาระผูกพัน และพันธกิจสำคัญเป็นระยะเวลาหนึ่ง ระดับเงินสดดังกล่าวอาจใช้เป็นฐานกำหนด Risk Capacity ด้านสภาพคล่อง ส่วน RA ควรกำหนดในระดับที่ปลอดภัยกว่าและมีระยะห่างจากเพดานวิกฤตอย่างเหมาะสม

5.4 ระดับ Risk Appetite ของมหาวิทยาลัย

5.4.1 ระดับของ Risk Appetite

ตารางที่ 5-2 *ระดับ Risk Appetite (RA) และความหมาย*

ระดับ RA	ความหมาย
ไม่ยอมรับ (Zero)	ไม่ยอมรับเหตุการณ์หรือพฤติกรรมดังกล่าว ต้องป้องกัน รายงาน และจัดการทันที
ต่ำ (Low)	ยอมรับความเสี่ยงได้น้อย ต้องมีการควบคุมและความเชื่อมั่นในระดับสูง
ปานกลาง (Moderate)	ยอมรับได้ในระดับจำกัดเมื่อมีเหตุผล มีการควบคุม และผลตอบแทนหรือคุณค่าที่เหมาะสม
สูง (High)	ยอมรับความไม่แน่นอนได้มากขึ้นเพื่อสร้างโอกาสหรือคุณค่า แต่ต้องไม่เกิน Risk Capacity และต้องมี Guardrail
แตกต่างตามบริบท (Selective/Variable)	ใช้เป็นลักษณะประกอบ RA เมื่อระดับที่ยอมรับแตกต่างกันตามกิจกรรม โครงการ กลุ่มผู้มีส่วนได้ส่วนเสีย หรือมิติผลกระทบ

Selective/Variable ไม่ใช่ระดับที่สูงกว่าหรือต่ำกว่า High แต่เป็นการกำหนด RA ให้แตกต่างกันตามบริบท ตัวอย่างเช่น มหาวิทยาลัยอาจมี RA ระดับปานกลางต่อการทดลองนวัตกรรม แต่มี Zero Appetite ต่อการละเมิดจริยธรรมการวิจัย

5.4.2 ระดับ RA จำแนกตามด้านความเสี่ยง

ตารางที่ 5-3 *ระดับความเสี่ยงที่ยอมรับได้ จำแนกตามด้านความเสี่ยง*

ด้านความเสี่ยง	ระดับ RA ที่เสนอ	เงื่อนไขสำคัญ
การจัดการศึกษาและคุณภาพบัณฑิต	ต่ำ	ไม่ยอมรับการดำเนินงานที่กระทบมาตรฐานการศึกษาอย่างมีนัยสำคัญ
การวิจัยและนวัตกรรม	ปานกลาง	ยอมรับความไม่แน่นอนเพื่อสร้างนวัตกรรม แต่ Zero ต่อการประพฤติผิดทางการวิจัยอย่างร้ายแรง
การเงินและสภาพคล่อง	ต่ำ–ปานกลาง	ยอมรับความผันผวนได้ในขอบเขตที่ไม่กระทบสภาพคล่องและพันธกิจ
กฎหมาย การทุจริต และจริยธรรมร้ายแรง	Zero	ต้องรายงานและดำเนินการทันที
ไซเบอร์และข้อมูลส่วนบุคคล	ต่ำ	ต้องมีการควบคุมสูง และ Zero ต่อเหตุรั่วไหลที่มีผลกระทบรุนแรงตามเกณฑ์
ชื่อเสียงและความเชื่อมั่น	ต่ำ	ยอมรับได้เฉพาะผลกระทบจำกัดและสามารถแก้ไขได้รวดเร็ว
ชีวิตและความปลอดภัยร้ายแรง	Zero	ไม่ยอมรับเหตุร้ายแรงที่เกี่ยวข้องกับการละเลยมาตรการ
นวัตกรรมและการเปลี่ยนผ่านดิจิทัล	ปานกลาง	ทดลองได้ภายใต้ Guardrail, Pilot, Data Governance และการกำกับ AI
สิ่งแวดล้อมและความยั่งยืน	ต่ำ–ปานกลาง	ยอมรับได้ตามลักษณะโครงการ แต่ Zero ต่อการฝ่าฝืนกฎหมายโดยเจตนาหรือผลกระทบรุนแรง

ระดับดังกล่าวเป็นกรอบเสนอเบื้องต้น ต้องผ่านการกลั่นกรองและอนุมัติตามโครงสร้าง อำนาจหน้าที่ และเอกสารที่มีผลใช้บังคับของมหาวิทยาลัย โดยให้เสนอคณะกรรมการและสภามหาวิทยาลัยตามลำดับที่กำหนด

5.5 การกำหนด Risk Tolerance

RT ต้องถ่ายทอด RA ให้เป็นขอบเขตเชิงปฏิบัติที่สามารถวัด ติดตาม และใช้ตัดสินใจได้ โดยกำหนดให้เหมาะสมกับทิศทางของตัวชี้วัด ดังนี้

- **ค่ายิ่งสูงยิ่งดี:** เมื่อค่าลดลงต้องเฝ้าระวัง เช่น รายได้ที่ไม่ใช่ค่าเล่าเรียน อัตราการผ่านการอบรม และอัตราการติดตั้ง Patch
- **ค่ายิ่งต่ำยิ่งดี:** เมื่อค่าเพิ่มขึ้นต้องเฝ้าระวัง เช่น จำนวนข้อบกพร่อง จำนวนเหตุการณ์ และระยะเวลาหยุดชะงัก
- **ค่าเป้าหมายเป็นช่วง:** ต้องอยู่ภายในช่วงที่กำหนด เช่น อัตราส่วนทางการเงินหรือภาระงาน
- **เหตุการณ์แบบ Zero Tolerance:** ไม่มีช่วงเบี่ยงเบน เมื่อเกิดเหตุให้ยกระดับทันที

ตารางที่ 5-4 ความเชื่อมโยงระหว่างวัตถุประสงค์ KRI, RA, RT และการดำเนินการ

ตัวอย่างการแปลง RA เป็น RT และ Trigger

วัตถุประสงค์/ความเสี่ยง	KRI	ภายใน RA	ช่วงเฝ้าระวัง RT	เกิน RT/Trigger	การดำเนินการ
ความยั่งยืนทางการเงิน	Non-Tuition Revenue	≥30%	25–<30%	<25%	จัดทำและยกระดับ Corrective Revenue Plan
การรักษาสภาพคล่อง	Days Cash on Hand	≥180 วัน	120–<180 วัน	<120 วัน	ทบทวนแผนสภาพคล่องและประมาณการกระแสเงินสด
การพัฒนาบุคลากร	อัตรา Re/Up-skill	≥85%	75–<85%	<75%	เร่งแผนพัฒนากลุ่มที่ไม่ผ่านเกณฑ์และรายงานผู้บริหาร
Cyber/PDPA	ผู้ผ่านการอบรม	≥90%	80–<90%	<80%	แจ้งส่วนงาน อบรมซ้ำ และจัดทำ Corrective Action
Compliance	กรณีทุจริตที่ยืนยัน ข้อเท็จจริง	0 กรณี	ไม่มีช่วงเบี่ยงเบน	≥1 กรณี	รายงานทันทีตาม Zero Tolerance

ตัวเลขดังกล่าวเป็นตัวอย่างหรือกรอบเสนอ ต้องตรวจสอบข้อมูลฐาน ความเป็นไปได้ และได้รับอนุมัติก่อนนำไปใช้เป็นเกณฑ์อย่างเป็นทางการ

5.6 การกำหนดและบริหาร KRI

KRI ต้องสะท้อนการเปลี่ยนแปลงของระดับความเสี่ยงหรือปัจจัยขับเคลื่อนความเสี่ยง ไม่ควรใช้ตัวชี้วัดกิจกรรมที่ไม่สามารถบ่งชี้ระดับหรือแนวโน้มความเสี่ยงได้

KRI แต่ละตัวต้องกำหนดองค์ประกอบอย่างน้อย ดังนี้

1. ชื่อและวัตถุประสงค์ของ KRI
2. ความเสี่ยง สาเหตุ หรือปัจจัยขับเคลื่อนที่เชื่อมโยง
3. ประเภทตัวชี้วัดนำหรือตัวชี้วัดตาม (Leading/Lagging Indicator)
4. สูตรคำนวณและหน่วยวัด
5. แหล่งข้อมูล
6. เจ้าของข้อมูล (Data Owner)
7. ความถี่ในการจัดเก็บและรายงาน
8. ค่าฐาน (Baseline)
9. เกณฑ์ที่ถ่ายทอดจาก RA และ RT
10. Trigger และระดับสถานะ

11. การดำเนินการเมื่อเข้าใกล้หรือเกินเกณฑ์
12. ผู้รับรายงานและผู้มีอำนาจตัดสินใจ
13. หลักฐานและวันที่ปรับปรุงข้อมูล

ตารางที่ 5-5 *องค์ประกอบและตัวอย่างการกำหนด KRI*

ตัวอย่าง KRI ที่สมบูรณ์

องค์ประกอบ	ตัวอย่าง
ความเสี่ยง	ระบบสารสนเทศสำคัญอาจถูกโจมตีจากช่องโหว่ที่ไม่ได้รับการแก้ไข
ชื่อ KRI	ร้อยละของระบบสำคัญที่ติดตั้ง Security Patch ภายใน SLA
ประเภท	Leading Indicator
สูตร	จำนวนระบบสำคัญที่ติดตั้ง Patch ภายใน SLA ÷ ระบบสำคัญทั้งหมด × 100
หน่วยวัด	ร้อยละ
แหล่งข้อมูล	Vulnerability Management System และ Patch Report
Data Owner	หน่วยงานด้านเทคโนโลยีดิจิทัล
ความถี่	รายเดือน
Baseline	ร้อยละ 88
ภายใน RA	ตั้งแต่ร้อยละ 95 ขึ้นไป
ช่วง RT	ตั้งแต่ร้อยละ 90 แต่ต่ำกว่าร้อยละ 95
เกิน RT	ต่ำกว่าร้อยละ 90
Trigger/Action	ต่ำกว่าร้อยละ 95 ให้เร่งแก้ไข; ต่ำกว่าร้อยละ 90 ให้จัดทำ Corrective Action และรายงานผู้บริหาร
ผู้รับรายงาน	Risk Owner ผู้บริหารที่กำกับ และหน่วยบริหารความเสี่ยง
หลักฐาน	Patch Log, Vulnerability Report และรายการระบบที่ยังไม่ดำเนินการ

KRI ควรมีทั้งตัวชี้วัดนำและตัวชี้วัดตาม ตัวอย่างเช่น

- Leading KRI: ร้อยละของระบบที่ติดตั้ง Patch ภายใน SLA
- Lagging KRI: จำนวนเหตุโจมตีที่ทำให้ระบบหยุดชะงักหรือข้อมูลรั่วไหล

5.7 สถานะ KRI และเกณฑ์ Trigger

มหาวิทยาลัยใช้สถานะสี่ระดับเพื่อสนับสนุนการติดตามและตัดสินใจ ดังนี้

ตารางที่ 5-6 *สถานะ KRI และการดำเนินการขั้นต่ำ*

สถานะ	ความหมาย	การดำเนินการขั้นต่ำ
เขียว (Green)	อยู่ภายใน RA	ควบคุมได้และติดตามตามรอบ
เหลือง (Yellow)	เบี่ยงเบนจาก RA แต่ยังอยู่ภายใน RT	วิเคราะห์สาเหตุ เฝ้าระวัง และดำเนินมาตรการภายในอำนาจ Risk Owner
ส้ม (Orange)	เกิน RT หรือแนวโน้มเสื่อมลงต่อเนื่อง	จัดทำ Corrective Action รายงานผู้บริหาร และพิจารณาทบทวน Residual Risk
แดง (Red)	เกิน Risk Limit เป็นเหตุ Zero Tolerance หรือเหตุรุนแรง	ระงับเหตุ ยกระดับ และรายงานทันที

การกำหนดสีต้องใช้เกณฑ์ที่ได้รับอนุมัติและสอดคล้องกับทิศทางของ KRI ไม่ควรกำหนดสีจากดุลยพินิจภายหลังทราบผลข้อมูล

หาก KRI หลายตัวของความเสี่ยงเดียวกันมีสถานะแตกต่างกัน ให้พิจารณาสถานะที่รุนแรงที่สุดร่วมกับแนวโน้ม ความสำคัญ และความน่าเชื่อถือของข้อมูล โดยไม่ใช้ค่าเฉลี่ยเพื่อลดทอนสัญญาณสำคัญ

5.8 ความเชื่อมโยง RA/RT กับ Risk Matrix

Risk Matrix และ RA/RT มีวัตถุประสงค์ต่างกันแต่ต้องใช้ร่วมกัน ดังนี้

- Risk Matrix ใช้ประเมินความรุนแรงและจัดลำดับความสำคัญของความเสี่ยง
- RA/RT ใช้กำหนดขอบเขตที่ยอมรับได้และ Trigger การตัดสินใจ
- KRI ใช้ติดตามการเปลี่ยนแปลงของความเสี่ยงระหว่างรอบการประเมิน
- คะแนนต่ำไม่ได้หมายความว่ายอมรับได้เสมอ หากเข้าเกณฑ์ Zero Tolerance หรือ Override
- คะแนนสูงไม่ได้หมายความว่าต้องยุติกิจกรรมทุกกรณี แต่ต้องยกระดับและตัดสินใจตามอำนาจ
- ความเสี่ยงที่เกิน RT ต้องมีมาตรการหรือการตัดสินใจ ไม่ควรเพียงบันทึกไว้ในรายงาน

มหาวิทยาลัยใช้เกณฑ์ระดับความเสี่ยงเดียวกับส่วนที่ 4 ดังนี้

ตารางที่ 5-7 *Risk Matrix และระดับความเสี่ยง*

คะแนน	ระดับ	รหัส
1–4	ต่ำ (Low)	L
5–9	ปานกลาง (Medium)	M
10–15	สูง (High)	H
16–25	สูงมาก (Extreme)	E

เมื่อผลจาก Risk Matrix, RA/RT, KRI หรือ Override ให้ข้อสรุปต่างกัน ให้ใช้เกณฑ์ที่เข้มงวดกว่าเป็นฐานการรายงานและตัดสินใจ พร้อมบันทึกเหตุผล

ตัวอย่าง: ความเสี่ยงไซเบอร์มี Residual Risk เท่ากับ 9 คะแนน หรือระดับปานกลาง แต่พบเหตุข้อมูลสำคัญรั่วไหลที่เข้าเกณฑ์ Zero Tolerance ต้องยกระดับและรายงานทันที ไม่สามารถใช้คะแนน 9 เป็นเหตุผลในการรอรายงานตามรอบไตรมาสได้

5.9 เกณฑ์ Zero Tolerance และ Override

เหตุ Zero Tolerance เป็นเหตุที่มหาวิทยาลัยไม่ยอมรับและต้องดำเนินการทันทีโดยไม่รอคะแนนรวม เช่น

- การทุจริต การคอร์รัปชัน หรือการรับสินบน
- การกระทำผิดกฎหมายโดยเจตนา
- การประพฤติมิชอบหรือผิดจริยธรรมอย่างร้ายแรง
- การเสียชีวิตหรือเหตุความปลอดภัยร้ายแรงที่เกี่ยวข้องกับการละเลยมาตรการ
- การล่วงละเมิดหรือคุกคามทางเพศอย่างร้ายแรง
- การเลือกปฏิบัติหรือการละเมิดสิทธิมนุษยชนอย่างร้ายแรง
- การปลอมแปลงผลงานหรือประพฤติผิดทางการวิจัยอย่างร้ายแรง
- การรั่วไหลของข้อมูลสำคัญหรือข้อมูลส่วนบุคคลที่มีผลกระทบรุนแรง
- การปกปิด ทำลาย หรือรายงานข้อมูลอันเป็นเท็จต่อผู้กำกับดูแล

เมื่อพบเหตุหรือสัญญาณที่เข้าเกณฑ์ ต้องดำเนินการตามความเหมาะสม ได้แก่ ระงับเหตุ คุ้มครองผู้ได้รับผลกระทบ รักษาหลักฐาน รายงาน สอบสวน แก้ไข และดำเนินการตามกฎหมายหรือนโยบายที่เกี่ยวข้อง

Zero Tolerance มิได้หมายความว่ามหาวิทยาลัยรับรองว่าเหตุการณ์จะไม่เกิดขึ้น แต่หมายถึงมหาวิทยาลัยไม่ยอมรับการเพิกเฉย การปกปิด หรือการคงเหตุไว้โดยไม่มีการตอบสนองที่เหมาะสม

นอกจาก Zero Tolerance ให้ใช้เกณฑ์ Override ร่วมด้วย เช่น

1. Impact ระดับ 5 ให้เป็นอย่างน้อยระดับสูง
2. เหตุ Zero Tolerance ให้ยกระดับเป็นระดับสูงมากและรายงานทันที
3. KRI เกิน RT หรือ Risk Limit
4. ความเสี่ยงกระทบหลายส่วนงานหรือวัตถุประสงค์เชิงยุทธศาสตร์
5. การควบคุมสำคัญล้มเหลว
6. ต้องการทรัพยากรหรืออำนาจตัดสินใจเกินขอบเขต Risk Owner
7. กฎหมายหรือข้อกำหนดเฉพาะกำหนดเกณฑ์ที่เข้มงวดกว่า

5.10 อำนาจการยอมรับความเสี่ยง

การพิจารณาอำนาจยอมรับความเสี่ยงให้ใช้ **Residual Risk ณ วันที่ตัดสินใจ** เป็นฐาน มิใช่ Inherent Risk หรือ Target Residual Risk

ตารางที่ 5-8 *ระดับ Residual Risk และอำนาจในการยอมรับความเสี่ยง*

ระดับ Residual Risk	อำนาจขั้นต่ำที่เสนอ	เงื่อนไข
ต่ำ 1–4	Risk Owner/หัวหน้าส่วนงาน	อยู่ภายใน RA มีการควบคุมและติดตามตามปกติ
ปานกลาง 5–9	หัวหน้าส่วนงานหรือผู้บริหารที่ได้รับมอบหมาย	มีเหตุผล หลักฐาน KRI และเงื่อนไขทบทวน
สูง 10–15	อธิการบดีหรือผู้บริหารที่ได้รับมอบอำนาจ ภายหลังการกลั่นกรอง	ต้องมี Risk Treatment Plan, Target Residual Risk และกำหนดเวลา
สูงมาก 16–25	ไม่ควรยอมรับเป็นการดำเนินงานปกติ ต้องยกระดับทันที	การคงไว้ชั่วคราวต้องได้รับอนุมัติจากผู้มีอำนาจสูงสุดตามข้อบังคับและรายงานผู้กำกับดูแล
Zero Tolerance	ไม่อยู่ในอำนาจการยอมรับ	ต้องระงับ รายงาน สอบสวน แก้ไข และดำเนินการตามกฎหมายหรือนโยบายทันที

การยอมรับความเสี่ยงต้องมีอายุการอนุมัติและวันที่ทบทวน ไม่ถือเป็นการอนุมัติถาวร และไม่เป็นการยกเว้นหน้าที่ตามกฎหมาย

Risk Acceptance Record ต้องประกอบด้วย

- รายละเอียดความเสี่ยงและ Residual Risk
- เหตุผลที่เสนอให้ยอมรับ
- ทางเลือกที่พิจารณาแล้ว
- ผลกระทบและผู้มีส่วนได้ส่วนเสีย
- KRI และเงื่อนไข Trigger

- ระยะเวลาที่อนุมัติ
- มาตรการชั่วคราวหรือเงื่อนไขกำกับ
- ผู้เสนอ ผู้กลั่นกรอง และผู้อนุมัติ
- วันที่ทบทวนครั้งถัดไป

ตัวอย่าง: ความเสี่ยงระดับสูงที่ไม่สามารถหยุดระบบได้ทันทีเนื่องจากจะกระทบการลงทะเบียนนักศึกษา อาจได้รับอนุมัติให้คงไว้ชั่วคราว โดยต้องเพิ่มการเฝ้าระวัง กำหนด Maintenance Window ระบุวันสิ้นสุด และรายงานความก้าวหน้าตามรอบที่ผู้อนุมัติกำหนด

5.11 การรายงานและยกระดับ

ตารางที่ 5-9 *เงื่อนไขและระยะเวลาขั้นต่ำในการรายงาน/ยกระดับ*

เงื่อนไข	เวลารายงานขั้นต่ำ
Zero Tolerance เหตุวิกฤต หรือ Impact ระดับ 5	รายงานทันที และจัดทำรายงานเบื้องต้นไม่เกิน 24 ชั่วโมง
ระดับสูงมาก 16–25	ยกระดับทันที และรายงานไม่เกิน 24 ชั่วโมง
ระดับสูง 10–15, KRI เกิน RT หรือมาตรการสำคัญล่าช้า	รายงานภายใน 3 วันทำการ
ระดับปานกลาง 5–9	อย่างน้อยรายไตรมาสหรือตามรอบที่กำหนด
ระดับต่ำ 1–4	ตามรอบปกติ

การรายงานให้ใช้สายการรายงานและบทบาทตามส่วนที่ 3 โดยไม่จำเป็นต้องกำหนดบทบาทซ้ำในส่วนนี้

หากกฎหมาย แผนฉุกเฉิน แผนสื่อสารวิกฤต หรือนโยบายเฉพาะกำหนดระยะเวลาที่สั้นกว่าหรือเข้มงวดกว่า ให้ใช้ข้อกำหนดที่เข้มงวดกว่า การรายงานไม่ทดแทนการระงับเหตุและการคุ้มครองชีวิต ข้อมูล ทรัพย์สิน หลักฐาน และความต่อเนื่องของพันธกิจ

5.12 การทบทวนและอนุมัติ

มหาวิทยาลัยกำหนดให้

1. ทบทวน Risk Capacity, RA, RT, Risk Limit และ KRI อย่างน้อยปีละหนึ่งครั้ง
2. ทบทวนเมื่อยุทธศาสตร์ ฐานะการเงิน กฎหมาย เทคโนโลยี หรือบริบทเปลี่ยนแปลงอย่างมีนัยสำคัญ
3. ทบทวนภายหลังเกิดเหตุรุนแรง เหตุ Zero Tolerance หรือ KRI เกิน RT ต่อเนื่อง
4. ทบทวนเมื่อข้อมูลฐานหรือสมมติฐานที่ใช้กำหนดเกณฑ์เปลี่ยนแปลง
5. หน่วยบริหารความเสี่ยงรวบรวมข้อมูล วิเคราะห์ และจัดทำข้อเสนอ
6. Risk Owner และ Data Owner รับรองคุณภาพและความเป็นไปได้ของข้อมูล

7. ฝ่ายบริหารและคณะกรรมการที่เกี่ยวข้องกลั่นกรองตามอำนาจหน้าที่
8. สภามหาวิทยาลัยอนุมัติถ้อยแถลง RA และหลักเกณฑ์สำคัญตามอำนาจ
9. กองตรวจสอบภายในให้ความเชื่อมั่นอย่างเป็นอิสระ โดยไม่เป็นผู้กำหนดหรืออนุมัติ RA/RT

การแก้ไขเกณฑ์ระหว่างปีต้องมีเหตุผล ข้อมูลสนับสนุน ผู้อนุมัติ วันที่มีผลใช้ และประวัติการเปลี่ยนแปลง ห้ามปรับเกณฑ์ย้อนหลังเพื่อทำให้ผลการดำเนินงานหรือระดับความเสี่ยงปรากฏว่าอยู่ในเกณฑ์

ตัวอย่างการใช้ RA/RT–KRI–Escalation แบบครบวงจร

ความเสี่ยงด้าน Cyber/PDPA กำหนด KRI คือร้อยละของบุคลากรกลุ่มเป้าหมายที่ผ่านการอบรม โดยกำหนด

- ภายใน RA: ตั้งแต่ร้อยละ 90 ขึ้นไป
- ช่วง RT: ตั้งแต่ร้อยละ 80 แต่ต่ำกว่าร้อยละ 90
- เกิน RT: ต่ำกว่าร้อยละ 80

ผลการติดตามพบว่าผ่านการอบรมร้อยละ 78 จึงมีสถานะสีส้มและเกิน RT ต้องดำเนินการดังนี้

1. Data Owner ตรวจสอบความถูกต้องและรายชื่อผู้ยังไม่ผ่าน
2. Risk Owner วิเคราะห์สาเหตุและผลต่อ Residual Risk
3. Action Owner จัดอบรมซ้ำและกำหนดระยะเวลาแล้วเสร็จ
4. จัดทำ Corrective Action และรายงานผู้บริหารภายใน 3 วันทำการ
5. ติดตามผลถี่ขึ้นจนกลับเข้าสู่ช่วงที่กำหนด
6. หากในช่วงดังกล่าวเกิดข้อมูลรั่วไหลที่มีผลกระทบรุนแรง ให้ใช้เกณฑ์ Zero Tolerance และยกระดับทันทีโดยไม่รอผลการอบรมรอบถัดไป

ตัวอย่างนี้แสดงให้เห็นว่า RA กำหนดท่าทีของมหาวิทยาลัย RT กำหนดช่วงเฝ้าระวัง KRI ทำหน้าที่ส่งสัญญาณ และ Trigger เชื่อมไปสู่ผู้รับผิดชอบ ระยะเวลา และการตัดสินใจที่ชัดเจน

บรรณานุกรมและเอกสารอ้างอิง
คู่มือการบริหารความเสี่ยง มหาวิทยาลัยแม่โจ้ ฉบับปรับปรุง พ.ศ. 2570

1. กฎหมายและข้อกำหนดของประเทศไทย

พระราชบัญญัติมหาวิทยาลัยแม่โจ้ พ.ศ. 2560. (2560). ราชกิจจานุเบกษา, 134(39 ก). ราชกิจจานุเบกษา

พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561. (2561). ราชกิจจานุเบกษา, 135(27 ก). ราชกิจจานุเบกษา

พระราชบัญญัติการอุดมศึกษา พ.ศ. 2562. (2562). ราชกิจจานุเบกษา, 136(57 ก). ราชกิจจานุเบกษา

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (2562). ราชกิจจานุเบกษา, 136(69 ก). ราชกิจจานุเบกษา

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562). ราชกิจจานุเบกษา, 136(69 ก). ราชกิจจานุเบกษา

พระราชบัญญัติความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน พ.ศ. 2554. (2554). ราชกิจจานุเบกษา, 128(4 ก). ราชกิจจานุเบกษา

กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม. (2564). *แนวปฏิบัติตามหลักธรรมาภิบาลในสถาบันอุดมศึกษา พ.ศ. 2564*. สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม. (2565). *แนวปฏิบัติตามหลักธรรมาภิบาลในสถาบันอุดมศึกษา (ฉบับที่ 2)*. สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

2. หลักเกณฑ์และแนวทางสำหรับหน่วยงานของรัฐ

กระทรวงการคลัง. (2561). *หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561* (หนังสือกระทรวงการคลัง ที่ กค 0409.3/ว 105 ลงวันที่ 5 ตุลาคม 2561). กรมบัญชีกลาง

กระทรวงการคลัง. (2561). *หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561* (หนังสือกระทรวงการคลัง ด่วนมาก ที่ กค 0409.2/ว 123 ลงวันที่ 14 พฤศจิกายน 2561). กรมบัญชีกลาง

กระทรวงการคลัง. (2562). *หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562* (หนังสือกระทรวงการคลัง ที่ กค 0409.4/ว 23 ลงวันที่ 19 มีนาคม 2562). กรมบัญชีกลาง

กระทรวงการคลัง. (2562). *หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2562* (หนังสือกระทรวงการคลัง ที่ กค 0409.2/ว 118 ลงวันที่ 9 ตุลาคม 2562). กรมบัญชีกลาง

กระทรวงการคลัง. (2564). *แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กร* (หนังสือกระทรวงการคลัง ที่ กค 0409.3/ว 36 ลงวันที่ 3 กุมภาพันธ์ 2564). กรมบัญชีกลาง

กระทรวงการคลัง. (2564). *หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ (ฉบับที่ 3) พ.ศ. 2564* (หนังสือกระทรวงการคลัง ที่ กค 0409.2/ว 107 ลงวันที่ 16 กรกฎาคม 2564). กรมบัญชีกลาง

กระทรวงการคลัง. (2566). *หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ (ฉบับที่ 4) พ.ศ. 2566*. กรมบัญชีกลาง

3. มาตรฐานและกรอบการบริหารความเสี่ยงและการควบคุมภายใน

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework*. COSO

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*. COSO

International Electrotechnical Commission. (2019). *IEC 31010:2019 risk management—Risk assessment techniques* (2nd ed.). ISO

International Organization for Standardization. (2018). *ISO 31000:2018 risk management—Guidelines* (2nd ed.). ISO

International Organization for Standardization. (2022). *ISO 31073:2022 risk management—Vocabulary*. ISO

4. มาตรฐานด้านการกำกับดูแล การตรวจสอบภายใน และการให้ความเชื่อมั่น

The Institute of Internal Auditors. (2024). *Global Internal Audit Standards*. The IIA

The Institute of Internal Auditors. (2026, July 8). *Three Lines Model: Assurance and advice in support of effective governance* [Statement of position]. The IIA

The Institute of Internal Auditors. (2026, July 8). *The role of the internal audit function in enterprise risk management* [Statement of position]. The IIA

5. มาตรฐานด้านความต่อเนื่อง ไซเบอร์ และการคุ้มครองข้อมูล

International Organization for Standardization. (2019). *ISO 22301:2019 security and resilience—Business continuity management systems—Requirements* (2nd ed.). ISO

International Organization for Standardization, & International Electrotechnical Commission. (2022). *ISO/IEC 27557:2022 information security, cybersecurity and privacy protection—Application of ISO 31000:2018 for organizational privacy risk management*. ISO

6. การพัฒนาองค์กร คุณภาพการศึกษา ESG และความยั่งยืน

สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม. (2567). *เกณฑ์คุณภาพการศึกษาเพื่อการดำเนินการที่เป็นเลิศ ฉบับปี 2567–2570 (Education Criteria for Performance Excellence: EdPEx)*. EdPEx

United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*. United Nations Sustainable Development

United Nations. (n.d.). *The 17 Sustainable Development Goals*. United Nations Sustainable Development Goals

ตารางเชื่อมโยงเอกสารอ้างอิงกับบทที่ 1–5

บท	สาระสำคัญ	เอกสารอ้างอิงหลัก
บทที่ 1 บทนำและความสำคัญ	นิยามความเสี่ยง หลักการ ISO 31000, GRC, ESG, Three Lines และกฎหมายพื้นฐาน	ISO 31000:2018; ISO 31073:2022; COSO ERM 2017; พ.ร.บ.วินัยการเงินการคลังฯ; พ.ร.บ.การอุดมศึกษาฯ; Three Lines 2026; SDGs
บทที่ 2 นโยบายและกรอบอ้างอิง	ถ้อยแถลง นโยบาย RA/RT, COSO ERM, ISO 31000, EdPEx, ESG และการควบคุมภายใน	COSO ERM 2017; ISO 31000:2018; COSO Internal Control 2013; EdPEx 2567–2570; SDGs; เอกสารนโยบายมหาวิทยาลัย
บทที่ 3 โครงสร้างและบทบาท	Governing Body, Three Lines, RACI, Internal Audit และอำนาจการยอมรับความเสี่ยง	พ.ร.บ.มหาวิทยาลัยแม่โจ้ฯ; พ.ร.บ.การอุดมศึกษาฯ; แนวปฏิบัติธรรมาภิบาลฯ; หลักเกณฑ์ตรวจสอบภายใน; Global Internal Audit Standards 2024; Three Lines 2026; คำสั่งและกฎบัตรของมหาวิทยาลัย
บทที่ 4 กรอบและกระบวนการ	กระบวนการ 8 ขั้นตอน การประเมิน การควบคุม BCM/BCP/DRP และการให้ความเชื่อมั่น	ISO 31000:2018; ISO 31073:2022; IEC 31010:2019; COSO ERM 2017; COSO Internal Control 2013; ISO 22301:2019; ISO/IEC 27557:2022; หลักเกณฑ์กระทรวงการคลัง
บทที่ 5 RA/RT, KRI และเกณฑ์ตัดสินใจ	Risk Capacity, RA, RT, Risk Limit, KRI, Trigger, Zero Tolerance และอำนาจยอมรับความเสี่ยง	COSO ERM 2017; ISO 31000:2018; ISO 31073:2022; หลักเกณฑ์กระทรวงการคลัง; ถ้อยแถลง RA/RT และมติอนุมัติของมหาวิทยาลัย

ภาคผนวก

แบบฟอร์มประเมินและวิเคราะห์ความเสี่ยง

แบบ Risk_MJU01

แบบฟอร์มการวิเคราะห์และประเมินความเสี่ยง (Risk-MJU01)

การได้มาซึ่งประเด็นความเสี่ยง F1 : .....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

รหัสความเสี่ยง	
ประเด็นความเสี่ยง	
ระดับความเสี่ยง	
ประเภทความเสี่ยง	
วัตถุประสงค์เชิงยุทธศาสตร์ **(Strategic Objective)**	
ผู้บริหารเจ้าของความเสี่ยง **(Risk Owner)**	
ผู้บริหาร/หน่วยงานร่วมกำกับ	
หน่วยงานหลักด้านการประสานงาน	
ปีงบประมาณ	
ฐานข้อมูลที่ใช้วิเคราะห์	
หลักฐานเชิงประจักษ์ที่สำคัญ	
แนวโน้มความเสี่ยง	
คำนิยามความเสี่ยง	
เหตุการณ์ความเสี่ยง **(Risk Event)**	
ขอบเขตความเสี่ยง	

(Risk Scope)	
คำแถลงระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite Statement)	

Root Cause			
รหัส	ปัจจัยเสี่ยงภายใน (Internal Risks)	รหัส	ปัจจัยเสี่ยงภายนอก (External Risks)
I1		E1	
I2		E2	
I3		E3	
I4		E4	
I5		E5	
I6		E6	
I7		E7	
I8		E8	
I9		E9	
I10		E10	

สัญญาณเตือนภัย (Early Warning Signals)	เกณฑ์เฝ้าระวัง/เงื่อนไข
1.	
2.	
3.	
4.	

มิติผลกระทบ	ผลกระทบด้านลบที่อาจเกิดขึ้น
1.	
2.	
3.	
4.	
5.	
6.	
7.	
โอกาสเชิงบวกและคุณค่าที่คาดว่าจะสร้างได้	
โอกาสเชิงบวก (Upside Opportunities)	**คุณค่าที่คาดว่าจะสร้างได้**
1.	
2.	
3.	
4.	

เกณฑ์การประเมินระดับความเสี่ยง : โอกาสที่จะเกิดความเสียหายและความรุนแรงของผลกระทบ			
ค่าคะแนน	ระดับคะแนน	“โอกาสที่จะเกิด” (Likelihood)	“ความรุนแรงของผลกระทบ” (Impact)
1	น้อยมาก		
2	น้อย		
3	ปานกลาง		
4	สูง		
5	สูงมาก		

Risk Matrix:

Impact \ Likelihood	1	2	3	4	5
5	5 M	10 H	15 H	20 E	25 E
4	4 M	8 M	12 H	16 E	20 E
3	3 L	6 M	M	12 H	15 H
2	2 L	4 L	6 M	8 M	10 H
1	1 L	2 L	3 L	4 M	5 M

หัวข้อ	การประเมินระดับความเสี่ยง “โอกาส” (L) X “ผลกระทบ” (I) : / เหตุผล
ระดับความเสี่ยงก่อนการจัดการ	ความเสี่ยงสูงมาก (Extreme Risk)
การประเมินระดับความเสี่ยงก่อนจัดการ– Likelihood	L = 4 (สูง) —
การประเมินระดับความเสี่ยงก่อนจัดการ– Impact	I = 5 (สูงมาก) —
Inherent Risk Score	4 × 5 = 20 คะแนน
ระดับจาก Risk Matrix	E – Extreme Risk
ระดับที่ยอมรับได้หลังจัดการ	ความเสี่ยงปานกลาง (Medium Risk)
ระดับความเสี่ยงเป้าหมายหลังการจัดการ – Likelihood	L = 3 (ปานกลาง)
ระดับความเสี่ยงเป้าหมายหลังการจัดการ – Impact	I = 3 (ปานกลาง)
Residual/Target Risk Score	3 × 3 = 9 คะแนน
ระดับจาก Risk Matrix	M – Medium Risk
วิธีตอบสนองความเสี่ยง Risk Response:	Treat/Reduce – ลดความเสี่ยงเป็นหลัก

ประเภท KRI / ตัวบ่งชี้ความเสี่ยง	ระดับความเสี่ยงที่ยอมรับได้ (RA)	ระดับความเบี่ยงเบนที่ยอมรับได้ (RT)
Leading 1:		
Leading 2:		
Lagging 1:		
Lagging 2:		

หลักการกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT)	
หัวข้อ	**หลักการ/แนวทางการกำหนด**
1.	
2.	
3.	
4.	

มาตรการควบคุมที่มีอยู่ในปัจจุบัน (Existing Controls)	มาตรการควบคุมปรับปรุง/ใหม่ (Additional Controls)	ส่วนงานผู้รับผิดชอบ	ระยะเวลาดำเนินการ
1.	**A1** (ปิดGap: I, E)	–	
2.	**A2** (ปิดGap: I, E)	–	
3.	**A3** (ปิดGap:)	–	
4.	**A4** (ปิดGap:)	–	
5.	**A5** (ปิดGap:)	–	

ผลลัพธ์ที่คาดหวัง (Expected Outcomes)	ตัววัดผลลัพธ์ / เป้าหมาย
1.	
2.	
3.	
4.	

ส่วนงานรับผิดชอบ	บทบาทหลักในการบริหารความเสี่ยง F1

คำอธิบายและแนวทางการจัดทำแบบวิเคราะห์และประเมินความเสี่ยง (Risk-MJU01)

1. วัตถุประสงค์ของแบบฟอร์ม

แบบ Risk-MJU01 จัดทำขึ้นเพื่อให้ส่วนงาน/หน่วยงานใช้เป็นเครื่องมือในการ **ระบุ วิเคราะห์ ประเมิน และจัดทำแผนบริหารความเสี่ยงอย่างเป็นระบบ** โดยเชื่อมโยงความเสี่ยงกับวัตถุประสงค์และเป้าหมายของส่วนงาน/หน่วยงาน วิเคราะห์สาเหตุและปัจจัยขับเคลื่อนความเสี่ยง ประเมินระดับความเสี่ยง กำหนดระดับความเสี่ยงที่ยอมรับได้ ตัวชี้วัดความเสี่ยง มาตรการจัดการความเสี่ยง และผลลัพธ์ที่คาดหวัง

การจัดทำแบบฟอร์มควรใช้ข้อมูล ข้อเท็จจริง และหลักฐานเชิงประจักษ์ประกอบการวิเคราะห์ และควรดำเนินการร่วมกันระหว่างเจ้าของความเสี่ยง ผู้รับผิดชอบกระบวนงาน และหน่วยงานที่เกี่ยวข้อง เพื่อให้ผลการประเมินสะท้อนสภาพความเสี่ยงที่แท้จริงและสามารถนำไปใช้ประกอบการตัดสินใจเชิงบริหารได้

---

2. คำอธิบายการกรอกแบบฟอร์มตามหัวข้อ

หัวข้อในแบบฟอร์ม	คำอธิบาย/แนวทางการกรอก
1. **การได้มาซึ่งประเด็นความเสี่ยง**	ระบุที่มาและเหตุผลที่คัดเลือกประเด็นดังกล่าวเป็นความเสี่ยงสำคัญ เช่น ผลการดำเนินงานที่ไม่เป็นไปตามเป้าหมาย ความเสี่ยงคงเหลือจากปีก่อน ผลการวิเคราะห์ยุทธศาสตร์/สภาพแวดล้อม ข้อเสนอแนะจากการตรวจสอบ ข้อร้องเรียน เหตุการณ์ความเสียหาย การเปลี่ยนแปลงกฎหมาย เทคโนโลยี เศรษฐกิจ สังคม หรือความคาดหวังของผู้มีส่วนได้ส่วนเสีย พร้อมอ้างอิงข้อมูลสนับสนุนที่สำคัญ
2. **รหัสความเสี่ยง**	กำหนดรหัสตามประเภทความเสี่ยงที่มหาวิทยาลัยกำหนด เช่น S = Strategic, O = Operational, F = Financial, C = Compliance and Governance และ D = Digital Technology ตามด้วยลำดับของความเสี่ยง เช่น S1, O1, F1
3. **ประเด็นความเสี่ยง (Risk Issue)**	ระบุความเสี่ยงในลักษณะของ **เหตุการณ์หรือความไม่แน่นอนที่อาจส่งผลต่อการบรรลุวัตถุประสงค์** ควรเขียนให้ชัดเจนว่า “อะไรอาจเกิดขึ้น” และ “ส่งผลต่ออะไร” หลีกเลี่ยงการเขียนเป็นเพียงสาเหตุ ปัญหาที่เกิดขึ้นแล้ว หรือชื่อกิจกรรม
4. **ระดับความเสี่ยง**	ระบุระดับความเสี่ยงจากผลการประเมินตาม Risk Matrix ของมหาวิทยาลัย เช่น ต่ำ (Low) ปานกลาง (Medium) สูง (High) หรือสูงมาก (Extreme)
5. **5. ประเภทความเสี่ยง (Risk Category)**	จำแนกประเภทหลักของความเสี่ยงตามสาเหตุหลักและวัตถุประสงค์ที่ได้รับผลกระทบ โดยกำหนดประเภทหลักเพียง 1 ประเภท และสามารถระบุประเภทหรือมิติที่เกี่ยวข้องเพิ่มเติมได้
6. **วัตถุประสงค์เชิงยุทธศาสตร์ (Strategic Objective)**	ระบุวัตถุประสงค์ เป้าประสงค์ หรือผลลัพธ์สำคัญที่ความเสี่ยงอาจส่งผลกระทบ โดยเชื่อมโยงกับแผนยุทธศาสตร์ แผนปฏิบัติการ พันธกิจ หรือวัตถุประสงค์สำคัญของส่วนงาน/หน่วยงาน

หัวข้อในแบบฟอร์ม	คำอธิบาย/แนวทางการกรอก
7. **ผู้บริหารเจ้าของความเสี่ยง (Risk Owner)**	ระบุผู้บริหารที่มีอำนาจ หน้าที่ และความรับผิดชอบในการกำกับความเสี่ยง ตัดสินใจเกี่ยวกับมาตรการจัดการความเสี่ยง ติดตามผล และรายงานหรือยกระดับประเด็นเมื่อความเสี่ยงเกินระดับที่กำหนด
8. **ผู้บริหาร/หน่วยงานร่วมกำกับ**	ระบุผู้บริหารหรือหน่วยงานที่มีบทบาทร่วมในการกำกับ สนับสนุน หรือขับเคลื่อนการจัดการความเสี่ยง โดยเฉพาะความเสี่ยงที่เชื่อมโยงหลายภารกิจหรือหลายหน่วยงาน
9. **หน่วยงานหลักด้านการประสานงาน**	ระบุหน่วยงานที่ทำหน้าที่รวบรวมข้อมูล ประสานผู้รับผิดชอบ ติดตามความก้าวหน้า และจัดทำข้อมูลหรือรายงานผลต่อ Risk Owner
10. **ปีงบประมาณ**	ระบุปีงบประมาณที่จัดทำและบริหารความเสี่ยง เช่น พ.ศ. 2570
11. **ฐานข้อมูลที่ใช้วิเคราะห์**	ระบุข้อมูลที่นำมาใช้วิเคราะห์และประเมินความเสี่ยง เช่น KPI/KRI ย้อนหลัง สถิติผู้เรียน ข้อมูลการเงิน ผลการตรวจสอบ ข้อร้องเรียน เหตุการณ์ความเสียหาย Benchmark ผลสำรวจ หรือข้อมูลแนวโน้มที่เกี่ยวข้อง
12. **หลักฐานเชิงประจักษ์ที่สำคัญ**	ระบุข้อเท็จจริง ตัวเลข ผลการประเมิน รายงาน หรือหลักฐานสำคัญที่สนับสนุนว่าความเสี่ยงมีอยู่จริงหรือมีแนวโน้มเกิดขึ้น โดยควรระบุแหล่งที่มาและช่วงเวลาของข้อมูลให้สามารถตรวจสอบย้อนกลับได้
13. **แนวโน้มความเสี่ยง (Risk Trend)**	ประเมินทิศทางของความเสี่ยงเมื่อเปรียบเทียบกับรอบก่อน เช่น **เพิ่มขึ้น (↑) / คงที่ (⟶) / ลดลง (↓)** พร้อมระบุเหตุผลหรือข้อมูลสนับสนุน
14. **คำนิยามความเสี่ยง**	อธิบายความหมายของประเด็นความเสี่ยงให้ชัดเจน เพื่อให้ผู้เกี่ยวข้องมีความเข้าใจตรงกัน โดยระบุลักษณะสำคัญและเงื่อนไขของความเสี่ยง
15. **เหตุการณ์ความเสี่ยง (Risk Event)**	ระบุเหตุการณ์ที่อาจเกิดขึ้นและทำให้ไม่สามารถบรรลุวัตถุประสงค์ ควรเขียนเป็นเหตุการณ์ที่ชัดเจนและสามารถติดตามหรือประเมินได้
16. **ขอบเขตความเสี่ยง (Risk Scope)**	กำหนดขอบเขตของการวิเคราะห์ เช่น ภารกิจ กระบวนงาน ระบบ กลุ่มผู้ได้รับผลกระทบ หน่วยงาน พื้นที่ หรือช่วงเวลาที่ครอบคลุม เพื่อป้องกันการวิเคราะห์กว้างหรือแคบเกินไป
17. **คำแถลงระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite Statement)**	ระบุหลักการหรือระดับความเสี่ยงที่ส่วนงาน/มหาวิทยาลัยยินดีรับในการดำเนินงานเพื่อให้บรรลุวัตถุประสงค์ โดยต้องสอดคล้องกับนโยบาย Risk Appetite ของมหาวิทยาลัย
18. **ปัจจัยเสี่ยงภายใน (Internal Risk Factors: I)**	วิเคราะห์ **สาเหตุรากหรือปัจจัยขับเคลื่อนความเสี่ยงที่เกิดจากภายในองค์กร** เช่น บุคลากร สมรรถนะ กระบวนงาน ระบบ เทคโนโลยี ข้อมูล งบประมาณ โครงสร้าง การกำกับ หรือการควบคุม โดยกำหนดรหัส I1, I2, I3...
19. **ปัจจัยเสี่ยงภายนอก (External Risk Factors: E)**	วิเคราะห์ปัจจัยภายนอกที่ส่วนงานควบคุมได้จำกัดหรือไม่สามารถควบคุมได้ เช่น เศรษฐกิจ สังคม ประชากร เทคโนโลยี กฎหมาย นโยบายรัฐ การแข่งขัน ภัยธรรมชาติ หรือพฤติกรรมผู้มีส่วนได้ส่วนเสีย โดยกำหนดรหัส E1, E2, E3...
20. **สัญญาณเตือนภัย (Early Warning Signals: EWS)**	ระบุข้อมูล เหตุการณ์ หรือแนวโน้มที่สามารถบ่งชี้ว่าความเสี่ยงกำลังเพิ่มขึ้นหรืออาจเกิดขึ้นในอนาคต ควรเป็นสิ่งที่สามารถติดตามได้ก่อนเกิดผลกระทบ

หัวข้อในแบบฟอร์ม	คำอธิบาย/แนวทางการกรอก
21. เกณฑ์เฝ้าระวัง/เงื่อนไข	กำหนดค่า เงื่อนไข หรือ Trigger ที่ชัดเจนสำหรับ EWS เช่น ต่ำกว่าเป้าหมายติดต่อกัน 2 รอบ เพิ่มขึ้นเกินร้อยละที่กำหนด หรือเกิดเหตุการณ์ตามเงื่อนไขที่กำหนด เพื่อให้สามารถดำเนินการตอบสนองได้ทันท่วงที
22. มิติผลกระทบ	ระบุมิติที่อาจได้รับผลกระทบจากความเสี่ยง เช่น ยุทธศาสตร์ การดำเนินงาน การเงิน กฎหมายและธรรมาภิบาล เทคโนโลยีดิจิทัล ชื่อเสียง ความปลอดภัย ผู้เรียน บุคลากร สิ่งแวดล้อม หรือความต่อเนื่อง
23. ผลกระทบด้านลบที่อาจเกิดขึ้น	อธิบายผลที่อาจเกิดขึ้นหากเหตุการณ์ความเสี่ยงเกิดขึ้น โดยควรระบุผลกระทบต่อวัตถุประสงค์ ผลลัพธ์ KPI ผู้มีส่วนได้ส่วนเสีย การเงิน ชื่อเสียง หรือความต่อเนื่องให้ชัดเจน
24. โอกาสเชิงบวก (Upside Opportunities)	พิจารณาว่าความไม่แน่นอนหรือการจัดการความเสี่ยงดังกล่าวอาจสร้างโอกาสใดให้แก่องค์กร เช่น เพิ่มประสิทธิภาพ สร้างรายได้ พัฒนานวัตกรรม ยกระดับบริการ หรือสร้างความได้เปรียบในการแข่งขัน
25. คุณค่าที่คาดว่าจะสร้างได้	ระบุคุณค่าหรือประโยชน์ที่คาดว่าจะได้รับหากสามารถใช้ประโยชน์จากโอกาสหรือบริหารความเสี่ยงได้อย่างมีประสิทธิผล โดยควรกำหนดให้สามารถเชื่อมโยงกับผลลัพธ์ขององค์กรได้
26. เกณฑ์การประเมินระดับความเสี่ยง – Likelihood	ประเมินโอกาสที่จะเกิดความเสี่ยงตามเกณฑ์ 1–5 ของมหาวิทยาลัย โดยใช้ข้อมูลย้อนหลัง ความถี่ ความน่าจะเป็น แนวโน้ม หรือหลักฐานประกอบ และระบุเหตุผลของคะแนน
27. เกณฑ์การประเมินระดับความเสี่ยง – Impact	ประเมินความรุนแรงของผลกระทบตามเกณฑ์ 1–5 โดยพิจารณาผลกระทบต่อวัตถุประสงค์ที่เกี่ยวข้อง และใช้ระดับผลกระทบที่รุนแรงที่สุดซึ่งมีความเป็นไปได้อย่างสมเหตุสมผล พร้อมระบุเหตุผลของคะแนน
28. ระดับความเสี่ยงก่อนการจัดการ (Inherent Risk)	ประเมินระดับความเสี่ยง **ก่อนพิจารณาผลของมาตรการควบคุมหรือมาตรการจัดการเพิ่มเติม** โดยคำนวณจาก **Likelihood × Impact** และเทียบกับ Risk Matrix ของมหาวิทยาลัย
29. ระดับความเสี่ยงเป้าหมายหลังการจัดการ (Target Risk)	กำหนดระดับความเสี่ยงที่คาดว่าจะเหลือภายหลังดำเนินมาตรการตามแผน โดยกำหนดค่า L และ I เป้าหมายให้มีเหตุผล สอดคล้องกับมาตรการและระดับความเสี่ยงที่ยอมรับได้
30. วิธีตอบสนองความเสี่ยง (Risk Response)	ระบุแนวทางตอบสนองที่เหมาะสม เช่น **หลีกเลี่ยง (Avoid), ลด/ควบคุม (Treat/Reduce), โอน/แบ่งปัน (Transfer/Share), ยอมรับ (Accept)** หรือแนวทางอื่นตามกรอบที่มหาวิทยาลัยกำหนด
31. ตัวชี้วัดความเสี่ยง (Key Risk Indicator: KRI)	กำหนดตัวชี้วัดที่สะท้อนการเปลี่ยนแปลงของระดับความเสี่ยง โดยควรมีทั้ง **Leading KRI** ซึ่งใช้เตือนล่วงหน้า และ **Lagging KRI** ซึ่งสะท้อนผลหรือเหตุการณ์ที่เกิดขึ้นแล้ว ตัวชี้วัดต้องมีข้อมูลที่สามารถติดตามได้จริง
32. ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA)	กำหนดระดับหรือค่าของ KRI ที่องค์กรเห็นว่ายอมรับได้และสอดคล้องกับวัตถุประสงค์ นโยบาย และความสามารถในการรองรับความเสี่ยง

หัวข้อในแบบฟอร์ม	คำอธิบาย/แนวทางการกรอก
33. ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT)	กำหนดขอบเขตความเบี่ยงเบนจาก RA ที่ยังสามารถยอมรับได้ชั่วคราว หากเกิน RT ต้องมีการดำเนินการแก้ไข รายงาน หรือยกระดับตามหลักเกณฑ์ที่กำหนด
34. มาตรการควบคุมที่มีอยู่ในปัจจุบัน (Existing Controls)	ระบุมาตรการ ระบบ กลไก หรือกิจกรรมที่มีอยู่และดำเนินการจริงในปัจจุบันเพื่อป้องกัน ลด ตรวจจับ หรือจัดการสาเหตุและผลกระทบของความเสี่ยง ไม่ควรระบุเพียงว่ามีระเบียบ คณะกรรมการ หรือระบบ หากไม่สามารถอธิบายได้ว่าการควบคุมนั้นทำงานอย่างไร
35. มาตรการควบคุมปรับปรุง/ใหม่ (Additional Controls)	กำหนดมาตรการเพิ่มเติมสำหรับสาเหตุหรือช่องว่างที่ Existing Controls ยังไม่สามารถจัดการได้เพียงพอ ควรระบุให้ชัดว่าแต่ละมาตรการ **ปิด Gap หรือจัดการ Root Cause ใด (I/E)** และต้องสามารถนำไปปฏิบัติและติดตามผลได้
36. ส่วนงานผู้รับผิดชอบ	ระบุส่วนงาน/หน่วยงานที่รับผิดชอบดำเนินมาตรการแต่ละรายการ โดยควรกำหนดหน่วยงานหลักและหน่วยงานร่วมให้ชัดเจนในกรณีที่มีหลายหน่วยงานเกี่ยวข้อง
37. ระยะเวลาดำเนินการ	กำหนดช่วงเวลา กำหนดแล้วเสร็จ หรือ Milestone ของมาตรการให้ชัดเจน เช่น ไตรมาส 1/2570 หรือภายในเดือนมีนาคม 2570 เพื่อให้สามารถติดตามความก้าวหน้าได้
38. ผลลัพธ์ที่คาดหวัง (Expected Outcomes)	ระบุการเปลี่ยนแปลงหรือผลที่ต้องการให้เกิดขึ้นจากการดำเนินมาตรการ โดยเน้น **Outcome** มากกว่าการระบุเพียงกิจกรรมหรือ Output เช่น “สัดส่วนบุคลากรที่มีสมรรถนะตามเกณฑ์เพิ่มขึ้น” แทน “จัดอบรมบุคลากร”
39. ตัววัดผลลัพธ์/เป้าหมาย	กำหนดตัวชี้วัดและค่าเป้าหมายที่สามารถใช้พิสูจน์ว่ามาตรการก่อให้เกิดผลตามที่คาดหวัง เช่น ร้อยละ จำนวน ระยะเวลา อัตราความสำเร็จ หรือค่าผลการดำเนินงานที่ชัดเจน
40. ส่วนงานรับผิดชอบและบทบาทหลักในการบริหารความเสี่ยง	สรุปบทบาทของแต่ละหน่วยงานที่เกี่ยวข้องกับความเสี่ยง เช่น หน่วยงานเจ้าภาพ หน่วยงานสนับสนุน หน่วยงานเจ้าของข้อมูล หรือหน่วยงานติดตาม เพื่อให้การประสานงานและความรับผิดชอบไม่ซ้ำซ้อนหรือเกิดช่องว่าง

3. ลำดับการคิดในการจัดทำแบบฟอร์ม

เพื่อให้การจัดทำแบบ Risk-MJU01 มีความเชื่อมโยงและไม่เป็นเพียงการกรอกข้อมูลตามช่อง ให้ส่วนงาน/หน่วยงานดำเนินการตามลำดับ ดังนี้

วัตถุประสงค์/เป้าหมาย ⟶ ประเด็นความเสี่ยง ⟶ เหตุการณ์ความเสี่ยง ⟶ Root Cause (I/E) ⟶ ผลกระทบ ⟶ Existing Controls ⟶ ประเมิน L × I ⟶ RA/RT และ KRI ⟶ วิเคราะห์ Control Gap ⟶ Additional Controls ⟶ ผู้รับผิดชอบ/ระยะเวลา ⟶ Expected Outcomes ⟶ ติดตามและประเมินผล

หลักสำคัญคือ **มาตรการเพิ่มเติมทุกมาตรการควรสามารถเชื่อมโยงกลับไปยังสาเหตุหรือช่องว่างที่ต้องการจัดการ และผลลัพธ์ที่คาดหวังต้องสามารถวัดได้** เพื่อให้สามารถประเมินได้ในรอบการติดตามว่าการดำเนินมาตรการช่วยลดระดับความเสี่ยงได้จริงหรือไม่

4. ข้อควรระวังในการจัดทำแบบฟอร์ม

- ไม่เขียน **“สาเหตุ”** เป็นประเด็นความเสี่ยง เช่น “บุคลากรไม่เพียงพอ” หากเหตุการณ์ความเสี่ยงที่แท้จริงคือ “การให้บริการอาจไม่เป็นไปตามมาตรฐานหรือระยะเวลาที่กำหนด”
- ไม่เขียน **“ผลกระทบ”** เป็นประเด็นความเสี่ยง เช่น “มหาวิทยาลัยเสียชื่อเสียง” โดยไม่ระบุเหตุการณ์และสาเหตุของความเสี่ยง
- ไม่กำหนดมาตรการเป็นเพียง **“ติดตามอย่างต่อเนื่อง” หรือ “กำชับให้ดำเนินการ”** โดยไม่มีวิธีดำเนินการ ผู้รับผิดชอบ กำหนดเวลา และผลลัพธ์ที่ต้องการ
- ไม่กำหนด KRI ที่เป็นเพียงตัวชี้วัดความสำเร็จของกิจกรรม หากตัวชี้วัดนั้นไม่สามารถสะท้อนการเพิ่มขึ้นหรือลดลงของความเสี่ยง
- การกำหนด Target Risk ต้องสัมพันธ์กับประสิทธิผลที่คาดหวังจากมาตรการ ไม่ควรลดคะแนน L หรือ I โดยไม่มีเหตุผลหรือหลักฐานรองรับ
- ข้อมูลที่ใช้ประเมินควรสามารถตรวจสอบย้อนกลับได้ และควรใช้ฐานข้อมูลหรือวิธีการประเมินเดียวกันในการติดตามแต่ละรอบ เพื่อให้สามารถเปรียบเทียบแนวโน้มได้อย่างเหมาะสม

แบบฟอร์มจัดทำแผนบริหารความเสี่ยง

(มจ-ส-01)

แผนบริหารความเสี่ยง ..... ประจำปีงบประมาณ พ.ศ.2XXX

ตัวชี้วัดความสำเร็จของแผน (KPI) ภาพรวม : 1. ดำเนินกิจกรรมควบคุมตามแผนอย่างน้อยร้อยละ 80 / 2. สามารถลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ไม่น้อยกว่าร้อยละ 80 (กำหนดตามบริบทส่วนงาน)

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ระดับความเสี่ยงก่อนการจัดการ				ระดับความเสี่ยงที่ยอมรับได้				Risk Treatment	สาเหตุ (Root Causes)	ตัวบ่งชี้ความเสี่ยง / สัญญาณเตือนภัย (KRI) :			กิจกรรมเพื่อลดความเสี่ยง		
			L	I	คะแนน	ระดับ	L	I	คะแนน	ระดับ			Leading Indicators	RA	RT	มาตรการ/ กิจกรรมลดความเสี่ยง	ผู้รับผิดชอบกิจกรรม	ระยะเวลาดำเนินการ
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)
S1		ด้านยุทธศาสตร์ (Strategic Risk: S)																
O1		ด้านการดำเนินงาน (Operational Risk: O)																
F1		ด้านการเงิน (Financial Risk: F)																
C1		ด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (Compliance and Governance Risk: C)																
D1		ด้านเทคโนโลยีดิจิทัล (Digital Technology Risk: D)																

แผนบริหารความเสี่ยง ..... ประจำปีงบประมาณ พ.ศ.2XXX

ตัวชี้วัดความสำเร็จของแผน (KPI) ภาพรวม : 1. ดำเนินกิจกรรมควบคุมตามแผนอย่างน้อยร้อยละ 80 / 2. สามารถลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ไม่น้อยกว่าร้อยละ 80 (กำหนดตามบริบทส่วนงาน)

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ระดับความเสี่ยงก่อนการจัดการ				ระดับความเสี่ยงที่ยอมรับได้				Risk Treatment	สาเหตุ (Root Causes)	ตัวบ่งชี้ความเสี่ยง / สัญญาณเตือนภัย (KRI) :			กิจกรรมเพื่อลดความเสี่ยง		
			L	I	คะแนน	ระดับ	L	I	คะแนน	ระดับ			Leading Indicators	RA	RT	มาตรการ/ กิจกรรมลดความเสี่ยง	ผู้รับผิดชอบกิจกรรม	ระยะเวลาดำเนินการ
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)

สรุปการจัดทำแผนการบริหารความเสี่ยง ประจำปีงบประมาณ 25XX

หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริการจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 (โดยที่สมควรให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการความเสี่ยง เพื่อให้การดำเนินงานบรรลุวัตถุประสงค์ตามยุทธศาสตร์ที่หน่วยงานของรัฐกำหนด)

ประเภทความเสี่ยง	ประเด็นความเสี่ยง	จำนวนกิจกรรม/ประเด็นความเสี่ยง
1. ความเสี่ยงเชิงกลยุทธ์ (Strategic Risk)	S1:	
2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)	O1:	
2. ความเสี่ยงด้านการเงิน (Financial Risk)	F1:	
4. ความเสี่ยงด้านการปฏิบัติตามกฎหมาย/กำกับดูแล (Compliance Risk)	C1:	
5. ความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Technology Risk: D)	D1:	

1. มีกิจกรรมเพื่อลดความเสี่ยงในแผน จำนวน _____ กิจกรรม
2. มีประเด็นความเสี่ยงในแผน จำนวน _____ ประเด็น

ผ่านความเห็นชอบจากคณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน คราวประชุมครั้งที่ ..... เมื่อวันที่ .....

ผ่านความเห็นชอบจากคณะกรรมการบริหารคณะ ในคราวประชุมครั้งที่ ..... เมื่อวันที่ .....

สรุปรายงานผลการดำเนินงานการบริหารความเสี่ยง มหาวิทยาลัยแม่โจ้

ประจำปีงบประมาณ พ.ศ. 2569 รอบ .....XX..... เดือน

(1 ตุลาคม ..... – XXXXXXXXXX)

.....

.....

.....

.....

.....

.....

.....

.....

.....

ตารางที่ 1: สรุปผลภาพรวมการดำเนินงานตามการบริหารความเสี่ยง

สรุปผลการดำเนินงานตามแผนบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ.XXXX *รอบ 6 เดือน ณ วันที่ 1 ตุลาคม 2568 ถึง 31 มีนาคม 2569*				
1. กิจกรรมลดความเสี่ยงมีทั้งหมด	**กิจกรรม**	**ผล 6 เดือน/%**	**ผล 9 เดือน/%**	**ผล 12 เดือน/%**
1.1 กิจกรรมดำเนินการแล้วเสร็จ				
1.2 กิจกรรมยังอยู่ระหว่างดำเนินการ				
1.3 กิจกรรมไม่ได้จัดทำ/ยังไม่ได้ดำเนินการ				
2. ประเด็นความเสี่ยง	**ประเด็น**	**ผล 6 เดือน/%**	**ผล 9 เดือน/%**	**ผล 12 เดือน/%**
2.1 ความเสี่ยงลดลงหรืออยู่ในระดับที่ยอมรับได้ เมื่อเทียบคะแนนที่ประเมินไว้ก่อนดำเนินกิจกรรม				
2.2 ความเสี่ยงไม่ลดลงและยังคงมีอยู่ เมื่อเทียบกับคะแนนที่ประเมินก่อนดำเนินกิจกรรม)	2 ประเด็น			
3. ตัวชี้วัด KPI ของแผนบริหารความเสี่ยง	**เป้าหมาย**	**ผล 6 เดือน/%**	**ผล 9 เดือน/%**	**ผล 12 เดือน/%**
1. ดำเนินการตามมาตรการ/กิจกรรมลดความเสี่ยง	≥ 80%			

ตารางที่ 2: สรุปผลการดำเนินงานตาม KRI ตัวชี้วัดความเสี่ยง

ความเสี่ยง	KRI	(RA)	(RT)	ผล 6 เดือน
S1:				
F1:				
O1:				
C1:				
D1:				

ตารางที่ 3 : สรุปแนวโน้มการบริหารความเสี่ยงตามแผน

คามเสี่ยง	ระดับค่าคะแนนความเสี่ยง		
	ก่อนดำเนินการ	หลังดำเนินการ	แน้วโน้มความเสี่ยง
S1:			
F1:			
O1:			
C1:			
D1:			

ตางรางที่ 4

สรุปผลการดำเนินงานรายประเด็นความเสี่ยง

รหัสความเสี่ยง :	**ชื่อความเสี่ยง:**
ประเภทความเสี่ยง:	
ผู้บริหารเจ้าของความเสี่ยง (Risk Owners)	
สัญญาณเตือนภัยล่วงหน้า (Early Warning Signals)	
วัตถุประสงค์ความเสี่ยง	

ผลการติดตามตัวบ่งชี้ความเสี่ยง (Key Risk Indicators : KRIs)

ตัวบ่งชี้ความเสี่ยง (KRI)	Risk Appetite: RA	Risk Tolerance: RT	ผลงานรอบ 6 เดือน	สถานะ

ผลการประเมินระดับความเสี่ยง:

รอบการรายงาน	ค่าคะแนนก่อนดำเนินงาน	ค่าคะแนนที่ยอมรับได้	ค่าคะแนนปัจจุบัน
รอบ 6 เดือน			
วิเคราะห์ผลการประเมินความเสี่ยง :			

สรุปผลการดำเนินมาตรการควบคุม (รอบ 6 เดือน):

มาตรการ/กิจกรรม	ผลการดำเนินงาน	ปัญหา/อุปสรรค	แนวทางแก้ไข	สถานะกิจกรรม
1.				✓
2.				O
3.				X
4.				

คำอธิบายแบบฟอร์มรายงานผลความก้าวหน้าการบริหารความเสี่ยง

(Risk Management Progress Report Guideline)

แบบฟอร์มรายงานผลความก้าวหน้าการบริหารความเสี่ยง จัดทำขึ้นเพื่อใช้เป็นมาตรฐานกลางในการติดตาม ประเมินผล และรายงานความก้าวหน้าการดำเนินงานตามแผนบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้ โดยรายงานครอบคลุมผลการดำเนินงาน ระดับความเสี่ยง ตัวชี้วัดความเสี่ยง (Key Risk Indicators: KRIs) ตลอดจนผลการดำเนินมาตรการควบคุม เพื่อใช้ประกอบการกำกับติดตามของผู้บริหารและคณะกรรมการบริหารความเสี่ยง

ส่วนหัวรายงาน (Report Information)

ให้ระบุข้อมูลพื้นฐานของรายงาน ดังนี้

- **ชื่อรายงาน (Report Title)** : *Risk Management Report*
- **หน่วยงาน (Organization)** : ระบุชื่อคณะ สำนัก สถาบัน หรือหน่วยงาน เช่น มหาวิทยาลัยแม่โจ้
- **ปีงบประมาณ (Fiscal Year)** : ระบุปีงบประมาณที่รายงาน
- **รอบการรายงาน (Reporting Period)** : เช่น รอบ 6 เดือน รอบ 9 เดือน หรือรอบ 12 เดือน
- **ช่วงเวลารายงาน (Reporting Period Date)** : ระบุวันที่เริ่มต้นและวันที่สิ้นสุดของรอบรายงาน

ตารางที่ 1 สรุปผลภาพรวมการดำเนินงานตามแผนบริหารความเสี่ยง

ใช้สำหรับสรุปผลการดำเนินงานภาพรวมของแผนบริหารความเสี่ยงของหน่วยงาน ประกอบด้วย

1. กิจกรรมลดความเสี่ยง

ให้ระบุจำนวนกิจกรรมทั้งหมดที่กำหนดไว้ในแผนบริหารความเสี่ยง และจำแนกผลการดำเนินงานเป็น

- **ดำเนินการแล้วเสร็จ** หมายถึง ดำเนินการครบถ้วนตามแผนและบรรลุผลตามวัตถุประสงค์
- **อยู่ระหว่างดำเนินการ** หมายถึง เริ่มดำเนินการแล้ว มีความก้าวหน้าตามแผน แต่ยังไม่แล้วเสร็จ
- **ยังไม่ได้ดำเนินการ** หมายถึง ยังไม่ได้เริ่มดำเนินการ หรือไม่สามารถดำเนินการได้ตามแผน

2. ประเด็นความเสี่ยง

ให้ระบุจำนวนประเด็นความเสี่ยงทั้งหมด พร้อมสรุปผล ดังนี้

- จำนวนประเด็นที่สามารถลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- จำนวนประเด็นที่ยังไม่สามารถลดระดับความเสี่ยงได้ และต้องติดตามต่อ

3. ตัวชี้วัดความสำเร็จของแผนบริหารความเสี่ยง (KPI)

รายงานผลการดำเนินงานเทียบกับค่าเป้าหมาย (Target) ที่กำหนด พร้อมสรุปผลความสำเร็จของการดำเนินงานในภาพรวมของหน่วยงาน

ตารางที่ 2 สรุปผลการดำเนินงานตามตัวชี้วัดความเสี่ยง (Key Risk Indicators : KRIs)

ใช้สำหรับติดตามผลการดำเนินงานของตัวชี้วัดความเสี่ยงในแต่ละประเด็น เพื่อประเมินแนวโน้มของความเสี่ยงและประสิทธิผลของมาตรการควบคุม

ให้ระบุข้อมูล ดังนี้

- รหัสและชื่อประเด็นความเสี่ยง เช่น
    - **S** : Strategic Risk
    - **O** : Operational Risk
    - **F** : Financial Risk
    - **C** : Compliance Risk
- ตัวชี้วัดความเสี่ยง (KRI)
- ค่า **Risk Appetite (RA)** ระดับความเสี่ยงที่องค์กรยอมรับได้
- ค่า **Risk Tolerance (RT)** ระดับความเบี่ยงเบนที่องค์กรยอมรับได้
- ผลการดำเนินงานในรอบรายงาน

ข้อมูลดังกล่าวใช้สำหรับติดตามแนวโน้มความเสี่ยงและประเมินว่าความเสี่ยงอยู่ภายในระดับที่องค์กรกำหนดหรือไม่

ตารางที่ 3 สรุปแนวโน้มการบริหารความเสี่ยงตามแผน

ใช้สำหรับเปรียบเทียบระดับความเสี่ยงก่อนดำเนินมาตรการกับระดับความเสี่ยงปัจจุบัน เพื่อประเมินประสิทธิผลของการบริหารจัดการความเสี่ยง

ให้ระบุ

- ระดับความเสี่ยงก่อนดำเนินมาตรการ
- ระดับความเสี่ยงปัจจุบัน
- แนวโน้มของความเสี่ยง ได้แก่
    - ลดลง
    - คงที่
    - เพิ่มขึ้น

ผลการเปรียบเทียบดังกล่าวใช้ประกอบการพิจารณาความเหมาะสมของมาตรการควบคุมและการปรับปรุงแผนบริหารความเสี่ยงในรอบถัดไป

ตารางที่ 4 สรุปผลการดำเนินงานรายประเด็นความเสี่ยง

ใช้สำหรับรายงานรายละเอียดเชิงลึกของแต่ละประเด็นความเสี่ยง โดยประกอบด้วยหัวข้อสำคัญ ดังนี้

1. ข้อมูลพื้นฐานของความเสี่ยง

ระบุข้อมูลพื้นฐาน ได้แก่

- รหัสความเสี่ยง
- ชื่อความเสี่ยง
- ประเภทความเสี่ยง
- ผู้บริหารเจ้าของความเสี่ยง (Risk Owner)
- สัญญาณเตือนภัยล่วงหน้า (Early Warning Signals)
- วัตถุประสงค์ของการบริหารความเสี่ยง

---

2. ผลการติดตามตัวบ่งชี้ความเสี่ยง (KRIs)

รายงานผลการติดตามตัวชี้วัดความเสี่ยง ประกอบด้วย

- ตัวชี้วัดความเสี่ยง (KRI)
- ค่า Risk Appetite (RA)
- ค่า Risk Tolerance (RT)
- ผลการดำเนินงานในรอบรายงาน
- สถานะของตัวชี้วัด

---

3. ผลการประเมินระดับความเสี่ยง

ระบุข้อมูล ดังนี้

- ค่าคะแนนก่อนดำเนินมาตรการ
- ค่าคะแนนความเสี่ยงที่ยอมรับได้
- ค่าคะแนนความเสี่ยงปัจจุบัน

พร้อมวิเคราะห์ผลการประเมิน โดยอธิบาย

- สาเหตุที่ทำให้ระดับความเสี่ยงเปลี่ยนแปลง
- ปัจจัยสนับสนุนหรือปัจจัยที่ส่งผลต่อระดับความเสี่ยง
- ผลกระทบที่เกิดขึ้น
- ประเด็นที่ต้องติดตามหรือเฝ้าระวังเพิ่มเติม

---

4. สรุปผลการดำเนินมาตรการควบคุม

ให้รายงานรายละเอียดของแต่ละมาตรการ ประกอบด้วย

- มาตรการหรือกิจกรรมที่ดำเนินการ
- ผลการดำเนินงานที่เกิดขึ้นจริง
- ปัญหาและอุปสรรค
- แนวทางแก้ไขหรือแนวทางพัฒนาเพิ่มเติม
- สถานะของกิจกรรม

ให้ใช้สถานะมาตรฐาน ดังนี้

สัญลักษณ์	สถานะ	ความหมาย
✓	ดำเนินการแล้ว	ดำเนินการครบถ้วนตามแผนและบรรลุผลตามวัตถุประสงค์
○	อยู่ระหว่างดำเนินการ	ดำเนินการตามแผน มีความก้าวหน้าอย่างต่อเนื่อง และคาดว่าจะแล้วเสร็จตามกำหนด
✗	ยังไม่ได้ดำเนินการ	ยังไม่สามารถดำเนินการได้ เนื่องจากมีข้อจำกัดหรืออยู่ระหว่างรอปัจจัยสนับสนุน โดยจะเร่งดำเนินการในรอบถัดไป

ข้อเสนอแนะในการจัดทำรายงาน

เพื่อให้รายงานมีคุณภาพและสามารถใช้ประกอบการตัดสินใจของผู้บริหารได้อย่างมีประสิทธิภาพ ควรดำเนินการดังนี้

- รายงานผลการดำเนินงานให้สะท้อนผลลัพธ์ที่เกิดขึ้นจริง พร้อมข้อมูลหรือหลักฐานเชิงประจักษ์ประกอบ
- ไม่ควรระบุเพียงว่า "อยู่ระหว่างดำเนินการ" โดยไม่มีรายละเอียดความก้าวหน้าหรือผลที่เกิดขึ้น
- ทบทวนและประเมินระดับความเสี่ยงให้สอดคล้องกับผลการดำเนินงานและสถานการณ์ปัจจุบัน
- กำหนดตัวชี้วัดความเสี่ยง (KRI) ที่สามารถสะท้อนแนวโน้มความเสี่ยงล่วงหน้า วัดผลได้อย่างชัดเจน และสามารถติดตามผลได้อย่างต่อเนื่อง
- วิเคราะห์สาเหตุของความเสี่ยงและผลกระทบที่เกิดขึ้น เพื่อใช้เป็นข้อมูลในการปรับปรุงมาตรการควบคุมและแผนบริหารความเสี่ยงในรอบถัดไป

หมายเหตุ:

- ใช้แบบฟอร์มที่มหาวิทยาลัยกำหนดเป็นมาตรฐานกลาง เพื่อให้ทุกส่วนงานจัดทำรายงานในรูปแบบเดียวกันและสามารถเปรียบเทียบข้อมูลได้อย่างเป็นระบบ
- ส่วนงานสามารถปรับรายละเอียดของรายงานให้สอดคล้องกับบริบทและลักษณะภารกิจของหน่วยงาน เช่น ด้านการเงิน บุคลากร การวิจัย เทคโนโลยีสารสนเทศ หรือภารกิจเฉพาะด้านอื่น ๆ โดยต้องคงสาระสำคัญตามที่มหาวิทยาลัยกำหนด
- ข้อมูลที่รายงานต้องมีความครบถ้วน ถูกต้อง เชื่อถือได้ และสามารถตรวจสอบย้อนกลับได้ ครอบคลุมกิจกรรมดำเนินงาน ตัวชี้วัด ผลการดำเนินงาน ปัญหา อุปสรรค และแนวทางปรับปรุงแก้ไข
- ให้จัดทำรายงานตามรอบระยะเวลาที่มหาวิทยาลัยกำหนด ได้แก่ รอบ 6 เดือน รอบ 9 เดือน และรอบ 12 เดือน เพื่อสะท้อนความก้าวหน้า ผลสัมฤทธิ์ และแนวโน้มของการบริหารความเสี่ยงอย่างต่อเนื่อง
- แบบฟอร์มสามารถประยุกต์ใช้ได้ทั้งใน **Microsoft Word** สำหรับจัดทำรายงานและเอกสารเสนออย่างเป็นทางการ และ **Microsoft Excel** สำหรับบันทึกข้อมูล ติดตามผล และวิเคราะห์ข้อมูลเชิงตัวเลขหรือสถิติ โดยทั้งสองรูปแบบควรมีโครงสร้างข้อมูลที่สอดคล้องกันเพื่อให้สามารถเชื่อมโยงและตรวจสอบข้อมูลได้อย่างมีประสิทธิภาพ