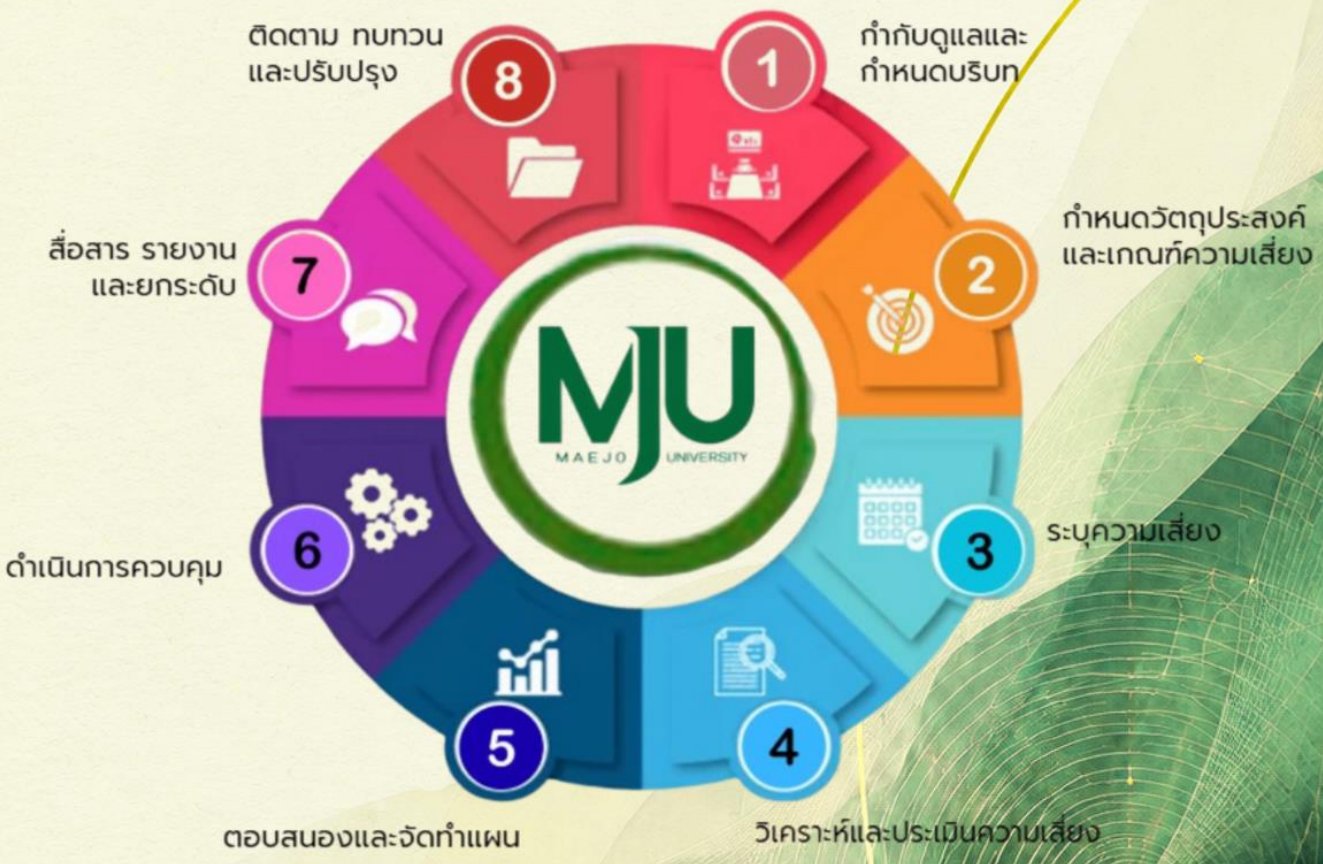
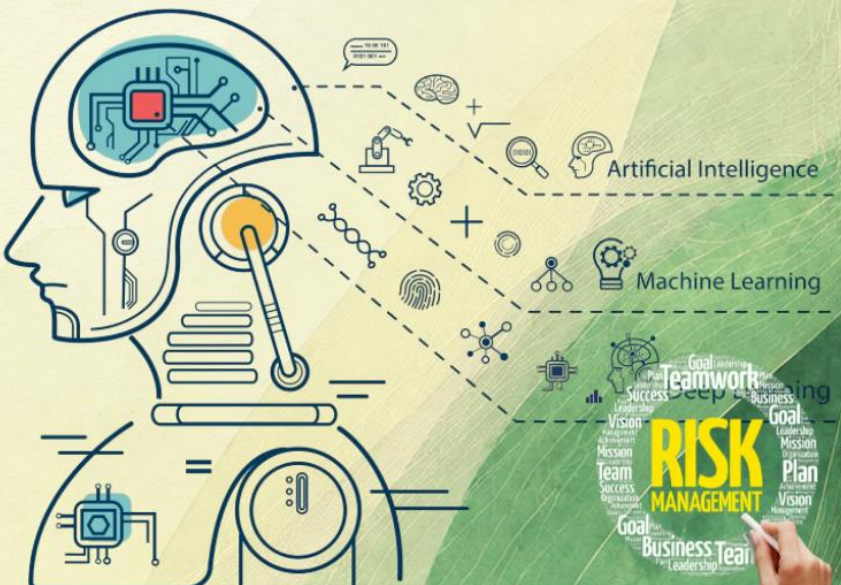
คู่มือการบริหารความเสี่ยง

มหาวิทยาลัยแม่โจ้

ENTERPRISE RISK MANAGEMENT

ฉบับปรับปรุง พ.ศ. 2570





MAEJO UNIVERSITY
ENTERPRISE RISK MANAGEMENT MANUAL
REVISED EDITION 2027

คำนำ

มหาวิทยาลัยแม่โจ้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM) ในฐานะกลไกที่สนับสนุนการกำกับดูแล การตัดสินใจ และการขับเคลื่อนยุทธศาสตร์ภายใต้ความไม่แน่นอน เพื่อให้มหาวิทยาลัยสามารถดำเนินพันธกิจได้อย่างมีประสิทธิผลและปรับตัวต่อการเปลี่ยนแปลง

คู่มือการบริหารความเสี่ยงองค์กร มหาวิทยาลัยแม่โจ้ พ.ศ. 2570 ฉบับนี้จัดทำขึ้นเพื่อเป็นกรอบกลางสำหรับมหาวิทยาลัยและส่วนงานในการบริหารความเสี่ยงและโอกาส โดยเชื่อมโยงกับการกำหนดยุทธศาสตร์ การบริหารผลการดำเนินงาน การจัดสรรทรัพยากร การควบคุมภายใน และการบริหารความต่อเนื่อง เพื่อสนับสนุนการสร้าง รักษา และเพิ่มคุณค่าให้แก่มหาวิทยาลัยและผู้มีส่วนได้ส่วนเสียอย่างยั่งยืน

คู่มือฉบับนี้ประยุกต์ใช้ ISO 31000:2018, COSO Enterprise Risk Management—Integrating with Strategy and Performance (2017) และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 รวมทั้งแนวทางด้านการควบคุมภายใน การตรวจสอบภายใน และการพัฒนาองค์กรสู่ความเป็นเลิศ โดยปรับให้เหมาะสมกับบริบทและพันธกิจของมหาวิทยาลัย ครอบคลุมหลักการ นโยบาย โครงสร้างความรับผิดชอบ กระบวนการ เกณฑ์ประเมิน ตัวชี้วัด และแบบฟอร์มที่ใช้ในการปฏิบัติงาน

สาระสำคัญของคู่มือมุ่งให้การบริหารความเสี่ยงสนับสนุนการตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเป็นฐาน เชื่อมโยงระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) และเงื่อนไขการตอบสนองหรือยกระดับ เพื่อให้ผู้รับผิดชอบสามารถตรวจพบการเปลี่ยนแปลงและดำเนินการได้อย่างทันเวลา พร้อมพิจารณาความสัมพันธ์และผลกระทบของความเสี่ยงในภาพรวมมหาวิทยาลัย

การบริหารความเสี่ยงเป็นความรับผิดชอบร่วมกันของบุคลากรทุกระดับ โดยฝ่ายบริหารและเจ้าของความเสี่ยงรับผิดชอบต่อการระบุ ประเมิน จัดการ และติดตามความเสี่ยงในงานที่ตนกำกับ หน่วยบริหารความเสี่ยงสนับสนุนกรอบ มาตรฐาน เครื่องมือ ข้อมูล และคำปรึกษา ตลอดจนสอบทานและรายงานภาพรวม ส่วนกองตรวจสอบภายในให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรมตามหลัก Three Lines บุคลากรทุกคนมีส่วนร่วมด้วยการปฏิบัติตามการควบคุม รายงานเหตุการณ์และสัญญาณเตือนโดยสุจริต และนำบทเรียนมาปรับปรุงการทำงาน

คณะผู้จัดทำหวังว่าคู่มือฉบับนี้จะช่วยให้ทุกส่วนงานนำการบริหารความเสี่ยงไปใช้ในการบริหารงานประจำและการตัดสินใจได้อย่างเป็นรูปธรรม โดยประยุกต์ใช้ให้เหมาะสมกับภารกิจและระดับความเสี่ยง เพื่อสนับสนุนการบรรลุวัตถุประสงค์ของมหาวิทยาลัยด้วยความโปร่งใส มีธรรมาภิบาล พร้อมรับการเปลี่ยนแปลง และพัฒนาอย่างยั่งยืน

คณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน
มหาวิทยาลัยแม่โจ้
พ.ศ. 2570

สารบัญ

		หน้า
คำนำ		
สารบัญ		
ส่วนที่ 1 บทนำและความสำคัญของการบริหารความเสี่ยง		1
1.1	ความเป็นมาและความสำคัญ	1
1.2	วัตถุประสงค์ของคู่มือและการบริหารความเสี่ยง	3
1.3	ขอบเขตการใช้คู่มือ	4
1.4	ความหมายและองค์ประกอบที่ใช้ในการบริหารความเสี่ยง	5
1.5	ความสำคัญและประโยชน์ของการบริหารความเสี่ยง	7
1.6	หลักการบริหารความเสี่ยงตาม COSO ERM 2017	9
1.7	หลักการบริหารความเสี่ยงตาม ISO 31000:2018	11
1.8	ความเชื่อมโยงระหว่างธรรมาภิบาล การบริหารความเสี่ยง การควบคุมภายในและการให้ความเชื่อมั่น	12
1.9	กฎหมาย หลักเกณฑ์ และมาตรฐานอ้างอิง	15
1.10	คำจำกัดความและศัพท์เฉพาะ	17
ส่วนที่ 2 นโยบายและกรอบการบริหารความเสี่ยง		**26**
2.1	ถ้อยแถลงการกำกับดูแลความเสี่ยงของมหาวิทยาลัย	26
2.2	นโยบายการบริหารความเสี่ยงมหาวิทยาลัยแม่โจ้	27
2.3	นโยบายระดับความเสี่ยงที่ยอมรับได้	30
2.4	วิสัยทัศน์ด้านการบริหารความเสี่ยง	36
2.5	วัตถุประสงค์เชิงนโยบาย	37
2.6	โครงสร้างกรอบการบริหารความเสี่ยงที่มหาวิทยาลัยประยุกต์ใช้	38
2.7	การประยุกต์ใช้กรอบ COSO ERM 2017	40
2.8	การประยุกต์ใช้หลักการบริหารความเสี่ยงตาม ISO 31000:2018	43
2.9	ความเชื่อมโยงกับแผนยุทธศาสตร์มหาวิทยาลัย	44
2.10	ความเชื่อมโยงกับการควบคุมภายในและการให้ความเชื่อมั่น	45
2.11	ความเชื่อมโยงกับการพัฒนาองค์กรสู่ความเป็นเลิศ	47
2.12	ความเชื่อมโยงกับ ESG และการพัฒนาอย่างยั่งยืน	49
2.13	แนวปฏิบัติขั้นต่ำด้านการบริหารความเสี่ยง	50
2.14	วัฒนธรรมความเสี่ยงองค์กร	53

สารบัญ (ต่อ)

		หน้า
ส่วนที่ 3 โครงสร้างการกำกับดูแลและบทบาทหน้าที่ความรับผิดชอบ		56
3.1	หลักการกำกับดูแลการบริหารความเสี่ยง	56
3.2	โครงสร้างการกำกับดูแลการบริหารความเสี่ยง	57
3.3	บทบาท หน้าที่ และความรับผิดชอบ	61
3.4	การกำกับดูแลตามหลัก Three Lines	66
3.5	ตารางบทบาทและความรับผิดชอบด้านการบริหารความเสี่ยง	67
3.6	สายการรายงานและการยกระดับความเสี่ยง	70
3.7	หลักการความรับผิดชอบร่วมกัน	73
3.8	อำนาจการยอมรับความเสี่ยง	74
3.9	เกณฑ์การยกระดับความเสี่ยง	77
ส่วนที่ 4 กรอบและกระบวนการบริหารความเสี่ยง มหาวิทยาลัยแม่โจ้		81
4.1	หลักการของกรอบการบริหารความเสี่ยงองค์กร	81
4.2	วัตถุประสงค์ของกรอบการบริหารความเสี่ยง	84
4.3	องค์ประกอบของกรอบการบริหารความเสี่ยง	86
4.4	กระบวนการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้	93
4.5	ขั้นตอนที่ 1 การกำกับดูแลและกำหนดบริบท (Governance and Context Setting)	96
4.6	ขั้นตอนที่ 2 การกำหนดวัตถุประสงค์และเกณฑ์ความเสี่ยง (Objectives and Risk Criteria)	105
4.7	ขั้นตอนที่ 3 การระบุความเสี่ยง (Risk Identification)	115
4.8	ขั้นตอนที่ 4 การวิเคราะห์และประเมินความเสี่ยง (Risk Analysis and Evaluation)	133
4.9	ขั้นตอนที่ 5 การตอบสนองและจัดทำแผนบริหารความเสี่ยง (Risk Response and Treatment Planning)	146
4.10	ขั้นตอนที่ 6 การดำเนินการควบคุมและมาตรการ (Implement Controls and Risk Treatment Actions)	153
4.11	ขั้นตอนที่ 7 การสื่อสาร การรายงาน และการยกระดับ (Communication, Reporting and Escalation)	158
4.12	ขั้นตอนที่ 8 การติดตาม ทบทวน และปรับปรุงอย่างต่อเนื่อง (Monitoring, Review and Continual Improvement)	164

สารบัญ (ต่อ)

	หน้า
4.13 การควบคุมคุณภาพข้อมูลและเอกสารความเสี่ยง	171
4.14 ผลลัพธ์ของกรอบการบริหารความเสี่ยง	173
ส่วนที่ 5 การกำหนดระดับความเสี่ยงที่ยอมรับได้ ตัวชี้วัดความเสี่ยง และเกณฑ์การตัดสินใจ	177
5.1 หลักการและวัตถุประสงค์	177
5.2 คำศัพท์และความสัมพันธ์	178
5.3 หลักการกำหนดความสามารถในการรองรับความเสียง	179
5.4 ระดับความเสียงทียอมรับได้ของมหาวิทยาลัย (Risk Appetite)	180
5.5 การกำหนดระดับความบียงเบนที่ยอมรับได้ (Risk Tolerance)	183
5.6 การกำหนดและบริหารตัวชี้วัดความเสี่ยงสำคัญ (KRI)	185
5.7 สถานะตัวชี้วัด (KRI) และเกณฑ์การแจ้งเตือน	188
5.8 ความเชื่อมโยงระหว่างกรอบการยอมรับความเสี่ยงกับตารางประเมินระดับความเสี่ยง	189
5.9 เกณฑ์ที่ไม่ยอมรับและการยกระดับเป็นกรณีพิเศษ	190
5.10 อำนาจการยอมรับความเสี่ยง	192
5.11 การรายงานและยกระดับความเสี่ยง	193
5.12 การทบทวนและอนุมัติเกณฑ์	194
เอกสารอ้างอิง	197
ภาคผนวก	200
แบบฟอร์มประเมินและวิเคราะห์ความเสี่ยง แบบ Risk-MJU01	201
คำอธิบายแบบวิเคราะห์และประเมินความเสี่ยง	210
แบบฟอร์มจัดทำแผนบริหารความเสี่ยง (มจ-ส-01)	215
คำอธิบายแบบฟอร์มแผนบริหารความเสี่ยง (มจ-ส-01)	218
แบบฟอร์มรายงานผลตามแผนบริหารความเสี่ยง (มจ-ส-02)	220
สรุปรายงานผลการดำเนินงานการบริหารความเสี่ยง	221
คำอธิบายแบบฟอร์มรายงานผลความก้าวหน้าการบริหารความเสี่ยง	226

สารบัญภาพ

		หน้า
ภาพที่ 3-1	โครงสร้างการกำกับดูแลการบริหารความเสี่ยง มหาวิทยาลัยแม่โจ้ (MJU–RM Structure)	60
ภาพที่ 4-1	กรอบการบริหารความเสี่ยงองค์กร มหาวิทยาลัยแม่โจ้ (MJU Enterprise Risk Management Framework)	84
ภาพที่ 4-2	กระบวนการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้ 8 ขั้นตอน (MJU 8-Step Risk Management Process)	95
ภาพที่ 4-2	เกณฑ์ระดับความเสี่ยง การตอบสนอง และอำนาจการตัดสินใจ	141
ภาพที่ 4-2	ตารางประเมินระดับความเสี่ยงแบบ 5 X 5	142

สารบัญตาราง

		หน้า
ตารางที่ 1-1	ตารางความแตกต่างระหว่างความเสี่ยงและปัญหาหรือเหตุการณ์ที่เกิดขึ้นแล้ว (Issue/Event)	7
ตารางที่ 2-1	ตารางแสดงระดับความเสี่ยงที่ยอมรับได้ของมหาวิทยาลัย จำแนกตามมิติ	33
ตารางที่ 2-2	ตารางแสดงกรอบอ้างอิงและการประยุกต์ใช้ในระบบบริหารความเสี่ยงของมหาวิทยาลัย	39
ตารางที่ 2-3	ตารางแสดงหลักการ ISO 31000:2018 และแนวทางการประยุกต์ใช้ของมหาวิทยาลัย	43
ตารางที่ 2-4	ตารางแสดงความเชื่อมโยงการบริหารความเสี่ยงกับการพัฒนาองค์กรตามเกณฑ์คุณภาพการศึกษาเพื่อการดำเนินการที่เป็นเลิศ	48
ตารางที่ 2-5	ตารางแสดงมิติ ESG และประเด็นที่ควรพิจารณาในการบริหารความเสี่ยง	49
ตารางที่ 3-1	ตารางแสดงกลุ่มบทบาท องค์ประกอบ และหน้าที่หลักในการกำกับดูแลความเสี่ยง	58
ตารางที่ 3-2	ตารางแสดงบทบาท ผู้เกี่ยวข้อง ความรับผิดชอบหลัก และขอบเขตที่ต้องระวัง	66
ตารางที่ 3-3	ตารางบทบาทและความรับผิดชอบด้านการบริหารความเสี่ยง	68
ตารางที่ 3-4	ตารางแสดงเกณฑ์กลางการรายงานและการยกระดับความเสี่ยง	71
ตารางที่ 3-5	ตารางแสดงข้อเสนอกรอบอำนาจการยอมรับความเสี่ยงและเงื่อนไขขั้นต่ำ	75
ตารางที่ 4-1	ตารางแสดงองค์ประกอบของกรอบการบริหารความเสี่ยงองค์กรมหาวิทยาลัยแม่โจ้	87
ตารางที่ 4-2	ตารางแสดงกระบวนการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้ 8 ขั้นตอน	93
ตารางที่ 4-3	ตารางแสดงองค์ประกอบที่ต้องกำหนดสำหรับการประเมินและจัดการความเสี่ยง	106
ตารางที่ 4-4	ตารางแสดงประเภทความเสี่ยง ขอบเขต และตัวอย่าง	120
ตารางที่ 4-5	ตัวอย่างทะเบียนความเสี่ยงด้านการใช้ปัญญาประดิษฐ์และเทคโนโลยีดิจิทัล	130
ตารางที่ 4-6	ตารางแสดงแนวทางการประเมินโอกาสเกิด	135
ตารางที่ 4-7	ตารางแสดงคำอธิบายกลางสำหรับการประเมินผลกระทบ	137
ตารางที่ 4-8	ตารางแสดงเกณฑ์สรุปผลการประเมินการควบคุม	140
ตารางที่ 4-9	ตารางแสดงเกณฑ์ระดับความเสี่ยงและแนวทางดำเนินการ	141

สารบัญตาราง (ต่อ)

		หน้า
ตารางที่ 4-10	ตัวอย่างการประเมินความเสี่ยงด้านยุทธศาสตร์เกี่ยวกับ AI และดิจิทัล	143
ตารางที่ 4-11	ตารางแสดงทางเลือกการตอบสนองต่อความเสี่ยง	146
ตารางที่ 4-12	ข้อมูลสรุปแผนบริหารความเสี่ยงตัวอย่าง	149
ตารางที่ 4-13	มาตรการและหลักฐานในแผนตัวอย่าง	150
ตารางที่ 4-14	ตัวอย่างการควบคุม เจ้าของ หลักฐาน และเกณฑ์ยืนยันผล	155
ตารางที่ 4-15	สรุประยะเวลาการรายงานและการติดตามความเสี่ยง	162
ตารางที่ 4-16	ความถี่ขั้นต่ำในการติดตามตามระดับความเสี่ยงคงเหลือ	165
ตารางที่ 4-17	เกณฑ์การควบคุมคุณภาพข้อมูลและเอกสารความเสี่ยง	171
ตารางที่ 4-18	ผลลัพธ์ที่คาดหวังของกรอบการบริหารความเสี่ยง	174
ตารางที่ 5-1	คำศัพท์และความหมายในการใช้งาน	178
ตารางที่ 5-2	ระดับ RA และความหมาย	181
ตารางที่ 5-3	กรอบเสนอระดับความเสี่ยงที่ยอมรับได้	181
ตารางที่ 5-4	สถานะ KRI และการดำเนินการขั้นต่ำ	188
ตารางที่ 5-5	เกณฑ์ระดับความเสี่ยงตามคะแนนโอกาสเกิด × ผลกระทบ	190
ตารางที่ 5-6	กรอบอำนาจยอมรับความเสี่ยงคงเหลือ	192
ตารางที่ 5-7	สรุปกำหนดเวลารายงานและการติดตาม	193

ส่วนที่ 1
บทนำและความสำคัญของการบริหารความเสี่ยง

1.1 ความเป็นมาและความสำคัญ

สถาบันอุดมศึกษาดำเนินงานท่ามกลางสภาพแวดล้อมที่เปลี่ยนแปลงอย่างรวดเร็ว มีความเชื่อมโยงซับซ้อน และมีความไม่แน่นอนเพิ่มขึ้น ทั้งการเปลี่ยนแปลงโครงสร้างประชากรและจำนวนผู้เรียน ความต้องการของผู้เรียนและตลาดแรงงาน การแข่งขันด้านการศึกษา การวิจัยและนวัตกรรม ความก้าวหน้าของปัญญาประดิษฐ์และเทคโนโลยีดิจิทัล ความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนความยั่งยืนทางการเงิน การเปลี่ยนแปลงสภาพภูมิอากาศ ความปลอดภัย และความคาดหวังด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (Environmental, Social and Governance: ESG) รวมถึงกฎหมาย นโยบาย และมาตรฐานการกำกับดูแล ปัจจัยเหล่านี้ก่อให้เกิดทั้งความเสี่ยงและโอกาสที่ส่งผลต่อการบรรลุพันธกิจ เป้าประสงค์ และความยั่งยืนในระยะยาวของมหาวิทยาลัย

มหาวิทยาลัยแม่โจ้ได้วางรากฐานการบริหารความเสี่ยงผ่านนโยบายและแนวทางปฏิบัติ เพื่อให้ทุกส่วนงานดำเนินงานภายใต้กรอบที่สอดคล้องกัน เมื่อบริบท ยุทธศาสตร์ รูปแบบการดำเนินงาน และความคาดหวังของผู้มีส่วนได้ส่วนเสียเปลี่ยนแปลง มหาวิทยาลัยจึงทบทวนและปรับปรุงคู่มือการบริหารความเสี่ยงองค์กร พ.ศ. 2570 ให้ครอบคลุมการกำกับดูแล การบริหาร และการตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเชิงประจักษ์ ควบคู่กับการควบคุมความเสียหายและการติดตามรายงานผล

การบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM) เป็นกลไกสนับสนุนให้สภามหาวิทยาลัยและฝ่ายบริหารกำหนดทิศทางและยุทธศาสตร์ พิจารณานโยบายและโครงการ จัดลำดับความสำคัญ จัดสรรทรัพยากร และติดตามผลการดำเนินงานภายใต้ความไม่แน่นอนได้อย่างเหมาะสม โดยพิจารณาความเสี่ยงที่เชื่อมโยงกับวัตถุประสงค์และผลลัพธ์ที่ต้องการ ตลอดจนความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัวของความเสี่ยงในภาพรวมของมหาวิทยาลัย

การบริหารความเสี่ยงครอบคลุมการป้องกันและลดความสูญเสีย การใช้ประโยชน์จากโอกาสและการสร้าง รักษา และเพิ่มคุณค่า รวมถึงการคุ้มครองชื่อเสียง ความเชื่อมั่น ความปลอดภัย และความยั่งยืนของมหาวิทยาลัย การตัดสินใจจึงต้องใช้ข้อมูลที่ถูกต้อง ครบถ้วน ทันเวลา และเหมาะสมกับระดับการตัดสินใจ ตามแนวทางการตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเป็นฐาน (Risk-informed and Data-driven Decision-making) พร้อมทบทวนสมมติฐาน ติดตามปัจจัยขับเคลื่อนความเสี่ยง ความเสี่ยงเกิดใหม่ และแนวโน้มการเปลี่ยนแปลงอย่างต่อเนื่อง

เพื่อให้การบริหารความเสี่ยงนำไปสู่การปฏิบัติ ระบบต้องเชื่อมโยงระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้ (Risk Appetite: RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) กับตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators: KRI) สัญญาณเตือนล่วงหน้า (Early Warning Signals: EWS) และเกณฑ์การตอบสนองและการยกระดับรายงาน โดยกำหนดผู้รับผิดชอบ อำนาจตัดสินใจ และระยะเวลาดำเนินการให้ชัดเจน เพื่อให้มหาวิทยาลัยเตรียมการและดำเนินมาตรการได้ก่อนเกิดผลกระทบอย่างมีนัยสำคัญ รวมทั้งตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างทันท่วงที

มหาวิทยาลัยบูรณาการการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ (Governance, Risk and Compliance: GRC) เข้ากับการควบคุมภายใน การบริหารความต่อเนื่องขององค์กร (Business Continuity Management: BCM) แผนความต่อเนื่องในการดำเนินงาน (Business Continuity Plan: BCP) และการเสริมสร้างความยืดหยุ่นขององค์กร (Organizational Resilience) โดยจัดบทบาทตามหลัก Three Lines ให้ฝ่ายบริหารและผู้ปฏิบัติงานรับผิดชอบการบริหารความเสี่ยง หน่วยงานในสายที่สองสนับสนุน ติดตาม และสอบทาน และกองตรวจสอบภายในให้ความเชื่อมั่นอย่างเป็นอิสระ ทั้งนี้ ต้องประสานข้อมูลและการทำงานร่วมกันโดยรักษาขอบเขตความรับผิดชอบและความเป็นอิสระของการตรวจสอบภายใน

คู่มือฉบับนี้กำหนดประเภทความเสี่ยงหลัก 5 ประเภท ได้แก่ ด้านยุทธศาสตร์ (Strategic Risk: S) ด้านการดำเนินงาน (Operational Risk: O) ด้านการเงิน (Financial Risk: F) ด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (Compliance and Governance Risk: C) และด้านเทคโนโลยีดิจิทัล (Digital Technology Risk: D) โดยจำแนกประเภทหลักจากสาเหตุและวัตถุประสงค์ที่ได้รับผลกระทบ เพื่อสนับสนุนการกำหนดเจ้าของความเสี่ยงและสายการรายงาน พร้อมระบุประเภทที่เกี่ยวข้องและพิจารณาความสัมพันธ์ข้ามประเภทควบคู่กัน ส่วนชื่อเสียงและความเชื่อมั่น ความปลอดภัย ความต่อเนื่อง สิ่งแวดล้อม สังคม และธรรมาภิบาล ตลอดจนคุณภาพการศึกษา การวิจัยและบริการวิชาการ ให้พิจารณาเป็นมิติผลกระทบร่วมตามลักษณะของความเสี่ยงแต่ละประเด็น

คู่มือการบริหารความเสี่ยงองค์กร พ.ศ. 2570 จึงเป็นกรอบกลางสำหรับเชื่อมโยงวัตถุประสงค์ ยุทธศาสตร์ ความเสี่ยง การควบคุม มาตรการ ตัวชี้วัด และหลักฐานผลการดำเนินงาน เพื่อให้ทุกส่วนงานใช้หลักเกณฑ์และข้อมูลที่สอดคล้องกัน สามารถตรวจสอบย้อนกลับและรายงานประเด็นที่ต้องตัดสินใจได้อย่างทันเวลา สนับสนุนให้มหาวิทยาลัยดำเนินพันธกิจได้อย่างต่อเนื่อง บรรลุเป้าประสงค์ และสร้างคุณค่าอย่างยั่งยืน

1.2 วัตถุประสงค์ของคู่มือและการบริหารความเสี่ยง

คู่มือฉบับนี้จัดทำขึ้นเพื่อเป็นกรอบกลางในการบริหารความเสี่ยงองค์กรของมหาวิทยาลัยแม่โจ้ ให้เชื่อมโยงกับการกำกับดูแล ยุทธศาสตร์ และผลการดำเนินงาน รวมทั้งสนับสนุนให้ทุกส่วนงานนำไปปฏิบัติได้อย่างสอดคล้องกัน โดยมีวัตถุประสงค์ดังต่อไปนี้

1. กำหนดมาตรฐานร่วมในการบริหารความเสี่ยง กำหนดหลักการ กระบวนการ เกณฑ์การประเมิน เครื่องมือ แบบฟอร์ม แบบรายงาน และคำศัพท์ให้ชัดเจนและสอดคล้องกันทั่วทั้งมหาวิทยาลัย โดยเปิดให้ส่วนงานกำหนดรายละเอียดที่เหมาะสมกับภารกิจภายใต้กรอบกลางที่ได้รับอนุมัติ

2. เชื่อมโยงความเสี่ยงและโอกาสกับยุทธศาสตร์และผลการดำเนินงาน บูรณาการการบริหารความเสี่ยงและโอกาสเข้ากับวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ เป้าประสงค์ ตัวชี้วัด แผนงานโครงการ การลงทุน และการจัดสรรทรัพยากร เพื่อสนับสนุนการบรรลุวัตถุประสงค์และการสร้างคุณค่าของมหาวิทยาลัย

3. สนับสนุนการตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเป็นฐาน จัดให้สภามหาวิทยาลัย คณะกรรมการที่เกี่ยวข้อง และฝ่ายบริหารได้รับข้อมูลความเสี่ยงและโอกาสที่ถูกต้อง ครบถ้วน เชื่อถือได้ ทันเวลา และตรวจสอบย้อนกลับได้ โดยแสดงสมมติฐานและข้อจำกัดของข้อมูลเพื่อประกอบการกำหนดนโยบาย พิจารณาโครงการ จัดลำดับความสำคัญ และจัดสรรทรัพยากร

4. กำหนดแนวทางการยอมรับความเสี่ยงและการตัดสินใจภายในขอบเขตอำนาจ วางแนวทางกำหนดความสามารถในการรองรับความเสี่ยง (Risk Capacity) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) รวมทั้งเกณฑ์การตอบสนอง การยกระดับรายงาน และการยอมรับความเสี่ยงตามอำนาจที่ได้รับมอบหมาย โดยคำนึงถึงข้อกำหนดทางกฎหมายและเหตุการณ์ที่มหาวิทยาลัยไม่ยอมรับ

5. พัฒนาการบริหารความเสี่ยงเชิงรุกและการติดตามผลที่ตรวจสอบได้ สนับสนุนให้ทุกส่วนงานกำหนดบริบทและวัตถุประสงค์ ระบุ วิเคราะห์ ประเมิน ตอบสนอง ติดตาม ทบทวน และรายงานความเสี่ยงอย่างเป็นระบบ โดยใช้ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators: KRI) สัญญาณเตือนล่วงหน้า (Early Warning Signals: EWS) และหลักฐานผลการดำเนินมาตรการ พร้อมติดตามความเสี่ยงเกิดใหม่และความสัมพันธ์ระหว่างความเสี่ยง

6. กำหนดบทบาทและความรับผิดชอบให้ชัดเจน กำหนดบทบาทของสภามหาวิทยาลัย คณะกรรมการ ฝ่ายบริหาร ส่วนงาน เจ้าของความเสี่ยง เจ้าของการควบคุม เจ้าของมาตรการ เจ้าของข้อมูล และผู้ประสานงาน รวมทั้งเส้นทางการรายงานให้สอดคล้องกับหลัก Three Lines และคำสั่งมอบหมายอำนาจหน้าที่ที่มีผลใช้บังคับ

7. เชื่อมโยงความเสี่ยง การควบคุม และการให้ความเชื่อมั่น เชื่อมโยงข้อมูลการบริหารความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ และผลการตรวจสอบตามแนวคิดความเสี่ยง–

การควบคุม–การให้ความเชื่อมั่น (Risk–Control–Assurance) เพื่อระบุช่องว่าง ลดความซ้ำซ้อน และประเมินประสิทธิผลของการควบคุม โดยรักษาความเป็นอิสระของการตรวจสอบภายใน

8. เสริมสร้างความพร้อม ความต่อเนื่อง และความยืดหยุ่นขององค์กร พัฒนาความสามารถในการเตรียมพร้อม ตอบสนอง และฟื้นตัวจากเหตุฉุกเฉิน ภาวะวิกฤต และเหตุหยุดชะงัก โดยเชื่อมโยงการบริหารความเสี่ยงกับการบริหารความต่อเนื่องขององค์กร (Business Continuity Management: BCM) และแผนความต่อเนื่องในการดำเนินงาน (Business Continuity Plan: BCP) พร้อมคำนึงถึงความปลอดภัย ชื่อเสียง และมิติสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG)

9. ส่งเสริมวัฒนธรรมความเสี่ยงและการปรับปรุงอย่างต่อเนื่องสร้างความตระหนัก ความโปร่งใส ความรับผิดชอบ และการมีส่วนร่วมของบุคลากร ส่งเสริมการรายงานข้อกังวลและเหตุการณ์อย่างทันเวลา พัฒนาความรู้และทักษะตามบทบาท และนำผลการประเมิน ข้อค้นพบจากการตรวจสอบ และบทเรียนจากการดำเนินงานมาปรับปรุงระบบอย่างต่อเนื่อง

10. สนับสนุนความคุ้มค่า ความเชื่อมั่น และความยั่งยืนของมหาวิทยาลัย สนับสนุนการใช้ทรัพยากรอย่างคุ้มค่า การใช้ประโยชน์จากโอกาส และการสร้าง รักษา และเพิ่มคุณค่า ควบคู่กับการคุ้มครองผู้มีส่วนได้ส่วนเสีย เพื่อให้มหาวิทยาลัยดำเนินพันธกิจและบรรลุเป้าประสงค์ภายใต้ระดับความเสี่ยงที่ยอมรับได้

1.3 ขอบเขตการใช้คู่มือ

คู่มือฉบับนี้ใช้เป็นกรอบกลางสำหรับการบริหารความเสี่ยงองค์กรของมหาวิทยาลัยแม่โจ้ ครอบคลุมสภามหาวิทยาลัย คณะกรรมการที่เกี่ยวข้อง ผู้บริหาร ส่วนงาน หน่วยงาน และบุคลากรทุกระดับ ตามโครงสร้าง อำนาจหน้าที่ และความรับผิดชอบที่มีผลใช้บังคับ โดยครอบคลุมการดำเนินงานในทุกพื้นที่จัดการศึกษาของมหาวิทยาลัยและส่วนงานหรือหน่วยงานดังต่อไปนี้

1. สำนักงานสภามหาวิทยาลัย
2. สำนักงานมหาวิทยาลัย
3. คณะและวิทยาลัย
4. สำนักหรือส่วนงานที่มีฐานะเทียบเท่า
5. หน่วยงานวิสาหกิจและหน่วยงานสนับสนุนอื่นตามโครงสร้างของมหาวิทยาลัย

ขอบเขตการบริหารความเสี่ยงครอบคลุมการกำหนดยุทธศาสตร์ การจัดทำแผนและงบประมาณ การดำเนินพันธกิจด้านการศึกษา การวิจัย การบริการวิชาการ และการทำนุบำรุงศิลปวัฒนธรรม ตลอดจนกระบวนการสนับสนุน โครงการ การลงทุน ระบบข้อมูลและเทคโนโลยี และการดำเนินงานอื่นที่อาจส่งผลต่อการบรรลุวัตถุประสงค์ของมหาวิทยาลัย โดยพิจารณาความเสี่ยงและโอกาสทั้งระดับมหาวิทยาลัย ระดับส่วนงาน และระดับกระบวนการหรือโครงการ รวมทั้งความสัมพันธ์และผลกระทบร่วมระหว่างระดับ

สำหรับการดำเนินงานที่เกี่ยวข้องกับผู้รับจ้าง ผู้ให้บริการ พันธมิตร และบุคคลภายนอก ให้ส่วนงานผู้รับผิดชอบใช้คู่มือนี้เป็นแนวทางในการประเมินและกำกับความเสี่ยง โดยกำหนดหน้าที่ มาตรการควบคุม การรายงานเหตุการณ์ และการติดตามผลผ่านสัญญา ข้อตกลง หรือกลไกการกำกับดูแลที่เหมาะสมกับลักษณะงานและระดับความเสี่ยง

การนำคู่มือไปใช้ให้ยึดหลักความเหมาะสมตามสัดส่วน (Proportionality) โดยคำนึงถึงภารกิจ ขนาด ความซับซ้อน บริบท ผู้มีส่วนได้ส่วนเสีย และระดับความเสี่ยงของแต่ละส่วนงาน ส่วนงานสามารถกำหนดรายละเอียดวิธีปฏิบัติและเครื่องมือเพิ่มเติมให้เหมาะสมกับการดำเนินงาน โดยต้องสอดคล้องกับกรอบกลางและเกณฑ์ที่มหาวิทยาลัยอนุมัติ และไม่ลดทอนข้อกำหนดขั้นต่ำหรือหน้าที่ความรับผิดชอบตามกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง และนโยบายที่เกี่ยวข้อง

การใช้คู่มือให้ดำเนินการควบคู่กับนโยบาย แผนบริหารความเสี่ยง คำสั่งมอบหมายอำนาจหน้าที่ และแนวปฏิบัติเฉพาะด้านที่เกี่ยวข้อง หากพบข้อความที่ไม่สอดคล้องกัน ให้ส่วนงานแจ้งงานบริหารความเสี่ยงและการควบคุมภายใน กองพัฒนาคุณภาพ เพื่อประสานการตรวจสอบและเสนอปรับปรุง โดยระหว่างการพิจารณาให้ยึดถือข้อกำหนดที่มีผลใช้บังคับตามลำดับศักดิ์และขอบเขตอำนาจของแต่ละเรื่อง

1.4 ความหมายและองค์ประกอบที่ใช้ในการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง ผลกระทบของความไม่แน่นอนต่อวัตถุประสงค์ ซึ่งอาจทำให้ผลการดำเนินงานเบี่ยงเบนจากผลลัพธ์ที่คาดหวังทั้งด้านลบและด้านบวก การระบุความเสี่ยงจึงต้องเชื่อมโยงกับวัตถุประสงค์ ยุทธศาสตร์ เป้าประสงค์ หรือผลลัพธ์ที่ต้องการบรรลุอย่างชัดเจน และอธิบายความไม่แน่นอนที่สามารถนำไปวิเคราะห์ ประเมิน กำหนดผู้รับผิดชอบ และเลือกแนวทางจัดการได้

ปัญหาหรือเหตุการณ์ที่เกิดขึ้นแล้วสามารถใช้เป็นข้อมูลประกอบการระบุความเสี่ยงได้ โดยพิจารณาความไม่แน่นอนเกี่ยวกับการเกิดซ้ำ การขยายตัว หรือผลกระทบในอนาคต พร้อมแยกการจัดการเหตุการณ์ปัจจุบันออกจากการบริหารความเสี่ยงที่ยังคงเหลืออยู่

การเขียนข้อความความเสี่ยง (Risk Statement) ให้แสดงความสัมพันธ์ระหว่างสาเหตุ เหตุการณ์ และผลกระทบต่อวัตถุประสงค์ โดยใช้โครงสร้างดังนี้

"เนื่องจาก [สาเหตุหรือปัจจัยขับเคลื่อนความเสี่ยง] อาจเกิด [เหตุการณ์ความเสี่ยง] ส่งผลให้ [ผลกระทบต่อวัตถุประสงค์หรือผลลัพธ์ที่ต้องการบรรลุ]"

ข้อความความเสี่ยงควรกระชับ ชัดเจน และมีขอบเขตเพียงพอสำหรับการประเมิน โดยหลีกเลี่ยงการระบุเฉพาะสาเหตุ เช่น "บุคลากรขาดทักษะ" เฉพาะผลกระทบ เช่น "ชื่อเสียงเสียหาย" หรือเฉพาะการขาดกิจกรรม เช่น "ไม่มีการอบรม" โดยไม่อธิบายเหตุการณ์และผลต่อวัตถุประสงค์

องค์ประกอบสำคัญที่ใช้ในการระบุและวิเคราะห์ความเสี่ยง ประกอบด้วย

1. วัตถุประสงค์ (Objective) ผลลัพธ์ที่มหาวิทยาลัยหรือส่วนงานต้องการบรรลุภายในช่วงเวลาที่กำหนด ใช้เป็นจุดอ้างอิงในการระบุ ประเมิน และติดตามความเสี่ยง โดยเชื่อมโยงกับเป้าหมายและตัวชี้วัดผลการดำเนินงานที่เกี่ยวข้อง

2. สาเหตุหรือปัจจัยขับเคลื่อนความเสี่ยง (Cause/Risk Driver) ปัจจัย เงื่อนไข หรือการเปลี่ยนแปลงภายในและภายนอกที่อาจทำให้เกิดเหตุการณ์ความเสี่ยง หรือทำให้โอกาสเกิดและผลกระทบเปลี่ยนแปลง การวิเคราะห์ต้องพิจารณาสาเหตุที่แท้จริงเพื่อให้กำหนดมาตรการได้ตรงประเด็น

3. เหตุการณ์ความเสี่ยง (Risk Event) เหตุการณ์หรือสถานการณ์ที่อาจเกิดขึ้นและส่งผลต่อการบรรลุวัตถุประสงค์ โดยระบุให้ชัดว่าอาจเกิดอะไรขึ้น ในกระบวนการ ระบบ โครงการ หรือขอบเขตใด

4. ผลกระทบหรือผลสืบเนื่อง (Impact/Consequence) ผลที่อาจเกิดขึ้นจากเหตุการณ์ความเสี่ยงต่อวัตถุประสงค์และผู้มีส่วนได้ส่วนเสีย เช่น คุณภาพการศึกษา การวิจัย การดำเนินงาน การเงิน การปฏิบัติตามกฎหมาย ข้อมูลและเทคโนโลยี ชื่อเสียง ความปลอดภัย ความต่อเนื่อง และมิติ ESG ทั้งนี้ เหตุการณ์หนึ่งอาจก่อให้เกิดผลกระทบหลายมิติ

5. โอกาสเกิด (Likelihood) ความเป็นไปได้ที่เหตุการณ์ความเสี่ยงจะเกิดขึ้นภายในช่วงเวลาที่กำหนด ประเมินจากข้อมูลความน่าจะเป็น ความถี่ แนวโน้ม สภาพแวดล้อม หรือความเห็นของผู้เชี่ยวชาญตามเกณฑ์ที่มหาวิทยาลัยกำหนด พร้อมระบุหลักฐานและสมมติฐานที่ใช้

6. การควบคุมที่มีอยู่ (Existing Controls) นโยบาย กระบวนการ ระบบ หรือกิจกรรมที่มีอยู่ ณ วันที่ประเมิน ซึ่งมุ่งป้องกันหรือลดโอกาสเกิด ลดผลกระทบ ตรวจจับเหตุการณ์ หรือสนับสนุนการตอบสนองและฟื้นตัว โดยต้องตรวจสอบทั้งความเหมาะสมของการออกแบบ การนำไปใช้ และประสิทธิผลในการปฏิบัติงาน มาตรการที่ยังอยู่ระหว่างวางแผนให้บันทึกเป็นมาตรการเพิ่มเติม และไม่ใช้เป็นเหตุลดระดับความเสี่ยงคงเหลือปัจจุบัน

7. เจ้าของความเสี่ยง (Risk Owner) ผู้ได้รับมอบหมายให้รับผิดชอบการบริหาร ติดตาม และรายงานความเสี่ยง รวมทั้งประสานการดำเนินมาตรการและเสนอประเด็นเพื่อการตัดสินใจ โดยตัดสินใจภายในขอบเขตอำนาจที่ได้รับมอบหมาย และยกระดับรายงานเมื่อเกินอำนาจหรือเข้าเกณฑ์ที่กำหนด

8. กรอบเวลา (Time Horizon) ช่วงเวลาที่ใช้พิจารณาการเกิดเหตุการณ์และผลกระทบ เช่น ปีงบประมาณ ระยะเวลาโครงการ หรือระยะแผนยุทธศาสตร์ ซึ่งต้องระบุให้ชัดเจนเพื่อให้การประเมินโอกาสเกิด ผลกระทบ และความเร่งด่วนสอดคล้องกัน

ความไม่แน่นอนต่อวัตถุประสงค์สามารถพิจารณาได้สองมุมมอง ได้แก่

- **ภัยคุกคามหรือความเสี่ยงเชิงลบ (Threat)** ความไม่แน่นอนที่อาจก่อให้เกิดความสูญเสีย ความเสียหาย การหยุดชะงัก หรือทำให้ผลการดำเนินงานต่ำกว่าเป้าหมาย

- **โอกาส (Opportunity)** ความไม่แน่นอนที่อาจนำไปสู่ผลลัพธ์ที่ดีกว่าคาด การพัฒนานวัตกรรม การเพิ่มประสิทธิภาพ หรือการสร้างคุณค่า โดยการใช้ประโยชน์จากโอกาสต้องพิจารณาความเสี่ยงที่เกี่ยวข้อง ความคุ้มค่า ทรัพยากร และขอบเขตอำนาจ ควบคู่กับหลักธรรมาภิบาล กฎหมาย และระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้

ตารางที่ 1-1 ความแตกต่างระหว่างความเสี่ยงและปัญหาหรือเหตุการณ์ที่เกิดขึ้นแล้ว

ประเด็น	ความเสี่ยง (Risk)	ปัญหาหรือเหตุการณ์ที่เกิดขึ้นแล้ว (Issue/Incident)
สถานะ	ยังมีความไม่แน่นอนเกี่ยวกับการเกิดเหตุการณ์ การเกิดซ้ำ หรือผลกระทบในอนาคต	มีข้อเท็จจริงว่าปัญหาหรือเหตุการณ์เกิดขึ้นแล้วหรือกำลังเกิดขึ้น
แนวทางหลัก	ป้องกัน ลด เตรียมพร้อม ยอมรับภายในอำนาจ หรือใช้ประโยชน์จากโอกาส	ระงับเหตุ ควบคุมผลกระทบ แก้ไข เยียวยา และฟื้นฟูตามลักษณะเหตุการณ์
การประเมิน	ประเมินโอกาสเกิดและผลกระทบภายในกรอบเวลาที่กำหนด พร้อมพิจารณาการควบคุมและเกณฑ์ RA/RT	ประเมินผลกระทบที่เกิดขึ้นและที่อาจตามมา ความเร่งด่วน และทรัพยากรที่ต้องใช้
ลักษณะการบริหาร	มองไปข้างหน้า ติดตามการเปลี่ยนแปลง และเตรียมการเชิงรุก	ตอบสนองต่อข้อเท็จจริงและสถานการณ์ปัจจุบัน พร้อมป้องกันการขยายตัวและการเกิดซ้ำ
ความเชื่อมโยง	เหตุการณ์ที่ระบุไว้ในความเสี่ยงอาจเกิดขึ้นจริง แม้มีมาตรการควบคุม	ข้อมูลเหตุการณ์และผลการแก้ไขใช้ทบทวนความเสี่ยง การควบคุม และมาตรการเพิ่มเติม

เมื่อเกิดปัญหาหรือเหตุการณ์ ส่วนงานต้องดำเนินการตอบสนองและรายงานตามลักษณะ ความรุนแรง และความเร่งด่วนของสถานการณ์ โดยคุ้มครองชีวิต ความปลอดภัย ข้อมูล ทรัพย์สิน และความต่อเนื่องของพันธกิจตามความเหมาะสม พร้อมเก็บรักษาหลักฐาน วิเคราะห์สาเหตุราก และทบทวนทะเบียนความเสี่ยง ระดับความเสี่ยงคงเหลือ และประสิทธิผลของการควบคุม รวมทั้งนำบทเรียนมาปรับปรุงมาตรการและระบบเพื่อป้องกันการเกิดซ้ำ การตอบสนองเร่งด่วนต้องดำเนินการทันทีเมื่อเข้าเกณฑ์ โดยไม่รอให้การวิเคราะห์สาเหตุเสร็จสิ้น

1.5 ความสำคัญและประโยชน์ของการบริหารความเสี่ยง

การบริหารความเสี่ยงที่มีประสิทธิผลเป็นองค์ประกอบสำคัญของการกำกับดูแลและการบริหารมหาวิทยาลัย เมื่อบูรณาการเข้ากับการวางแผน การตัดสินใจ การดำเนินงาน และการติดตาม

ผล จะช่วยให้มหาวิทยาลัยจัดการความไม่แน่นอน ใช้ประโยชน์จากโอกาส และรักษาความต่อเนื่องของพันธกิจ โดยมีประโยชน์สำคัญดังต่อไปนี้

1. สนับสนุนการบรรลุยุทธศาสตร์และเป้าประสงค์ ช่วยให้มหาวิทยาลัยเข้าใจปัจจัยและความไม่แน่นอนที่อาจส่งผลต่อวิสัยทัศน์ พันธกิจ เป้าประสงค์ และตัวชี้วัดสำคัญ สามารถทบทวนสมมติฐาน พิจารณาทางเลือกเชิงยุทธศาสตร์ และปรับแผนให้เหมาะสมกับบริบทที่เปลี่ยนแปลง

2. ยกระดับคุณภาพการตัดสินใจ ช่วยให้สภามหาวิทยาลัย คณะกรรมการที่เกี่ยวข้อง และฝ่ายบริหารใช้ข้อมูลความเสี่ยงและโอกาสประกอบการเปรียบเทียบทางเลือก ผลประโยชน์ ต้นทุน ผลกระทบ และข้อจำกัด ก่อนกำหนดนโยบาย พิจารณาแผนงาน โครงการ หรือการลงทุน โดยคำนึงถึงระดับความเสี่ยงที่ยอมรับได้และขอบเขตอำนาจตัดสินใจ

3. เพิ่มประสิทธิภาพและความคุ้มค่าในการจัดสรรทรัพยากร ช่วยจัดลำดับความสำคัญและจัดสรรงบประมาณ บุคลากร เทคโนโลยี และทรัพยากรอื่นตามความสำคัญเชิงยุทธศาสตร์ ระดับความเสี่ยง และความเร่งด่วน รวมทั้งพิจารณาความคุ้มค่าของมาตรการและผลกระทบจากการไม่ดำเนินการ

4. เสริมสร้างธรรมาภิบาลและความรับผิดชอบ ทำให้เจ้าของความเสี่ยง ผู้รับผิดชอบการควบคุมและมาตรการ อำนาจในการยอมรับความเสี่ยง และเส้นทางการรายงานมีความชัดเจน สนับสนุนการตัดสินใจที่โปร่งใสและตรวจสอบย้อนกลับได้ โดยแบ่งบทบาทตามหลัก Three Lines และรักษาความเป็นอิสระของการตรวจสอบภายใน

5. พัฒนาการควบคุมภายในให้ตอบสนองต่อความเสี่ยง ช่วยระบุช่องว่างและความซ้ำซ้อนของการควบคุม เลือกมาตรการที่ตรงกับสาเหตุและผลกระทบ และลดภาระที่ไม่จำเป็น โดยประเมินความเหมาะสมของการออกแบบ การนำไปใช้ และประสิทธิผลในการปฏิบัติงานจากหลักฐานที่ตรวจสอบได้

6. ลดความสูญเสียและผลกระทบจากเหตุหยุดชะงัก เพิ่มความพร้อมในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นตัวจากเหตุฉุกเฉิน ภาวะวิกฤต เหตุการณ์ไซเบอร์ ภัยพิบัติ และเหตุหยุดชะงัก โดยเชื่อมโยงกับแผนความต่อเนื่องในการดำเนินงานและการทดสอบความพร้อม เพื่อคุ้มครองชีวิต ความปลอดภัย ข้อมูล ทรัพย์สิน และพันธกิจสำคัญ

7. ส่งเสริมวัฒนธรรมความเสี่ยงและการเรียนรู้ร่วมกัน สนับสนุนให้บุคลากรตระหนักถึงความเสี่ยงในงานของตน รายงานสัญญาณเตือน เหตุการณ์ ข้อผิดพลาด และข้อกังวลโดยสุจริตอย่างทันเวลา พร้อมนำบทเรียนและผลการวิเคราะห์สาเหตุมาปรับปรุงกระบวนการและป้องกันการเกิดซ้ำ

8. เพิ่มความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย ช่วยให้มหาวิทยาลัยแสดงความรับผิดชอบผ่านข้อมูลการบริหารความเสี่ยง ผลการดำเนินมาตรการ และการแก้ไขข้อบกพร่องที่ตรวจสอบได้ รวมทั้งสื่อสารอย่างเหมาะสมกับนักศึกษา บุคลากร หน่วยงานกำกับดูแล คู่ความร่วมมือ และสังคม

9. สนับสนุนคุณภาพและความเป็นเลิศขององค์กร เชื่อมโยงข้อมูลความเสี่ยง การควบคุม และผลการดำเนินงานเข้ากับการประกันคุณภาพ เกณฑ์คุณภาพการศึกษาเพื่อการดำเนินการที่เป็นเลิศ (EdPEx) และการให้ความเชื่อมั่น เพื่อใช้ระบุโอกาสในการปรับปรุงและติดตามผลลัพธ์ของการพัฒนาองค์กร

10. สร้าง รักษา และเพิ่มคุณค่าอย่างยั่งยืน ช่วยให้มหาวิทยาลัยปรับตัวต่อการเปลี่ยนแปลง ใช้ประโยชน์จากโอกาสและนวัตกรรมอย่างเหมาะสม รักษาความต่อเนื่องของพันธกิจ และคำนึงถึงผลกระทบด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG) เพื่อเสริมสร้างความยืดหยุ่นและความยั่งยืนในระยะยาว

1.6 หลักการบริหารความเสี่ยงตาม COSO ERM 2017

มหาวิทยาลัยแม่โจ้ประยุกต์ใช้กรอบ COSO Enterprise Risk Management—Integrating with Strategy and Performance (2017) เพื่อเชื่อมโยงการบริหารความเสี่ยงกับการกำหนดยุทธศาสตร์ วัตถุประสงค์ และผลการดำเนินงาน สนับสนุนการสร้าง รักษา และเพิ่มคุณค่า โดยกรอบดังกล่าวประกอบด้วย 5 องค์ประกอบและ 20 หลักการ ดังต่อไปนี้

1. การกำกับดูแลและวัฒนธรรมองค์กร (Governance and Culture) เป็นรากฐานของการบริหารความเสี่ยง โดยกำหนดบทบาทการกำกับดูแล โครงสร้างความรับผิดชอบ ค่านิยม และพฤติกรรมที่สนับสนุนการตัดสินใจอย่างเหมาะสม ประกอบด้วย 5 หลักการ ได้แก่

1) คณะกรรมการกำกับดูแลความเสี่ยง
2) จัดให้มีโครงสร้างการดำเนินงานที่เหมาะสม
3) กำหนดวัฒนธรรมองค์กรที่พึงประสงค์
4) แสดงความมุ่งมั่นต่อค่านิยมหลักขององค์กร
5) ดึงดูด พัฒนา และรักษาบุคลากรที่มีความสามารถ

มหาวิทยาลัยนำมาประยุกต์ใช้โดยกำหนดบทบาทของสภามหาวิทยาลัย คณะกรรมการ ฝ่ายบริหาร และส่วนงานให้ชัดเจน ส่งเสริมความรับผิดชอบของเจ้าของความเสี่ยง การรายงานข้อกังวลโดยสุจริต และการพัฒนาความรู้และทักษะตามบทบาท

2. ยุทธศาสตร์และการกำหนดวัตถุประสงค์ (Strategy and Objective-Setting) บูรณาการความเสี่ยงเข้ากับการวิเคราะห์บริบท การเลือกยุทธศาสตร์ และการกำหนดวัตถุประสงค์ โดยพิจารณาระดับความเสี่ยงที่องค์กรยอมรับได้ ประกอบด้วย 4 หลักการ ได้แก่

6) วิเคราะห์บริบทการดำเนินงาน
7) กำหนดระดับความเสี่ยงที่ยอมรับได้
8) ประเมินทางเลือกเชิงยุทธศาสตร์
9) กำหนดวัตถุประสงค์ขององค์กร

มหาวิทยาลัยนำมาประยุกต์ใช้โดยวิเคราะห์บริบทภายในและภายนอก พิจารณาความเสี่ยงและโอกาสของทางเลือกเชิงยุทธศาสตร์ และเชื่อมโยงวัตถุประสงค์ เป้าหมาย และตัวชี้วัดกับระดับความเสี่ยงที่ยอมรับได้ ก่อนตัดสินใจดำเนินแผนงาน โครงการ หรือการลงทุนสำคัญ

3. ผลการดำเนินงาน (Performance) ระบุและประเมินความเสี่ยงที่อาจส่งผลต่อการบรรลุวัตถุประสงค์ จัดลำดับความสำคัญ เลือกแนวทางตอบสนอง และพิจารณาความเสี่ยงในภาพรวม ประกอบด้วย 5 หลักการ ได้แก่

10) ระบุความเสี่ยง

11) ประเมินความรุนแรงของความเสี่ยง

12) จัดลำดับความสำคัญของความเสี่ยง

13) ดำเนินการตอบสนองต่อความเสี่ยง

14) พัฒนามุมมองความเสี่ยงในภาพรวมขององค์กร

มหาวิทยาลัยนำมาประยุกต์ใช้โดยระบุความเสี่ยงที่เชื่อมโยงกับวัตถุประสงค์ ประเมินโอกาสเกิดและผลกระทบโดยพิจารณาการควบคุมที่มีอยู่ จัดลำดับความสำคัญตามเกณฑ์ที่กำหนด และจัดทำมาตรการพร้อมผู้รับผิดชอบ ทรัพยากร กำหนดเวลา และหลักฐานผลการดำเนินงาน รวมทั้งวิเคราะห์ความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัวของความเสี่ยงระดับมหาวิทยาลัย

4. การทบทวนและปรับปรุง (Review and Revision) ทบทวนความเสี่ยงและผลการดำเนินงานเมื่อบริบทเปลี่ยนแปลง เพื่อปรับปรุงการบริหารความเสี่ยงให้เหมาะสมและมีประสิทธิผล ประกอบด้วย 3 หลักการ ได้แก่

15) ประเมินการเปลี่ยนแปลงที่มีนัยสำคัญ

16) ทบทวนความเสี่ยงและผลการดำเนินงาน

17) มุ่งปรับปรุงการบริหารความเสี่ยงองค์กร

มหาวิทยาลัยนำมาประยุกต์ใช้โดยติดตามการเปลี่ยนแปลงของยุทธศาสตร์ กฎหมาย เทคโนโลยี ทรัพยากร และผู้มีส่วนได้ส่วนเสีย ทบทวนผลการดำเนินงาน สถานะความเสี่ยง และประสิทธิผลของมาตรการ พร้อมนำเหตุการณ์ ข้อค้นพบจากการตรวจสอบ และบทเรียนมาปรับปรุงระบบอย่างต่อเนื่อง

5. สารสนเทศ การสื่อสาร และการรายงาน (Information, Communication, and Reporting) จัดให้มีข้อมูลและการสื่อสารที่สนับสนุนการบริหารความเสี่ยงและการตัดสินใจ รวมทั้งรายงานความเสี่ยง วัฒนธรรม และผลการดำเนินงานแก่ผู้เกี่ยวข้อง ประกอบด้วย 3 หลักการ ได้แก่

18) ใช้ประโยชน์จากสารสนเทศและเทคโนโลยี

19) สื่อสารข้อมูลความเสี่ยง

20) รายงานความเสี่ยง วัฒนธรรม และผลการดำเนินงาน

มหาวิทยาลัยนำมาประยุกต์ใช้โดยจัดให้มีข้อมูลที่ถูกต้อง ครบถ้วน ทันเวลา และตรวจสอบย้อนกลับได้ เชื่อมโยงทะเบียนความเสี่ยง ตัวชี้วัดความเสี่ยง สัญญาณเตือนล่วงหน้า และผลการดำเนินมาตรการ พร้อมกำหนดรูปแบบ ความถี่ ผู้รับรายงาน และเกณฑ์การยกระดับรายงานให้เหมาะสมกับความรุนแรงและอำนาจตัดสินใจ

องค์ประกอบทั้ง 5 และหลักการทั้ง 20 มีความเชื่อมโยงและสนับสนุนกัน มหาวิทยาลัยประยุกต์ใช้เป็นกรอบสำหรับออกแบบ ดำเนินงาน และทบทวนระบบบริหารความเสี่ยง โดยเชื่อมโยงกับหลักการ ISO 31000:2018 และกระบวนการปฏิบัติที่กำหนดไว้ในคู่มือ ทั้งนี้ การประเมินการประยุกต์ใช้ต้องพิจารณาการปฏิบัติจริงและหลักฐานผลลัพธ์ตามบริบทของมหาวิทยาลัย เพื่อให้การบริหารความเสี่ยงสนับสนุนยุทธศาสตร์และผลการดำเนินงานอย่างเป็นรูปธรรม

1.7 หลักการบริหารความเสี่ยงตาม ISO 31000:2018

มหาวิทยาลัยแม่โจ้ประยุกต์ใช้หลักการบริหารความเสี่ยงตามมาตรฐาน ISO 31000:2018 เพื่อสนับสนุนการสร้างและคุ้มครองคุณค่า การตัดสินใจ และการบรรลุวัตถุประสงค์ภายใต้ความไม่แน่นอน โดยนำหลักการสำคัญ 8 ประการมาใช้ในการออกแบบ ดำเนินงาน และปรับปรุงระบบบริหารความเสี่ยง ดังต่อไปนี้

1. บูรณาการ (Integrated) ให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการกำกับดูแลและกิจกรรมของมหาวิทยาลัยทุกระดับ ตั้งแต่การกำหนดยุทธศาสตร์ การวางแผนและงบประมาณ การดำเนินพันธกิจ การบริหารโครงการ การจัดสรรทรัพยากร จนถึงการติดตามผล โดยใช้ข้อมูลความเสี่ยงประกอบการตัดสินใจและการปฏิบัติงานอย่างต่อเนื่อง

2. มีโครงสร้างและครอบคลุม (Structured and Comprehensive) ใช้กรอบและกระบวนการที่เป็นระบบ มีคำศัพท์ เกณฑ์การประเมิน แบบฟอร์ม และแนวทางรายงานที่สอดคล้องกัน ครอบคลุมความเสี่ยงสำคัญและความสัมพันธ์ระหว่างความเสี่ยง เพื่อให้ผลการประเมินมีความสม่ำเสมอ สามารถเปรียบเทียบ ติดตาม และตรวจสอบย้อนกลับได้ โดยคำนึงถึงความแตกต่างของบริบทและสมมติฐานที่ใช้

3. เหมาะสมกับบริบท (Customized) ออกแบบและประยุกต์ใช้กรอบและกระบวนการให้เหมาะสมกับบริบทภายในและภายนอก วัตถุประสงค์ ภารกิจ ขนาด และความซับซ้อนของมหาวิทยาลัยและแต่ละส่วนงาน โดยยึดหลักความเหมาะสมตามสัดส่วน และรักษาความสอดคล้องกับกรอบกลางและข้อกำหนดที่เกี่ยวข้อง

4. มีส่วนร่วม (Inclusive) เปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องมีส่วนร่วมอย่างเหมาะสมและทันเวลา เพื่อให้ข้อมูล ความรู้ ประสบการณ์ และมุมมองที่หลากหลายได้รับการพิจารณาในการระบุ ประเมิน และจัดการความเสี่ยง รวมทั้งสร้างความเข้าใจเกี่ยวกับเหตุผลทางเลือก และผลกระทบของการตัดสินใจ

5. มีพลวัต (Dynamic) ติดตาม คาดการณ์ ตรวจจับ และตอบสนองต่อการเปลี่ยนแปลงของบริบทอย่างทันเวลา เนื่องจากความเสี่ยงอาจเกิดขึ้นใหม่ เปลี่ยนแปลง หรือหมดความสำคัญไป ให้ใช้ตัวชี้วัดความเสี่ยง สัญญาณเตือนล่วงหน้า และข้อมูลเหตุการณ์ประกอบการทบทวนทะเบียนความเสี่ยง การควบคุม และมาตรการ โดยทบทวนเมื่อเกิดการเปลี่ยนแปลงสำคัญควบคู่กับรอบรายงานปกติ

6. ใช้สารสนเทศที่ดีที่สุดเท่าที่มี (Best Available Information) ใช้ข้อมูลในอดีต ข้อมูลปัจจุบัน และการคาดการณ์ที่เกี่ยวข้อง รวมทั้งความเห็นของผู้เชี่ยวชาญตามความเหมาะสม โดยพิจารณาความถูกต้อง ความทันเวลา ความน่าเชื่อถือ และความเพียงพอของข้อมูล พร้อมเปิดเผยข้อจำกัด สมมติฐาน และความไม่แน่นอนที่อาจมีผลต่อการประเมินหรือการตัดสินใจ และจัดให้ผู้เกี่ยวข้องเข้าถึงข้อมูลได้ตามสิทธิและหน้าที่

7. คำนึงถึงปัจจัยมนุษย์และวัฒนธรรม (Human and Cultural Factors) พิจารณาค่านิยม ทัศนคติ พฤติกรรม ความรู้ ความสามารถ แรงจูงใจ อคติ และวัฒนธรรมองค์กร ซึ่งมีอิทธิพลต่อการรับรู้ การตัดสินใจ และการจัดการความเสี่ยง ส่งเสริมความรับผิดชอบตามบทบาท การสื่อสารอย่างเปิดเผย และการรายงานข้อกังวลหรือเหตุการณ์โดยสุจริต พร้อมพัฒนาทักษะที่จำเป็นต่อการบริหารความเสี่ยง

8. ปรับปรุงอย่างต่อเนื่อง (Continual Improvement) เรียนรู้จากผลการดำเนินงาน ประสบการณ์ เหตุการณ์ ข้อค้นพบจากการตรวจสอบ และการเปลี่ยนแปลงของบริบท เพื่อนำมาปรับปรุงกรอบ กระบวนการ เกณฑ์ เครื่องมือ ข้อมูล และความสามารถของบุคลากร โดยกำหนดผู้รับผิดชอบและติดตามผลการปรับปรุงว่าช่วยเพิ่มประสิทธิผลของการบริหารความเสี่ยงได้เพียงใด

หลักการทั้ง 8 ประการเป็นคุณลักษณะที่สนับสนุนการบริหารความเสี่ยงอย่างมีประสิทธิผล ให้มหาวิทยาลัยและส่วนงานประยุกต์ใช้ร่วมกันตลอดการกำกับดูแล การบริหาร และการตัดสินใจ โดยแยกให้ชัดเจนจากกระบวนการปฏิบัติ 8 ขั้นตอนที่กำหนดไว้ในคู่มือ ซึ่งเป็นแนวทางดำเนินงานภายใต้หลักการดังกล่าว

1.8 ความเชื่อมโยงระหว่างธรรมาภิบาล การบริหารความเสี่ยง การควบคุมภายใน และการให้ความเชื่อมั่น

ธรรมาภิบาล การบริหารความเสี่ยง การควบคุมภายใน และการให้ความเชื่อมั่นเป็นองค์ประกอบที่เชื่อมโยงกันของระบบกำกับดูแลมหาวิทยาลัย เพื่อสนับสนุนการบรรลุวัตถุประสงค์ ลดช่องว่างและความซ้ำซ้อน และทำให้ผู้กำกับดูแลและฝ่ายบริหารได้รับข้อมูลที่เพียงพอสำหรับการตัดสินใจ โดยมีสาระสำคัญดังนี้

1. ธรรมาภิบาล (Governance) ระบบและกระบวนการสำหรับกำหนดทิศทาง กำกับดูแล มอบหมายความรับผิดชอบ กำหนดอำนาจตัดสินใจ และติดตามผล เพื่อให้มหาวิทยาลัยดำเนินงานอย่างโปร่งใส รับผิดชอบ และคำนึงถึงผู้มีส่วนได้ส่วนเสีย

2. การบริหารความเสี่ยง (Risk Management) การดำเนินงานอย่างเป็นระบบเพื่อระบุ วิเคราะห์ ประเมิน ตอบสนอง ติดตาม ทบทวน และสื่อสารความเสี่ยงและโอกาสที่อาจส่งผลต่อวัตถุประสงค์ โดยเชื่อมโยงกับยุทธศาสตร์ ผลการดำเนินงาน และระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้

3. การควบคุมภายใน (Internal Control) กระบวนการที่ผู้กำกับดูแล ฝ่ายบริหาร และบุคลากรร่วมกันดำเนินการ ผ่านนโยบาย ระบบ และกิจกรรมควบคุม เพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลต่อการบรรลุวัตถุประสงค์ด้านการดำเนินงาน การรายงาน และการปฏิบัติตามกฎหมายและข้อกำหนด โดยต้องประเมินทั้งการออกแบบ การนำไปใช้ และประสิทธิผลในการปฏิบัติงาน

4. การให้ความเชื่อมั่น (Assurance) การประเมินหลักฐานอย่างเป็นระบบเพื่อให้ข้อสรุปต่อความเพียงพอและประสิทธิผลของการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายใน โดยระบุผู้ให้ความเชื่อมั่น ขอบเขต เกณฑ์ วิธีการ ข้อจำกัด และระดับความเป็นอิสระอย่างชัดเจน เพื่อให้ผู้ใช้ผลการประเมินเข้าใจและพิจารณาความน่าเชื่อถือได้อย่างเหมาะสม

การเชื่อมโยงองค์ประกอบดังกล่าวเริ่มจากการกำหนดวัตถุประสงค์ ระบุความเสี่ยงที่อาจกระทบต่อวัตถุประสงค์ ออกแบบและดำเนินการควบคุม ติดตามผลและประเมินหลักฐาน แล้วรายงานข้อค้นพบและประเด็นที่ต้องตัดสินใจต่อฝ่ายบริหารและผู้กำกับดูแล ผลการประเมินต้องนำกลับมาทบทวนความเสี่ยง การควบคุม และการดำเนินงานอย่างต่อเนื่อง

การจัดวางบทบาทตามหลัก Three Lines มหาวิทยาลัยประยุกต์ใช้หลัก Three Lines โดยพิจารณาจากลักษณะหน้าที่และความรับผิดชอบ ควบคู่กับโครงสร้างและคำสั่งที่มีผลใช้บังคับ ดังนี้

1. สภามหาวิทยาลัยและคณะกรรมการที่เกี่ยวข้อง (Governing Body) กำหนดทิศทางและความคาดหวังด้านธรรมาภิบาล พิจารณานโยบายและกรอบระดับความเสี่ยงที่ยอมรับได้ตามอำนาจหน้าที่ กำกับและติดตามฝ่ายบริหาร และรับข้อมูลความเสี่ยง การควบคุม และผลการให้ความเชื่อมั่นที่เพียงพอและทันเวลา รวมทั้งส่งเสริมความเป็นอิสระและการเข้าถึงผู้กำกับดูแลของกองตรวจสอบภายใน

2. บทบาทสายงานที่หนึ่ง (First Line Roles) ฝ่ายบริหาร ผู้บริหารส่วนงาน เจ้าของวัตถุประสงค์ เจ้าของกระบวนการ และเจ้าของความเสี่ยง รับผิดชอบการดำเนินงานและผลลัพธ์ในขอบเขตที่ได้รับมอบหมาย รวมทั้งระบุ ประเมิน จัดการ ติดตาม และรายงานความเสี่ยง ออกแบบ

และดำเนินการควบคุม และแก้ไขข้อบกพร่อง โดยตัดสินใจภายในอำนาจและยกระดับรายงานเมื่อเข้าเกณฑ์ที่กำหนด

3. บทบาทสายงานที่สอง (Second Line Roles) หน่วยงานหรือผู้รับผิดชอบด้านการบริหารความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ และการกำกับเฉพาะด้าน ทำหน้าที่พัฒนาหรือเสนอกรอบ มาตรฐาน และเครื่องมือ ให้คำปรึกษา สนับสนุน ติดตาม วิเคราะห์ และสอบทานข้อมูลกับสมมติฐานอย่างสร้างสรรค์ เพื่อสนับสนุนการตัดสินใจของฝ่ายบริหาร โดยไม่ทำให้เจ้าของความเสี่ยงพ้นจากความรับผิดชอบ ทั้งนี้ สายงานที่สองเป็นส่วนหนึ่งของฝ่ายบริหาร และอาจมีอำนาจตัดสินใจเฉพาะด้านตามที่ได้รับมอบหมาย

4. บทบาทสายงานที่สาม (Third Line Roles) กองตรวจสอบภายในให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรมต่อความเพียงพอและประสิทธิผลของธรรมาภิบาล การบริหารความเสี่ยง และการควบคุมภายใน ครอบคลุมการดำเนินงานของสายงานที่หนึ่งและสายงานที่สอง โดยรายงานตามกฎบัตรและโครงสร้างการกำกับดูแลที่มีผลใช้บังคับ และติดตามการแก้ไขข้อค้นพบโดยไม่รับผิดชอบดำเนินการแก้ไขแทนฝ่ายบริหาร

หน่วยงานหนึ่งอาจปฏิบัติทั้งบทบาทสายงานที่หนึ่งและสายงานที่สองในกิจกรรมต่างกัน เช่น การดำเนินระบบเทคโนโลยีเป็นบทบาทสายงานที่หนึ่ง ส่วนการกำหนดมาตรฐานและติดตามความมั่นคงปลอดภัยอาจเป็นบทบาทสายงานที่สอง จึงต้องกำหนดหน้าที่ ผู้รับผิดชอบ และแนวทางจัดการความขัดแย้งของบทบาทให้ชัดเจน

ผู้ให้ความเชื่อมั่นอื่น (Other Assurance Providers) ผู้สอบบัญชี ผู้ประเมินภายนอก หน่วยรับรอง หน่วยงานกำกับดูแล และผู้เชี่ยวชาญอิสระ อาจให้ความเชื่อมั่นเพิ่มเติมตามขอบเขตและอำนาจหน้าที่ของตน มหาวิทยาลัยควรประสานข้อมูล แผน และผลการประเมินตามความเหมาะสม เพื่อเพิ่มความครอบคลุมและลดความซ้ำซ้อน โดยพิจารณาความสามารถ ความเป็นอิสระ ความเที่ยงธรรม วิธีการ และข้อจำกัดก่อนใช้ผลการประเมินของผู้ให้ความเชื่อมั่นรายอื่น

มหาวิทยาลัยอาจจัดทำแผนผังการให้ความเชื่อมั่น (Assurance Map) เพื่อเชื่อมโยงความเสี่ยงสำคัญ การควบคุม ผู้รับผิดชอบ และแหล่งความเชื่อมั่น พร้อมระบุช่องว่างหรือความซ้ำซ้อนที่ต้องปรับปรุง โดยใช้ประกอบการวางแผนติดตามและการตรวจสอบตามบทบาทของแต่ละฝ่าย

การประสานงานและการรักษาความเป็นอิสระ ทุกฝ่ายต้องประสานงานและแลกเปลี่ยนข้อมูลอย่างเหมาะสม โดยรักษาความรับผิดชอบ อำนาจหน้าที่ และความเป็นอิสระตามบทบาท การประสานงานกับกองตรวจสอบภายในต้องไม่ทำให้กองตรวจสอบภายในรับผิดชอบตัดสินใจหรือดำเนินงานแทนฝ่ายบริหาร เช่น อนุมัติ RA/RT ยอมรับความเสี่ยง เป็นเจ้าของทะเบียนความเสี่ยงหรือเลือกและดำเนินมาตรการควบคุม หากได้รับมอบหมายภารกิจเพิ่มเติมที่อาจกระทบต่อความเป็นอิสระหรือความเที่ยงธรรม ให้เปิดเผยต่อผู้มีหน้าที่กำกับดูแลการตรวจสอบภายใน และพิจารณาความเหมาะสมตามกฎบัตรและมาตรฐานที่เกี่ยวข้องก่อนรับภารกิจ โดยกำหนดขอบเขต ระยะเวลา สาย

การรายงาน และมาตรการคุ้มครองให้ชัดเจน รวมทั้งจัดให้มีผู้ให้ความเชื่อมั่นที่เป็นอิสระสำหรับงานที่กองตรวจสอบภายในมีส่วนรับผิดชอบ ทั้งนี้ การอนุมัติภารกิจเพียงอย่างเดียวไม่ทดแทนมาตรการรักษาความเป็นอิสระและความเที่ยงธรรม

1.9 กฎหมาย หลักเกณฑ์ และมาตรฐานอ้างอิง

คู่มือฉบับนี้จัดทำขึ้นโดยคำนึงถึงกฎหมาย หลักเกณฑ์ และข้อกำหนดที่เกี่ยวข้องกับมหาวิทยาลัยแม่โจ้ พร้อมประยุกต์ใช้มาตรฐานและกรอบแนวปฏิบัติเพื่อพัฒนาระบบบริหารความเสี่ยง โดยจำแนกเอกสารอ้างอิงตามสถานะและวัตถุประสงค์การใช้งาน ดังนี้

1.9.1 กฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

ให้มหาวิทยาลัยและส่วนงานพิจารณาข้อกำหนดต่อไปนี้ตามขอบเขตการใช้บังคับ อำนาจหน้าที่ และลักษณะภารกิจของตน โดยใช้ฉบับที่มีผลใช้บังคับ รวมถึงบทแก้ไขเพิ่มเติมและข้อกำหนดที่ออกตามกฎหมายนั้น หากมี

1. พระราชบัญญัติมหาวิทยาลัยแม่โจ้ พ.ศ. 2560
2. พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561
3. พระราชบัญญัติการอุดมศึกษา พ.ศ. 2562
4. หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 ตามหนังสือกระทรวงการคลัง ที่ กค 0409.4/ว 23 ลงวันที่ 19 มีนาคม 2562
5. แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กร ตามหนังสือกระทรวงการคลัง ที่ กค 0409.3/ว 36 ลงวันที่ 3 กุมภาพันธ์ 2564หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561
6. หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 รวมถึงฉบับแก้ไขเพิ่มเติมที่มีผลใช้บังคับ
7. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
8. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
9. พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 รวมทั้งระเบียบประกาศ และข้อกำหนดที่เกี่ยวข้อง
10. พระราชบัญญัติมาตรฐานทางจริยธรรม พ.ศ. 2562 และกฎหมายหรือข้อกำหนดด้านการป้องกันการทุจริตและประพฤติมิชอบที่เกี่ยวข้อง
11. กฎหมาย กฎกระทรวง ประกาศ และข้อกำหนดด้านมาตรฐานการอุดมศึกษา ธรรมาภิบาลของสถาบันอุดมศึกษา การวิจัย และจริยธรรมการวิจัย

12. กฎหมายและข้อกำหนดด้านความปลอดภัย อาชีวอนามัย สิ่งแวดล้อม การสาธารณสุข การป้องกันและบรรเทาสาธารณภัย และการจัดการภาวะฉุกเฉินที่เกี่ยวข้องกับภารกิจ

13. ข้อบังคับ ระเบียบ นโยบาย ประกาศ คำสั่ง และมติของสภามหาวิทยาลัยหรือมหาวิทยาลัยแม่โจ้ รวมทั้งกฎบัตรของคณะกรรมการและหน่วยงานที่เกี่ยวข้อง

1.9.2 มาตรฐานและกรอบแนวปฏิบัติที่นำมาประยุกต์ใช้

มหาวิทยาลัยนำมาตรฐานและกรอบแนวปฏิบัติต่อไปนี้มาประยุกต์ใช้ตามวัตถุประสงค์และบริบท โดยกำหนดขอบเขตการใช้ให้ชัดเจนและสอดคล้องกับข้อกำหนดของมหาวิทยาลัย

1. ISO 31000:2018, Risk management—Guidelines ใช้เป็นแนวทางด้านหลักการ กรอบ และกระบวนการบริหารความเสี่ยง เพื่อสนับสนุนการสร้างและคุ้มครองคุณค่าและการตัดสินใจภายใต้ความไม่แน่นอน

2. COSO, Enterprise Risk Management—Integrating with Strategy and Performance (2017) ใช้เชื่อมโยงการบริหารความเสี่ยงกับการกำหนดยุทธศาสตร์ วัตถุประสงค์ ผลการดำเนินงาน และมุมมองความเสี่ยงในภาพรวมของมหาวิทยาลัย

3. COSO, Internal Control—Integrated Framework (2013) ใช้ประกอบการออกแบบ ประเมิน และปรับปรุงการควบคุมภายใน โดยเชื่อมโยงกับวัตถุประสงค์ด้านการดำเนินงาน การรายงาน และการปฏิบัติตามข้อกำหนด

4. ISO 22301:2019, Security and resilience—Business continuity management systems—Requirements รวมถึง Amendment 1:2024 เรื่อง Climate action changes ใช้ประกอบการพัฒนาระบบบริหารความต่อเนื่องขององค์กรและแผนความต่อเนื่องในการดำเนินงาน (BCM/BCP) ตามขอบเขตที่มหาวิทยาลัยกำหนด

5. มาตรฐานการตรวจสอบภายในสากล (Global Internal Audit Standards) และกรอบมาตรฐานวิชาชีพการตรวจสอบภายในสากล (International Professional Practices Framework: IPPF) ใช้ประกอบการกำกับและพัฒนางานตรวจสอบภายในตามข้อกำหนดและกฎบัตรที่เกี่ยวข้อง โดย Global Internal Audit Standards ฉบับปี 2024 มีผลตั้งแต่วันที่ 9 มกราคม พ.ศ. 2568

6. หลัก Three Lines ของ The Institute of Internal Auditors (IIA) ใช้จัดวางบทบาทของผู้กำกับดูแล ฝ่ายบริหารในสายงานที่หนึ่งและสายงานที่สอง และการตรวจสอบภายในในสายงานที่สาม พร้อมประสานการให้ความเชื่อมั่นโดยรักษาความรับผิดชอบและความเป็นอิสระตามบทบาท

7. เป้าหมายการพัฒนาที่ยั่งยืน (Sustainable Development Goals: SDGs) และแนวคิดด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG) ใช้ประกอบการพิจารณาความเสี่ยง โอกาส และผลกระทบต่อผู้มีส่วนได้ส่วนเสียและความยั่งยืนตามทิศทางของมหาวิทยาลัย

8. เกณฑ์คุณภาพการศึกษาเพื่อการดำเนินการที่เป็นเลิศ (Education Criteria for Performance Excellence: EdPEx) ใช้เชื่อมโยงการบริหารความเสี่ยงกับการนำองค์กร การวางแผน การดำเนินงาน การเรียนรู้ และผลลัพธ์ โดยอ้างอิงฉบับที่มหาวิทยาลัยกำหนดใช้

1.10 คำจำกัดความและศัพท์เฉพาะ

คำจำกัดความในหัวข้อนี้ใช้เป็นมาตรฐานร่วมสำหรับการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้ โดยคำศัพท์ด้านบทบาท เครื่องมือ และเกณฑ์เฉพาะของมหาวิทยาลัยให้ใช้ตามขอบเขตที่กำหนดในคู่มือ หากกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานเฉพาะกำหนดความหมายไว้ ให้พิจารณาความหมายนั้นตามขอบเขตการใช้บังคับของแต่ละเรื่อง

1.10.1 หน่วยงาน บทบาท และผู้เกี่ยวข้อง

คำศัพท์	ความหมายที่ใช้ในคู่มือ
ผู้กำกับดูแล (Governing Body)	สภามหาวิทยาลัยแม่โจ้ ซึ่งกำหนดทิศทาง กำกับดูแล และติดตามความรับผิดชอบของฝ่ายบริหารตามอำนาจหน้าที่ โดยมีคณะกรรมการที่เกี่ยวข้องสนับสนุนตามข้อบังคับ คำสั่ง หรือมติที่มีผลใช้บังคับ
หัวหน้าหน่วยงานของรัฐ	อธิการบดีมหาวิทยาลัยแม่โจ้ สำหรับการดำเนินงานตามกฎหมายและหลักเกณฑ์ที่กำหนดบทบาทดังกล่าว
คณะกรรมการที่เกี่ยวข้อง (Relevant Committees)	คณะกรรมการที่ได้รับมอบหมายหน้าที่ด้านการบริหารความเสี่ยง การควบคุมภายใน การตรวจสอบ หรือการกำกับเฉพาะด้าน โดยมีอำนาจและความรับผิดชอบตามข้อบังคับ คำสั่ง กฎบัตร หรือมติที่เกี่ยวข้อง
ส่วนงานหรือหน่วยงาน (Organizational Unit)	ส่วนงานหรือหน่วยงานตามโครงสร้างของมหาวิทยาลัย โดยใช้สถานะและขอบเขตหน้าที่ตามข้อบังคับ ประกาศ หรือคำสั่งที่มีผลใช้บังคับ
เจ้าของวัตถุประสงค์ (Objective Owner)	ผู้ได้รับมอบหมายให้รับผิดชอบการบรรลุวัตถุประสงค์ เป้าหมาย ผลลัพธ์ หรือตัวชี้วัดที่กำหนด
เจ้าของความเสี่ยง (Risk Owner)	ผู้ได้รับมอบหมายให้รับผิดชอบการประเมิน จัดการ ติดตาม และรายงานความเสี่ยง รวมทั้งประสานผู้เกี่ยวข้อง ตัดสินใจภายในขอบเขตอำนาจ และเสนอการยอมรับหรือยกระดับรายงานตามเกณฑ์
เจ้าของการควบคุม (Control Owner)	ผู้รับผิดชอบการออกแบบหรือดูแลการควบคุมที่ได้รับมอบหมาย ให้มีการปฏิบัติอย่างต่อเนื่อง ติดตามประสิทธิผล แก้ไขข้อบกพร่อง และจัดเก็บหลักฐานที่ตรวจสอบได้
เจ้าของมาตรการ (Action Owner)	ผู้รับผิดชอบดำเนินมาตรการเพิ่มเติมตามแผนให้แล้วเสร็จ ส่งมอบผลผลิตและหลักฐานตามกำหนด และรายงานความก้าวหน้า ปัญหา และผลการดำเนินงาน
เจ้าของข้อมูล (Data Owner)	ผู้รับผิดชอบกำหนดนิยามและมาตรฐานข้อมูล ดูแลความถูกต้อง ครบถ้วน ทันเวลา และการเข้าถึงข้อมูลที่ใช้ประเมิน ติดตาม และรายงานความเสี่ยง โดยประสานผู้ดูแลระบบและผู้เกี่ยวข้องด้านความมั่นคงปลอดภัย

ผู้ประสานงานความเสี่ยง (Risk Coordinator)	ผู้สนับสนุนและประสานการจัดทำทะเบียนความเสี่ยง แผน การติดตามตัวชี้วัด การรวบรวมหลักฐาน และการรายงาน โดยไม่รับผิดชอบตัดสินใจแทนเจ้าของความเสี่ยง
ผู้ส่งเสริมการบริหารความเสี่ยง (Risk Champion)	ผู้ส่งเสริมความเข้าใจ การมีส่วนร่วม และการนำแนวทางบริหารความเสี่ยงไปใช้ในส่วนงาน ทั้งนี้ อาจเป็นบุคคลเดียวกับผู้ประสานงานตามที่ได้รับมอบหมาย

บุคคลหนึ่งอาจได้รับมอบหมายหลายบทบาทได้ตามความเหมาะสม แต่ต้องระบุหน้าที่ อำนาจ และความรับผิดชอบให้ชัดเจน รวมทั้งพิจารณาความขัดแย้งของบทบาทและการสอบทานที่จำเป็น

1.10.2 คำศัพท์พื้นฐานด้านการบริหารความเสี่ยง

คำศัพท์	ความหมายที่ใช้ในคู่มือ
การบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM)	วัฒนธรรม ความสามารถ และแนวปฏิบัติที่บูรณาการกับการกำหนดยุทธศาสตร์และการบริหารผลการดำเนินงาน เพื่อจัดการความเสี่ยงและโอกาสในการสร้าง รักษา และเพิ่มคุณค่า
ความเสี่ยง (Risk)	ผลกระทบของความไม่แน่นอนต่อวัตถุประสงค์ ซึ่งอาจทำให้ผลลัพธ์เบี่ยงเบนจากที่คาดหวังทั้งด้านลบและด้านบวก
โอกาส (Opportunity)	สถานการณ์หรือความเป็นไปได้ที่อาจนำไปสู่ผลลัพธ์ที่ดีกว่าคาด นวัตกรรม ประสิทธิภาพ หรือคุณค่าเพิ่ม โดยต้องพิจารณาความเสี่ยงและข้อจำกัดที่เกี่ยวข้องก่อนตัดสินใจใช้ประโยชน์
ข้อความความเสี่ยง (Risk Statement)	ข้อความที่เชื่อมโยงสาเหตุหรือปัจจัยขับเคลื่อน เหตุการณ์ที่อาจเกิดขึ้น และผลกระทบต่อวัตถุประสงค์ เพื่อให้สามารถประเมินและกำหนดแนวทางจัดการได้
สาเหตุหรือปัจจัยขับเคลื่อนความเสี่ยง (Cause/Risk Driver)	ปัจจัย เงื่อนไข หรือการเปลี่ยนแปลงภายในและภายนอกที่มีอิทธิพลต่อการเกิดเหตุการณ์หรือความรุนแรงของผลกระทบ
เหตุการณ์ความเสี่ยง (Risk Event)	เหตุการณ์หรือสถานการณ์ที่อาจเกิดขึ้นและส่งผลต่อวัตถุประสงค์ รวมถึงการเกิดซ้ำหรือการขยายตัวของเหตุการณ์ที่เคยเกิดขึ้นแล้ว
ปัญหา (Issue)	สภาพหรือข้อบกพร่องที่เกิดขึ้นแล้วหรือกำลังดำรงอยู่ และต้องได้รับการแก้ไข ควบคุม หรือติดตามจนได้ข้อยุติ
อุบัติการณ์หรือเหตุการณ์ที่เกิดขึ้นจริง (Incident)	เหตุการณ์ที่เกิดขึ้นแล้วและต้องได้รับการประเมิน ตอบสนอง และรายงานตามลักษณะและความรุนแรง รวมทั้งใช้เป็นข้อมูลทบทวนความเสี่ยง
เหตุการณ์เกือบเกิดความเสียหาย (Near Miss)	เหตุการณ์ที่เกิดขึ้นแต่ยังไม่ก่อให้เกิดความเสียหาย หรือความเสียหายถูกป้องกันได้ก่อนเกิดผลกระทบ ใช้เป็นข้อมูลเตือนและปรับปรุงการควบคุม
โอกาสเกิด (Likelihood)	ความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้นภายในช่วงเวลาที่กำหนด โดยประเมินจากความน่าจะเป็น ความถี่ แนวโน้ม หรือข้อมูลเชิงคุณภาพตามเกณฑ์ที่ใช้

คำศัพท์	ความหมายที่ใช้ในคู่มือ
ผลกระทบหรือผลสืบเนื่อง (Impact/Consequence)	ผลที่อาจเกิดขึ้นต่อวัตถุประสงค์หรือผู้มีส่วนได้ส่วนเสีย โดยพิจารณาทั้งความรุนแรงและมิติที่เกี่ยวข้อง เหตุการณ์หนึ่งอาจมีผลกระทบหลายมิติ
กรอบเวลา (Time Horizon)	ช่วงเวลาที่ใช้พิจารณาการเกิดเหตุการณ์และผลกระทบ เช่น ปีงบประมาณ ระยะเวลาโครงการ หรือระยะแผนยุทธศาสตร์
การควบคุมที่มีอยู่ (Existing Controls)	นโยบาย กระบวนการ ระบบ หรือกิจกรรมที่มีอยู่ ณ วันที่ประเมิน เพื่อป้องกัน ลด ตรวจจับ หรือตอบสนองต่อความเสี่ยง โดยต้องตรวจสอบว่ามีการนำไปใช้และทำงานจริงเพียงใด
ความเสี่ยงโดยธรรมชาติ (Inherent Risk)	ระดับความเสี่ยงก่อนพิจารณาผลของการควบคุมหรือมาตรการตอบสนอง โดยระบุสมมติฐานและขอบเขตการประเมินให้ชัดเจน
ประสิทธิผลของการควบคุม (Control Effectiveness)	ผลการประเมินความเหมาะสมของการออกแบบ การนำไปใช้ และการทำงานของการควบคุมตามวัตถุประสงค์ โดยมีหลักฐานรองรับ
ความเสี่ยงคงเหลือ (Residual Risk)	ระดับความเสี่ยง ณ วันที่ประเมิน ภายหลังพิจารณาผลของการควบคุมที่นำไปใช้และมีหลักฐานแสดงประสิทธิผลแล้ว
ความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk)	ระดับความเสี่ยงที่คาดว่าจะเหลือภายหลังดำเนินมาตรการเพิ่มเติมและยืนยันประสิทธิผลภายในเวลาที่กำหนด เป็นเป้าหมายที่ต้องมีสมมติฐานรองรับ และไม่ใช้แทนระดับความเสี่ยงปัจจุบัน
ความเสี่ยงเกิดใหม่ (Emerging Risk)	ความเสี่ยงใหม่หรือความเสี่ยงเดิมที่เปลี่ยนแปลงจนข้อมูลหรือความเข้าใจที่มีอยู่ยังไม่เพียงพอ และอาจส่งผลสำคัญต่อวัตถุประสงค์ในอนาคต
ความสัมพันธ์ระหว่างความเสี่ยง (Risk Interdependency)	ความเชื่อมโยงที่ความเสี่ยงหนึ่งอาจเป็นสาเหตุ เปลี่ยนโอกาสเกิด เพิ่มหรือลดผลกระทบ หรือส่งผลต่อการจัดการความเสี่ยงอื่น
การกระจุกตัวของความเสี่ยง (Risk Concentration)	การที่ความเสี่ยงหลายรายการมีการพึ่งพาปัจจัย แหล่งรายได้ ระบบ ผู้ให้บริการ หรือทรัพยากรร่วมกัน จนอาจเกิดผลกระทบรวมอย่างมีนัยสำคัญ
ข้อมูลสรุปลักษณะและสถานะความเสี่ยง (Risk Profile)	ข้อมูลที่แสดงลักษณะ ระดับ แนวโน้ม และสถานะความเสี่ยงของมหาวิทยาลัย ส่วนงาน กระบวนการ หรือโครงการ ณ ช่วงเวลาที่กำหนด
มุมมองความเสี่ยงในภาพรวม (Risk Portfolio View)	การพิจารณาความเสี่ยงหลายรายการร่วมกัน รวมถึงความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัว เพื่อสนับสนุนการตัดสินใจระดับมหาวิทยาลัย
มิติผลกระทบร่วม (Cross-cutting Impact Dimension)	มิติผลกระทบที่ต้องพิจารณาข้ามประเภทความเสี่ยง เช่น ชื่อเสียง ความปลอดภัย ความต่อเนื่อง และ ESG โดยไม่ใช้แทนการจำแนกประเภทหลักของความเสี่ยง

1.10.3 ระดับการยอมรับและการตัดสินใจด้านความเสี่ยง

คำศัพท์	ความหมายที่ใช้ในคู่มือ
ความสามารถในการรองรับความเสี่ยง (Risk Capacity)	ขอบเขตความเสี่ยงสูงสุดที่มหาวิทยาลัยสามารถรองรับได้ภายใต้ทรัพยากร ฐานะการเงิน ข้อผูกพัน และความสามารถในการรักษาพันธกิจสำคัญ โดยไม่ถือเป็นการอนุญาตให้ฝ่าฝืนกฎหมาย
ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA)	ประเภทและระดับความเสี่ยงที่มหาวิทยาลัยยินดีรับในการดำเนินยุทธศาสตร์และบรรลุวัตถุประสงค์ ภายในความสามารถในการรองรับความเสี่ยงและข้อจำกัดที่เกี่ยวข้อง
ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT)	ขอบเขตความเบี่ยงเบนที่ยอมรับได้ในการดำเนินงานหรือผลลัพธ์ที่สัมพันธ์กับวัตถุประสงค์ โดยกำหนดเป็นเกณฑ์ที่ติดตามและใช้ตัดสินใจได้ และต้องสอดคล้องกับ RA
ขีดจำกัดความเสี่ยง (Risk Limit)	ขีดจำกัดเชิงปฏิบัติที่กำหนดสำหรับกิจกรรม การดำเนินงาน หรือการเปิดรับความเสี่ยง โดยระบุการดำเนินการและผู้มีอำนาจเมื่อเข้าใกล้หรือเกินขีดจำกัด
เหตุที่ไม่ยอมรับ (Zero Tolerance Event)	เหตุการณ์หรือพฤติการณ์ที่มหาวิทยาลัยกำหนดให้ต้องระงับ ควบคุม ผลกระทบ รายงาน และยกระดับตามเกณฑ์ทันที โดยไม่รอคะแนนความเสี่ยงรวมและไม่ยอมรับให้ดำเนินต่อ การใช้เกณฑ์นี้ไม่หมายความว่าสามารถป้องกันเหตุได้ทั้งหมด
การยอมรับความเสี่ยง (Risk Acceptance)	การตัดสินใจโดยผู้มีอำนาจให้คงความเสี่ยงไว้ภายใต้เหตุผล เงื่อนไข และการติดตามที่กำหนด โดยต้องพิจารณา RA/RT กฎหมาย และขอบเขตอำนาจ หากเกินเกณฑ์ต้องเสนอพิจารณาตามกระบวนการ และไม่ใช้การยอมรับเพื่ออนุญาตเหตุที่ไม่ยอมรับ
การตัดสินใจโดยคำนึงถึงความเสี่ยง (Risk-informed Decision-making)	การใช้ข้อมูลความเสี่ยง โอกาส ทางเลือก สมมติฐาน และข้อจำกัดประกอบการตัดสินใจ พร้อมบันทึกเหตุผลและประเด็นสำคัญที่ใช้พิจารณา
การยกระดับรายงานความเสี่ยง (Risk Escalation)	การส่งต่อข้อมูลความเสี่ยงหรือเหตุการณ์ไปยังผู้มีอำนาจตัดสินใจระดับสูงขึ้นตามเกณฑ์ ความเร่งด่วน ระยะเวลา และเส้นทางรายงานที่กำหนด
เกณฑ์ยกระดับเป็นกรณีพิเศษ (Override Criteria)	เงื่อนไขที่ทำให้ต้องเพิ่มความเร่งด่วนหรือระดับการตอบสนอง แม้คะแนนความเสี่ยงไม่ถึงเกณฑ์ปกติ โดยไม่เปลี่ยนคะแนน L × I เว้นแต่มีข้อมูลใหม่รองรับการประเมิน

RA RT และ Risk Limit ต้องระบุขอบเขต ตัวชี้วัด หน่วยวัด ช่วงเวลา และผู้มีอำนาจอนุมัติให้ชัดเจน เพื่อหลีกเลี่ยงการใช้เกณฑ์ต่างความหมายแทนกัน

1.10.4 การติดตามและรายงานความเสี่ยง

คำศัพท์	ความหมายที่ใช้ในคู่มือ
ทะเบียนความเสี่ยง (Risk Register)	เอกสารหรือฐานข้อมูลที่บันทึกวัตถุประสงค์ ข้อความความเสี่ยง ประเภท สาเหตุ ผลกระทบ การประเมิน การควบคุม ผู้รับผิดชอบ มาตรการ ตัวชี้วัด และผลการติดตาม พร้อมวันที่และหลักฐานอ้างอิง
แผนบริหารความเสี่ยง (Risk Treatment Plan)	แผนที่กำหนดแนวทางตอบสนองและมาตรการ เจ้าของมาตรการ ทรัพยากร กำหนดเวลา ผลส่งมอบ ตัวชี้วัด หลักฐาน และระดับความเสี่ยงคงเหลือเป้าหมาย
ตัวชี้วัดผลการดำเนินงาน (Key Performance Indicator: KPI)	ตัววัดความก้าวหน้าหรือความสำเร็จในการบรรลุวัตถุประสงค์และเป้าหมายผลการดำเนินงาน
ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI)	ตัววัดระดับ แนวโน้ม หรือปัจจัยขับเคลื่อนความเสี่ยง ใช้ติดตามการเปลี่ยนแปลงและเชื่อมโยงกับเกณฑ์การเฝ้าระวัง การตอบสนอง และการยกระดับรายงาน
ตัวชี้วัดการควบคุมที่สำคัญ (Key Control Indicator: KCI)	ตัววัดการดำเนินการหรือประสิทธิผลของการควบคุมสำคัญ ซึ่งต้องใช้ร่วมกับหลักฐานที่เหมาะสม ไม่สรุปประสิทธิผลจากความครบถ้วนของกิจกรรมเพียงอย่างเดียว
สัญญาณเตือนล่วงหน้า (Early Warning Signal: EWS)	ข้อมูล เหตุการณ์ หรือแนวโน้มที่บ่งชี้ว่าความเสี่ยงอาจเปลี่ยนแปลงหรือเข้าใกล้เกณฑ์ เพื่อให้เตรียมการหรือตอบสนองก่อนเกิดผลกระทบสำคัญ
จุดกระตุ้นการดำเนินการ (Trigger)	ค่าเกณฑ์ เหตุการณ์ หรือเงื่อนไขที่กำหนดให้เริ่มการตรวจสอบ เฝ้าระวัง แก้ไข รายงาน หรือยกระดับ โดยระบุผู้รับผิดชอบและระยะเวลาดำเนินการ
ค่าฐาน (Baseline)	ข้อมูลเริ่มต้นที่ใช้เปรียบเทียบแนวโน้มหรือผลการเปลี่ยนแปลง โดยระบุวันที่ ขอบเขต นิยาม และแหล่งข้อมูล
หลักฐานผลการดำเนินงาน (Evidence)	ข้อมูลหรือเอกสารที่ตรวจสอบย้อนกลับได้ เช่น บันทึกการปฏิบัติ รายงานระบบ ผลการทดสอบ และผลการตรวจสอบ ซึ่งใช้รองรับการประเมินและข้อสรุป
บันทึกการตัดสินใจ (Decision Log)	บันทึกประเด็น ข้อมูล ทางเลือก เหตุผล ผู้มีอำนาจตัดสินใจ วันที่ เงื่อนไข และการติดตามผลของการตัดสินใจด้านความเสี่ยง

ตัวชี้วัดหนึ่งอาจใช้เป็น KPI KRI หรือ KCI ได้ตามวัตถุประสงค์ แต่ต้องระบุบทบาท นิยาม สูตรคำนวณ และเกณฑ์การใช้ให้ชัดเจน รวมทั้งแยกผลสำเร็จของกิจกรรมออกจากผลต่อระดับความเสี่ยง

1.10.5 การตอบสนอง การควบคุม และการให้ความเชื่อมั่น

คำศัพท์	ความหมายที่ใช้ในคู่มือ
การตอบสนองต่อความเสี่ยง (Risk Response)	การเลือกแนวทางจัดการความเสี่ยงหรือโอกาส เช่น หลีกเลี่ยง ลดหรือควบคุม แบ่งปันหรือถ่ายโอน ยอมรับ หรือใช้ประโยชน์จากโอกาส โดยพิจารณาความคุ้มค่าและข้อจำกัดที่เกี่ยวข้อง
การควบคุมภายใน (Internal Control)	กระบวนการที่ผู้กำกับดูแล ฝ่ายบริหาร และบุคลากรร่วมดำเนินการ ผ่านนโยบาย ระบบ และกิจกรรม เพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลต่อวัตถุประสงค์ด้านการดำเนินงาน การรายงาน และการปฏิบัติตามข้อกำหนด
การให้ความเชื่อมั่น (Assurance)	การประเมินหลักฐานอย่างเป็นระบบเพื่อให้ข้อสรุปต่อความเพียงพอและประสิทธิผลของการกำกับดูแล การบริหารความเสี่ยง และการควบคุม โดยระบุขอบเขต เกณฑ์ วิธีการ ข้อจำกัด และระดับความเป็นอิสระของผู้ประเมิน
หลัก Three Lines	หลักการจัดวางและประสานบทบาทของผู้กำกับดูแล ฝ่ายบริหารในสายงานที่หนึ่งและสายงานที่สอง และการตรวจสอบภายในในสายงานที่สาม โดยรักษาความรับผิดชอบและความเป็นอิสระตามบทบาท
ความเชื่อมโยงความเสี่ยง–การควบคุม–การให้ความเชื่อมั่น (Risk–Control–Assurance)	การเชื่อมความเสี่ยงสำคัญกับการควบคุมและหลักฐานหรือแหล่งความเชื่อมั่นเพื่อประเมินว่าการควบคุมตอบสนองต่อความเสี่ยงและทำงานอย่างมีประสิทธิผลเพียงใด
แผนผังการให้ความเชื่อมั่น (Assurance Map)	เครื่องมือที่แสดงความเสี่ยงสำคัญ การควบคุม ผู้รับผิดชอบ และแหล่งความเชื่อมั่น เพื่อระบุช่องว่าง ความซ้ำซ้อน และแนวทางประสานงาน
การกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ (Governance, Risk and Compliance: GRC)	แนวทางเชื่อมโยงการกำกับดูแล ความเสี่ยง และข้อกำหนด เพื่อให้การตัดสินใจ ความรับผิดชอบ การควบคุม ข้อมูล และการรายงานสนับสนุนกัน
วัฒนธรรมความเสี่ยง (Risk Culture)	ค่านิยม ทัศนคติ พฤติกรรม และแนวปฏิบัติร่วมที่มีอิทธิพลต่อการรับรู้ การตัดสินใจ การรายงาน และความรับผิดชอบด้านความเสี่ยง
การวิเคราะห์สาเหตุราก (Root Cause Analysis)	การวิเคราะห์ปัจจัยต้นเหตุของปัญหา เหตุการณ์ หรือข้อบกพร่อง เพื่อกำหนดมาตรการที่แก้ไขสาเหตุและลดการเกิดซ้ำ
มาตรการแก้ไขและป้องกัน (Corrective and Preventive Action: CAPA)	มาตรการแก้ไขสาเหตุของข้อบกพร่องหรือเหตุการณ์ที่เกิดขึ้น และมาตรการป้องกันเหตุที่อาจเกิดขึ้น โดยกำหนดผู้รับผิดชอบ เวลา และวิธีตรวจสอบผล

การแบ่งปันหรือถ่ายโอนความเสี่ยง เช่น การประกันภัยหรือการจ้างบริการ ไม่ทำให้มหาวิทยาลัยพ้นจากความรับผิดชอบตามกฎหมาย สัญญา หรือหน้าที่กำกับดูแลที่ยังคงมีอยู่

1.10.6 ความต่อเนื่อง ความยืดหยุ่น และความยั่งยืน

คำศัพท์	ความหมายที่ใช้ในคู่มือ
การบริหารความต่อเนื่องขององค์กร (Business Continuity Management: BCM)	การบริหารเพื่อเตรียมพร้อมและรักษาหรือฟื้นคืนการดำเนินพันธกิจสำคัญให้อยู่ในระดับและระยะเวลาที่กำหนดเมื่อเกิดเหตุหยุดชะงัก
แผนความต่อเนื่องในการดำเนินงาน (Business Continuity Plan: BCP)	แผนที่กำหนดภารกิจสำคัญ ผู้รับผิดชอบ ทรัพยากร เกณฑ์การใช้แผน วิธีดำเนินงานทดแทน การสื่อสาร และการฟื้นคืนการดำเนินงาน
การวิเคราะห์ผลกระทบต่อการดำเนินงาน (Business Impact Analysis: BIA)	การวิเคราะห์ผลกระทบของการหยุดชะงักที่เปลี่ยนแปลงตามเวลาเพื่อกำหนดลำดับความสำคัญ ระดับบริการ และความต้องการในการฟื้นคืน
ระยะเวลาเป้าหมายในการฟื้นคืน (Recovery Time Objective: RTO)	ระยะเวลาเป้าหมายภายหลังเหตุหยุดชะงักที่ต้องฟื้นคืนกิจกรรมหรือบริการให้อยู่ในระดับที่กำหนด
จุดเป้าหมายการกู้คืนข้อมูล (Recovery Point Objective: RPO)	จุดเวลาเป้าหมายที่ต้องกู้คืนข้อมูลกลับมาได้ โดยมักแสดงเป็นช่วงเวลาข้อมูลย้อนหลังที่ยอมสูญเสียได้
ความยืดหยุ่นขององค์กร (Organizational Resilience)	ความสามารถในการคาดการณ์ เตรียมพร้อม ตอบสนอง ปรับตัว และฟื้นตัวจากการเปลี่ยนแปลงหรือเหตุหยุดชะงัก พร้อมรักษาพันธกิจสำคัญและคุณค่า
สิ่งแวดล้อม สังคม และธรรมาภิบาล (Environmental, Social and Governance: ESG)	กรอบพิจารณาปัจจัยและผลกระทบด้านสิ่งแวดล้อม สังคม และธรรมาภิบาลที่เกี่ยวข้องกับยุทธศาสตร์ การดำเนินงาน ผู้มีส่วนได้ส่วนเสีย และความยั่งยืน
ความปลอดภัย (Safety)	มิติที่พิจารณาการป้องกันอันตรายต่อชีวิต สุขภาพ และสวัสดิภาพในการศึกษา การวิจัย การปฏิบัติงาน และการให้บริการ รวมถึงสภาพแวดล้อมและอาคารสถานที่ที่เกี่ยวข้อง
ระดับการพัฒนาระบบบริหารความเสี่ยง (Risk Management Maturity)	ระดับความพร้อม ความสามารถ การบูรณาการ และประสิทธิผลของระบบ ซึ่งประเมินจากการปฏิบัติและหลักฐาน เพื่อระบุช่องว่างและกำหนดแนวทางพัฒนา

1.10.7 คะแนน ระดับความเสี่ยง และเกณฑ์การตอบสนอง

มหาวิทยาลัยใช้คะแนนโอกาสเกิด (Likelihood: L) และผลกระทบ (Impact: I) ระดับ 1–5 ตามเกณฑ์ที่กำหนด โดยคำนวณดังนี้

คะแนนความเสี่ยง (Risk Score) = โอกาสเกิด (L) × ผลกระทบ (I)

ให้ใช้เกณฑ์คะแนนและระดับเดียวกันในการประเมินความเสี่ยงโดยธรรมชาติ ความเสี่ยงคงเหลือ และความเสี่ยงคงเหลือเป้าหมาย พร้อมระบุวันที่ กรอบเวลา และหลักฐานหรือสมมติฐานของแต่ละระดับ

คะแนน	ระดับความเสี่ยง	รหัสระดับ	แนวทางดำเนินการขั้นต่ำ
1–4	ต่ำ (Low)	L	ติดตามการควบคุมและการเปลี่ยนแปลงตามรอบปกติ การยอมรับต้องอยู่ภายในเกณฑ์และอำนาจที่กำหนด
5–9	ปานกลาง (Medium)	M	ทบทวนความเพียงพอของการควบคุม กำหนดมาตรการเพิ่มเติมตามความจำเป็น และติดตามโดยเจ้าของความเสี่ยง
10–15	สูง (High)	H	จัดทำหรือทบทวนแผนบริหารความเสี่ยง กำหนดผู้รับผิดชอบและเป้าหมาย และรายงานผู้บริหารตามเกณฑ์
16–25	สูงมาก (Extreme)	E	เร่งควบคุมผลกระทบและดำเนินมาตรการ พร้อมยกระดับรายงานตามความเร่งด่วนและระยะเวลาที่กำหนด

รหัส **L** ในคอลัมน์ระดับความเสี่ยงหมายถึง Low ส่วน **L** ในสูตร L × I หมายถึง Likelihood ให้พิจารณาตามบริบทของข้อมูล

คะแนนความเสี่ยงใช้ประกอบการจัดลำดับความสำคัญ แต่ไม่ใช่ข้อยุติในการยอมรับความเสี่ยง ต้องพิจารณา RA/RT ข้อจำกัดตามกฎหมาย ประสิทธิผลของการควบคุม ความสัมพันธ์ระหว่างความเสี่ยง และขอบเขตอำนาจร่วมด้วย

ให้พิจารณาเพิ่มความเร่งด่วนหรือยกระดับการตอบสนองเป็นกรณีพิเศษเมื่อมีเงื่อนไข เช่น

1. ผลกระทบอยู่ในระดับ 5 ให้ตอบสนองอย่างน้อยตามแนวทางความเสี่ยงระดับสูง แม้คะแนนรวมต่ำกว่า 10
2. เกิดเหตุที่ไม่ยอมรับหรือเหตุฉุกเฉิน ให้ตอบสนองและยกระดับทันทีตามเกณฑ์ โดยไม่รอการคำนวณคะแนน
3. KRI เข้าใกล้หรือเกิน RT หรือ Risk Limit ให้ดำเนินการตาม Trigger ที่กำหนด
4. ความเสี่ยงกระทบหลายส่วนงาน มีผลกระทบร่วม หรือมีการกระจุกตัวอย่างมีนัยสำคัญ
5. ความเสี่ยงกระทบวัตถุประสงค์เชิงยุทธศาสตร์ พันธกิจสำคัญ ชีวิต ความปลอดภัย กฎหมาย หรือชื่อเสียงอย่างมีนัยสำคัญ
6. ระดับความเสี่ยงเพิ่มขึ้นอย่างรวดเร็ว ข้อมูลไม่เพียงพอ หรือสมมติฐานสำคัญมีความไม่แน่นอนสูง จนต้องทบทวนหรือเตรียมมาตรการเพิ่มเติม

การใช้เกณฑ์ยกระดับเป็นกรณีพิเศษให้บันทึกเหตุผล หลักฐาน ผู้เสนอ ผู้มีอำนาจพิจารณา วันที่ตัดสินใจ ระดับการตอบสนอง มาตรการ และกำหนดเวลาทบทวน โดยคงคะแนน L × I ตามผลการประเมินที่มีหลักฐานรองรับ หากมีข้อมูลใหม่จึงประเมินและบันทึกคะแนนใหม่ การดำเนินการเร่งด่วนเมื่อเข้าเกณฑ์ต้องไม่รอให้การบันทึกหรือการวิเคราะห์สาเหตุเสร็จสิ้น

1.10.8 ประเภทความเสี่ยงหลักของมหาวิทยาลัย

มหาวิทยาลัยแม่โจ้จำแนกความเสี่ยงหลักเป็น 5 ประเภท ได้แก่ S O F C และ D โดยพิจารณาจากสาเหตุ ลักษณะเหตุการณ์ และวัตถุประสงค์ที่ได้รับผลกระทบ ดังนี้

รหัส	ประเภทความเสี่ยง	ความหมาย
S	**ความเสี่ยงด้านยุทธศาสตร์ (Strategic Risk)**	ความไม่แน่นอนที่อาจส่งผลต่อการกำหนดหรือดำเนินยุทธศาสตร์ การบรรลุเป้าประสงค์ และความสามารถในการแข่งขันหรือปรับตัวของมหาวิทยาลัย เช่น การเปลี่ยนแปลงจำนวนและความต้องการของผู้เรียน ความเหมาะสมของหลักสูตร และการปรับตัวต่อ AI และเทคโนโลยีดิจิทัล
O	**ความเสี่ยงด้านการดำเนินงาน (Operational Risk)**	ความไม่แน่นอนที่เกิดจากบุคลากร กระบวนการ ระบบงาน ทรัพยากร หรือเหตุการณ์ภายนอก ซึ่งอาจกระทบประสิทธิภาพ คุณภาพ และความต่อเนื่องของการดำเนินพันธกิจ เช่น ช่องว่างทักษะบุคลากร กระบวนการทำงานผิดพลาด และการหยุดชะงักของบริการ
F	**ความเสี่ยงด้านการเงิน (Financial Risk)**	ความไม่แน่นอนที่อาจกระทบรายได้ ค่าใช้จ่าย งบประมาณ สภาพคล่อง การลงทุน ภาระผูกพัน และความยั่งยืนทางการเงิน เช่น รายได้ต่ำกว่าเป้าหมาย ต้นทุนเพิ่มขึ้น และเงินสดไม่เพียงพอต่อการดำเนินงาน
C	**ความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (Compliance and Governance Risk)**	ความไม่แน่นอนที่อาจนำไปสู่การไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ สัญญา มาตรฐาน จริยธรรม หรือหลักธรรมาภิบาล เช่น การทุจริต ผลประโยชน์ทับซ้อน การจัดซื้อจัดจ้างไม่ถูกต้อง และการละเมิดข้อกำหนดด้านข้อมูลส่วนบุคคล
D	**ความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Technology Risk)**	ความไม่แน่นอนที่เกิดจากเทคโนโลยี ระบบสารสนเทศ โครงสร้างพื้นฐานดิจิทัล ข้อมูล หรือการใช้ AI ซึ่งอาจกระทบความมั่นคงปลอดภัย ความถูกต้อง ความพร้อมใช้งาน และการบรรลุวัตถุประสงค์ เช่น การโจมตีไซเบอร์ ระบบล่ม ข้อมูลสูญหาย และผลลัพธ์จาก AI ที่คลาดเคลื่อน

ให้กำหนดประเภทหลักหนึ่งประเภทต่อรายการความเสี่ยง เพื่อสนับสนุนการกำหนดเจ้าของความเสี่ยงและการรายงาน พร้อมระบุประเภทอื่นที่เกี่ยวข้องได้ โดยไม่บันทึกความเสี่ยงเดียวกันซ้ำหลายรายการเพียงเพราะมีผลกระทบหลายด้าน

ตัวอย่างเช่น ความเสี่ยงข้อมูลส่วนบุคคลรั่วไหลอาจจัดเป็น **D** เมื่อสาเหตุหลักเกิดจากช่องโหว่ทางเทคนิค เป็น **O** เมื่อเกิดจากกระบวนการปฏิบัติงาน และเป็น **C** เมื่อประเด็นหลักเกี่ยวข้องกับการไม่ปฏิบัติตามข้อกำหนดทางกฎหมาย ทั้งนี้ ให้พิจารณาความเชื่อมโยงระหว่างประเภทควบคู่กัน

ชื่อเสียงและความเชื่อมั่น ความปลอดภัย ความต่อเนื่อง และมิติสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG) ให้พิจารณาเป็น **มิติผลกระทบร่วม** ของความเสี่ยงทั้ง 5 ประเภทตามลักษณะของแต่ละประเด็น

ส่วนที่ 2
นโยบายและกรอบการบริหารความเสี่ยง

2.1 ถ้อยแถลงการกำกับดูแลความเสี่ยงของมหาวิทยาลัย

สภามหาวิทยาลัยแม่โจ้ตระหนักว่าความเสี่ยงและโอกาสเป็นส่วนหนึ่งของการกำหนดยุทธศาสตร์ การตัดสินใจ และการดำเนินพันธกิจภายใต้ความไม่แน่นอน การบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM) จึงเป็นกลไกสำคัญของธรรมาภิบาลที่สนับสนุนการบรรลุวิสัยทัศน์ พันธกิจ เป้าประสงค์ และผลลัพธ์เชิงยุทธศาสตร์ รวมทั้งการสร้าง รักษา และเพิ่มคุณค่าให้แก่มหาวิทยาลัยและผู้มีส่วนได้ส่วนเสียอย่างยั่งยืน

สภามหาวิทยาลัยกำหนดทิศทางและความคาดหวังด้านการบริหารความเสี่ยง พิจารณาอนุมัตินโยบายและกรอบระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite Framework) ตามอำนาจหน้าที่ และกำกับติดตามความเพียงพอและประสิทธิผลของระบบ โดยมีคณะกรรมการที่เกี่ยวข้องสนับสนุนตามขอบเขตที่ได้รับมอบหมาย ทั้งนี้ ต้องได้รับข้อมูลความเสี่ยง การควบคุม และผลการให้ความเชื่อมั่นที่ถูกต้อง ครบถ้วน ทันเวลา และตรวจสอบย้อนกลับได้ พร้อมข้อจำกัดของข้อมูลและประเด็นที่ต้องตัดสินใจ

ฝ่ายบริหารรับผิดชอบนำนโยบายและกรอบที่ได้รับอนุมัติไปสู่การปฏิบัติ โดยเชื่อมโยงความเสี่ยงกับวัตถุประสงค์และผลการดำเนินงาน กำหนดเจ้าของความเสี่ยงและผู้รับผิดชอบที่เกี่ยวข้อง จัดสรรทรัพยากร ดำเนินการควบคุมและมาตรการ ตลอดจนติดตามตัวชี้วัดความเสี่ยงที่สำคัญ (KRI) และสัญญาณเตือนล่วงหน้า (EWS) เมื่อความเสี่ยงเข้าใกล้หรือเกินเกณฑ์ เกิดเหตุที่ไม่ยอมรับ หรือเกินอำนาจตัดสินใจ ต้องตอบสนองและยกระดับรายงานตามความเร่งด่วน เส้นทาง และระยะเวลาที่กำหนด

มหาวิทยาลัยกำหนดให้ฝ่ายบริหารและส่วนงานรับผิดชอบความเสี่ยงในขอบเขตงานของตน โดยบูรณาการการบริหารความเสี่ยงกับยุทธศาสตร์ แผนงาน งบประมาณ การบริหารผลการดำเนินงาน การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ และการบริหารความต่อเนื่อง หน่วยงานในสายงานที่สองทำหน้าที่สนับสนุน ติดตาม และสอบทานตามบทบาท ส่วนกองตรวจสอบภายในให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรม โดยไม่รับผิดชอบตัดสินใจหรือบริหารความเสี่ยงแทนฝ่ายบริหาร

มหาวิทยาลัยส่งเสริมวัฒนธรรมที่เปิดกว้างต่อการรายงานความเสี่ยง สัญญาณเตือน เหตุการณ์ ข้อผิดพลาด และข้อกังวลโดยสุจริต เพื่อให้สามารถตอบสนอง เรียนรู้ และปรับปรุงได้ทันเวลา พร้อมรักษาความลับและคุ้มครองผู้รายงานตามข้อกำหนดที่เกี่ยวข้อง มหาวิทยาลัยไม่ยอมรับการปกปิดหรือบิดเบือนข้อมูล การทุจริต การกระทำผิดกฎหมาย และการละเมิดจริยธรรมหรือหลักธรรมาภิบาล โดยให้ดำเนินการตรวจสอบและจัดการอย่างเป็นธรรมตามกระบวนการและอำนาจหน้าที่

การกำกับดูแลความเสี่ยงต้องพิจารณาทั้งความเสี่ยงรายประเด็นและภาพรวมของมหาวิทยาลัย รวมถึงความสัมพันธ์ ผลกระทบร่วม การกระจุกตัว และความเสี่ยงเกิดใหม่ โดยใช้ผลการติดตามและหลักฐานประสิทธิผลของการควบคุมประกอบการทบทวนยุทธศาสตร์ กรอบการยอมรับความเสี่ยง และการจัดสรรทรัพยากรอย่างต่อเนื่อง

หลักการกำกับดูแล: การบริหารความเสี่ยงต้องให้ข้อมูลและเหตุผลที่ใช้ตัดสินใจได้ แสดงผู้รับผิดชอบ การตอบสนอง และผลลัพธ์ที่ตรวจสอบได้ เพื่อสนับสนุนการบรรลุวัตถุประสงค์ คุ้มครองพันธกิจสำคัญ และเสริมสร้างความยืดหยุ่นของมหาวิทยาลัยภายใต้ความไม่แน่นอน

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 การบริหาร

ทรัพยากร 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) ให้สอดคล้องกับบริบท เป้าหมาย และศักยภาพในการบริหารจัดการขององค์กร เพื่อใช้เป็นกรอบในการตัดสินใจ การจัดลำดับความสำคัญ และการตอบสนองต่อความเสี่ยง

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

5. การใช้มาตรฐานและแนวปฏิบัติเดียวกันทั่วทั้งองค์กร มหาวิทยาลัยกำหนดกระบวนการ เครื่องมือ หลักเกณฑ์ และรูปแบบการรายงานด้านการบริหารความเสี่ยงให้เป็น

มาตรฐานเดียวกันทั่วทั้งองค์กร 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

สภามหาวิทยาลัยมีมติเห็นชอบ ในการประชุมครั้งที่ 9/2569
เมื่อวันที่ 24 กันยายน 2569

2.3 นโยบายระดับความเสี่ยงที่ยอมรับได้

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

การกำหนดระดับความเสี่ยงที่ยอมรับได้สะท้อนถึงระดับความเสี่ยงที่มหาวิทยาลัยยินดีรับเพื่อให้บรรลุเป้าหมายเชิงยุทธศาสตร์ โดยคำนึงถึงผลกระทบที่อาจเกิดขึ้นต่อผู้เรียน บุคลากร ผู้มีส่วนได้ส่วนเสีย ชื่อเสียง ความมั่นคงทางการเงิน และความยั่งยืนขององค์กร ทั้งนี้ มหาวิทยาลัยกำหนดระดับความเสี่ยงที่ยอมรับได้ในแต่ละมิติ ดังต่อไปนี้

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 โดยกำหนดระดับความเสี่ยงที่ยอมรับได้ดังนี้

3.1 การปฏิบัติตามวินัยการเงินการคลัง

มหาวิทยาลัยยึดมั่นในการบริหารงบประมาณ การเงิน และทรัพย์สินของรัฐอย่างโปร่งใส ถูกต้อง และเป็นไปตามกฎหมาย 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 หรือการกระทำที่ส่งผลกระทบต่อความน่าเชื่อถือและความถูกต้องขององค์กร

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 เพื่อให้สอดคล้องกับลักษณะ

ภารกิจ บริบทการดำเนินงาน และสภาพแวดล้อมที่เปลี่ยนแปลงไป โดยต้องไม่ขัดต่อหลักเกณฑ์ นโยบาย และระดับความเสี่ยงที่มหาวิทยาลัยกำหนด

การกำหนด Risk Tolerance ต้องสามารถวัดผลได้อย่างชัดเจน มีตัวชี้วัดหรือเกณฑ์ควบคุมที่เหมาะสม และได้รับการทบทวนเป็นประจำ เพื่อให้สามารถสนับสนุนการบรรลุเป้าหมายเชิงยุทธศาสตร์ ควบคู่ไปกับการรักษาความเชื่อมั่นของผู้มีส่วนได้ส่วนเสียและความยั่งยืนของมหาวิทยาลัยในระยะยาว

ตารางที่ 2-1 ***ตารางแสดงระดับความเสี่ยงที่ยอมรับได้ของมหาวิทยาลัย จำแนกตามมิติ***

มิติ	ระดับโดยรวม	เจตนารมณ์และขอบเขต
1. **การจัดการศึกษาและคุณภาพผู้เรียน/บัณฑิต**	ต่ำ	➢ รักษามาตรฐานหลักสูตร ผลลัพธ์การเรียนรู้ คุณภาพบัณฑิต และสิทธิของผู้เรียน ไม่ยอมรับการลดมาตรฐานที่มีนัยสำคัญ
2. **การวิจัย นวัตกรรม และการใช้ประโยชน์**	ปานกลาง	➢ ยอมรับความไม่แน่นอนที่ผ่านการประเมินเพื่อส่งเสริมนวัตกรรม งานวิจัยผลกระทบสูง และการใช้ประโยชน์ภายใต้กรอบจริยธรรม 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) 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 และเมื่อเกิดกรณีใดกรณีหนึ่งดังต่อไปนี้

- 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

“เป็นมหาวิทยาลัยที่บูรณาการการบริหารความเสี่ยงและการควบคุมภายในกับยุทธศาสตร์และการดำเนินงาน ตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเป็นฐาน พร้อมปรับตัวและฟื้นตัวเพื่อสร้างคุณค่าอย่างยั่งยืน”

“A resilient university that integrates risk management and internal control into strategy and operations, makes risk-informed and data-driven decisions, and adapts and recovers to create sustainable value.”

องค์ประกอบสำคัญของวิสัยทัศน์ ได้แก่

1. บูรณาการ (Integrated) เชื่อมโยงการบริหารความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ และการให้ความเชื่อมั่นเข้ากับการบริหารและการดำเนินงาน โดยกำหนดความรับผิดชอบให้ชัดเจนและรักษาความเป็นอิสระตามบทบาท

2. เชื่อมโยงยุทธศาสตร์ (Strategy-aligned) ใช้ข้อมูลความเสี่ยงและโอกาสประกอบการกำหนดยุทธศาสตร์ วัตถุประสงค์ แผนงาน และการจัดสรรทรัพยากร เพื่อสนับสนุนการบรรลุเป้าประสงค์ของมหาวิทยาลัย

3. ตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเป็นฐาน (Risk-informed and Data-driven Decision-making) ใช้ข้อมูลผลการดำเนินงาน สถานะความเสี่ยงเทียบกับ RA/RT ตัวชี้วัดความเสี่ยงที่สำคัญ (KRI) และสัญญาณเตือนล่วงหน้า (EWS) พร้อมพิจารณาทางเลือก สมมติฐาน และข้อจำกัด เพื่อให้ตัดสินใจและตอบสนองได้อย่างเหมาะสมและทันเวลา

4. มีความยืดหยุ่น (Resilient) พัฒนาความสามารถในการคาดการณ์ เตรียมพร้อม ตอบสนอง ปรับตัว และฟื้นตัวจากการเปลี่ยนแปลงหรือเหตุหยุดชะงัก โดยรักษาความต่อเนื่องของพันธกิจสำคัญ

5. สร้างคุณค่าอย่างยั่งยืน (Sustainable Value Creation) สร้าง รักษา และเพิ่มคุณค่าให้แก่มหาวิทยาลัยและผู้มีส่วนได้ส่วนเสีย ผ่านการใช้ประโยชน์จากโอกาส การใช้ทรัพยากรอย่างคุ้มค่า และการคำนึงถึงผลกระทบด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล

2.5 วัตถุประสงค์เชิงนโยบาย

นโยบายการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้มีวัตถุประสงค์ดังต่อไปนี้

1. สนับสนุนการบรรลุยุทธศาสตร์และผลลัพธ์สำคัญ เชื่อมโยงการบริหารความเสี่ยงและโอกาสกับวิสัยทัศน์ พันธกิจ เป้าประสงค์เชิงยุทธศาสตร์ และตัวชี้วัด เพื่อสนับสนุนการบรรลุผลลัพธ์ที่มหาวิทยาลัยกำหนดภายใต้ความไม่แน่นอน

2. ยกระดับคุณภาพการตัดสินใจ ส่งเสริมการตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเป็นฐาน (Risk-informed and Data-driven Decision-making) ในการกำหนดนโยบาย พิจารณาการลงทุน อนุมัติแผนงานและโครงการ จัดลำดับความสำคัญ และจัดสรรทรัพยากร โดยพิจารณาทางเลือก ผลกระทบ สมมติฐาน และข้อจำกัดของข้อมูลอย่างรอบด้าน

3. บริหารความเสี่ยงภายในกรอบและอำนาจที่กำหนด กำกับให้การดำเนินงานสอดคล้องกับความสามารถในการรองรับความเสี่ยง (Risk Capacity) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) พร้อมกำหนดการตอบสนองและการยกระดับรายงานเมื่อเข้าใกล้หรือเกินเกณฑ์ โดยคำนึงถึงข้อกำหนด ทางกฎหมายและขอบเขตอำนาจตัดสินใจ

4. บูรณาการการบริหารความเสี่ยงทั่วทั้งมหาวิทยาลัย เชื่อมโยงความเสี่ยงระดับมหาวิทยาลัย ส่วนงาน กระบวนการ และโครงการ รวมถึงความเสี่ยงจากผู้รับจ้าง ผู้ให้บริการ และคู่ความร่วมมือ โดยพิจารณาความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัวของความเสี่ยง เพื่อสนับสนุนการกำกับดูแลและการตัดสินใจในภาพรวม

5. ลดผลกระทบและเสริมสร้างความต่อเนื่องและความยืดหยุ่น พัฒนาความพร้อมในการคาดการณ์ ป้องกัน ตรวจจับ ตอบสนอง ปรับตัว และฟื้นตัวจากเหตุฉุกเฉิน ภาวะวิกฤต และเหตุหยุดชะงัก พร้อมติดตามความเสี่ยงเกิดใหม่ เพื่อคุ้มครองชีวิต ความปลอดภัย ข้อมูล ทรัพย์สิน และพันธกิจสำคัญของมหาวิทยาลัย

6. เสริมสร้างธรรมาภิบาล การควบคุม และการให้ความเชื่อมั่น เชื่อมโยงการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ (GRC) กับการควบคุมภายในและการให้ความเชื่อมั่นตามหลัก Three Lines โดยกำหนดความรับผิดชอบให้ชัดเจน ส่งเสริมความโปร่งใสและการตรวจสอบย้อนกลับ และรักษาความเป็นอิสระของการตรวจสอบภายใน

7. ส่งเสริมวัฒนธรรมความเสี่ยงและความรับผิดชอบตามบทบาท พัฒนาความตระหนัก ความรู้ และทักษะของผู้บริหารและบุคลากรทุกระดับ ส่งเสริมความเป็นเจ้าของความเสี่ยง การประสานงาน และการรายงานข้อมูลหรือข้อกังวลโดยสุจริตอย่างทันเวลา พร้อมนำผลการติดตามและบทเรียนมาปรับปรุงการดำเนินงานอย่างต่อเนื่อง

8. สร้าง รักษา และเพิ่มคุณค่าอย่างยั่งยืน สนับสนุนการใช้ประโยชน์จากโอกาสและนวัตกรรม การใช้ทรัพยากรอย่างคุ้มค่า และการพัฒนาคุณภาพและความเป็นเลิศ ควบคู่กับการคุ้มครองผู้มีส่วนได้ส่วนเสีย การรักษาความเชื่อมั่น และความรับผิดชอบด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG)

การติดตามวัตถุประสงค์เชิงนโยบายให้พิจารณาผลลัพธ์และหลักฐานร่วมกัน ทั้งการบรรลุเป้าประสงค์ สถานะความเสี่ยงเทียบกับเกณฑ์ ประสิทธิผลของการควบคุม การตอบสนองต่อสัญญาณเตือน และความพร้อมในการรักษาพันธกิจสำคัญ เพื่อให้การบริหารความเสี่ยงสนับสนุนการตัดสินใจและสร้างคุณค่าได้อย่างเป็นรูปธรรม

2.6 โครงสร้างกรอบการบริหารความเสี่ยงที่มหาวิทยาลัยประยุกต์ใช้

มหาวิทยาลัยแม่โจ้บูรณาการกฎหมาย หลักเกณฑ์ มาตรฐาน และกรอบแนวปฏิบัติที่เกี่ยวข้องให้เป็นระบบบริหารความเสี่ยงที่เชื่อมโยงกัน โดยแยกข้อกำหนดที่ต้องปฏิบัติตามออกจากแนวทางที่นำมาประยุกต์ใช้ และกำหนดบทบาทของแต่ละกรอบให้ชัดเจน ดังนี้

ตารางที่ 2-2 ***ตารางแสดงกรอบอ้างอิงและการประยุกต์ใช้ในระบบบริหารความเสี่ยงของมหาวิทยาลัย***

กรอบอ้างอิง	บทบาทในการประยุกต์ใช้	การนำมาใช้ในมหาวิทยาลัย
หลักเกณฑ์และแนวทางกระทรวงการคลังด้านการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ	กำหนดพื้นฐานการจัดให้มีระบบบริหารความเสี่ยงตามขอบเขตการใช้บังคับ	กำหนดความรับผิดชอบ กระบวนการ แผน การติดตาม การรายงาน และหลักฐานการดำเนินงาน
COSO ERM 2017	เชื่อมโยงการบริหารความเสี่ยงกับยุทธศาสตร์ ผลการดำเนินงาน และการสร้างคุณค่า	ใช้กำกับดูแลและพัฒนาวัฒนธรรมความเสี่ยง ประเมินทางเลือกเชิงยุทธศาสตร์ และพิจารณาความเสี่ยงในภาพรวม
ISO 31000:2018	ให้แนวทางด้านหลักการ กรอบ และกระบวนการบริหารความเสี่ยง	ใช้ออกแบบการกำหนดขอบเขต บริบท และเกณฑ์ การประเมินและจัดการความเสี่ยง การสื่อสาร การติดตาม และการทบทวน
หลักเกณฑ์กระทรวงการคลังด้านการควบคุมภายใน และ COSO Internal Control 2013	สนับสนุนการออกแบบ ดำเนินการ และประเมินการควบคุมภายใน โดยแยกสถานะของหลักเกณฑ์กับกรอบแนวปฏิบัติ	ประเมินความเหมาะสมของการออกแบบ การนำไปใช้ และประสิทธิผลของการควบคุม พร้อมจัดทำรายงานและแผนปรับปรุงตามข้อกำหนด
หลัก Three Lines และมาตรฐานการตรวจสอบภายในที่เกี่ยวข้อง	จัดวางความรับผิดชอบของผู้กำกับดูแล ฝ่ายบริหาร และการให้ความเชื่อมั่นอย่างเป็นอิสระ	กำหนดและประสานบทบาทของสายงานที่หนึ่ง สายงานที่สอง และกองตรวจสอบภายใน โดยรักษาความเป็นอิสระของการตรวจสอบ
ISO 22301:2019 และฉบับแก้ไขเพิ่มเติมที่มหาวิทยาลัยนำมาใช้	สนับสนุนระบบบริหารความต่อเนื่องขององค์กร	เชื่อมโยงความเสี่ยงกับ BIA ภารกิจสำคัญ เป้าหมายการฟื้นคืน แผน BCP ทรัพยากร และการทดสอบความพร้อม
Governance, Risk and Compliance: GRC	เชื่อมโยงการกำกับดูแล ความเสี่ยง และการปฏิบัติตามกฎเกณฑ์	เชื่อมโยงวัตถุประสงค์ ข้อกำหนด ความเสี่ยง การควบคุม ผู้รับผิดชอบ และข้อมูลการรายงาน เพื่อลดช่องว่างและความซ้ำซ้อน
เกณฑ์ EdPEx ฉบับที่มหาวิทยาลัยกำหนดใช้	สนับสนุนการบริหารองค์กรและการปรับปรุงผลการดำเนินงาน	ใช้ข้อมูลความเสี่ยงประกอบการนำองค์กร การวางแผน การบริหารบุคลากร การปฏิบัติการ และการประเมินผลลัพธ์

กรอบอ้างอิง	บทบาทในการประยุกต์ใช้	การนำมาใช้ในมหาวิทยาลัย
SDGs และแนวคิด ESG	สนับสนุนการพิจารณาความยั่งยืนและผลกระทบต่อผู้มีส่วนได้ส่วนเสีย	วิเคราะห์ปัจจัย ความเสี่ยง และโอกาสด้านสิ่งแวดล้อม สังคม และธรรมาภิบาลที่สัมพันธ์กับภารกิจและยุทธศาสตร์

<u>หลักการบูรณาการกรอบอ้างอิง</u>

มหาวิทยาลัยใช้แนวทาง “ระบบบริหารที่เชื่อมโยงกัน หลายกรอบอ้างอิง” (One Integrated System, Multiple Frameworks) โดยกำหนดให้

1. ใช้กระบวนการ คำศัพท์ เกณฑ์ และแบบฟอร์มกลางด้านการบริหารความเสี่ยง พร้อมกำหนดรายละเอียดเพิ่มเติมตามภารกิจและข้อกำหนดเฉพาะ
2. เชื่อมโยงข้อมูลวัตถุประสงค์ ความเสี่ยง การควบคุม ข้อกำหนด ตัวชี้วัด มาตรการ ผู้รับผิดชอบ และผลการให้ความเชื่อมั่น เพื่อให้ตรวจสอบย้อนกลับและใช้ข้อมูลร่วมกันได้
3. ประสานระบบข้อมูลและการรายงาน ลดการบันทึกซ้ำ โดยรักษาสิทธิการเข้าถึง ความลับ และเส้นทางรายงานเฉพาะตามกฎหมายหรือกฎบัตร
4. จัดทำตารางเทียบเคียงกรอบอ้างอิง (Framework Crosswalk) เพื่อแสดงความเชื่อมโยงระหว่างข้อกำหนด กระบวนการ ผู้รับผิดชอบ และหลักฐาน พร้อมระบุช่องว่างที่ต้องปรับปรุง
5. ประยุกต์ใช้ตามหลักความเหมาะสมตามสัดส่วน โดยคำนึงถึงภารกิจ ขนาด ความซับซ้อน และระดับความเสี่ยงของแต่ละส่วนงาน
6. ยึดข้อกำหนดที่มีผลใช้บังคับตามลำดับศักดิ์และขอบเขตอำนาจ ส่วนมาตรฐานและกรอบภายนอกให้ใช้ตามนโยบายและขอบเขตที่มหาวิทยาลัยกำหนด

การบูรณาการมุ่งให้ข้อมูล กระบวนการ และหลักฐานสนับสนุนกัน โดยไม่ลดทอนข้อกำหนดเฉพาะหรือความเป็นอิสระของผู้ให้ความเชื่อมั่น และไม่ถือเป็นการประกาศว่ามหาวิทยาลัยได้รับการรับรองตามมาตรฐานที่อ้างอิง

2.7 การประยุกต์ใช้กรอบ COSO ERM 2017

มหาวิทยาลัยประยุกต์ใช้กรอบ COSO Enterprise Risk Management—Integrating with Strategy and Performance (2017) ซึ่งประกอบด้วย 5 องค์ประกอบและ 20 หลักการ ตามที่อธิบายในหัวข้อ 1.6 โดยกำหนดแนวทางปฏิบัติและหลักฐานที่ใช้สนับสนุนแต่ละองค์ประกอบ ดังนี้

2.7.1 การกำกับดูแลและวัฒนธรรมองค์กร (Governance and Culture) ครอบคลุมหลักการที่ 1–5 ได้แก่ การกำกับดูแลความเสี่ยง การจัดโครงสร้างการดำเนินงาน การกำหนด

วัฒนธรรมที่พึงประสงค์ ความมุ่งมั่นต่อค่านิยมหลัก และการดึงดูด พัฒนา และรักษาบุคลากรที่มีความสามารถ

มหาวิทยาลัยนำมาประยุกต์ใช้โดย

- กำหนดบทบาทของสภามหาวิทยาลัย คณะกรรมการ ฝ่ายบริหาร และส่วนงานตามอำนาจหน้าที่ พร้อมกำกับติดตามความเพียงพอและประสิทธิผลของระบบ
- ระบุเจ้าของความเสี่ยง ผู้รับผิดชอบการควบคุม มาตรการ และข้อมูล รวมทั้งอำนาจตัดสินใจและเส้นทางรายงาน
- ส่งเสริมการรายงานโดยสุจริต ความรับผิดชอบตามบทบาท และการปฏิบัติตามค่านิยมและจริยธรรม
- พัฒนาความรู้และทักษะด้านความเสี่ยงตามหน้าที่ และติดตามพฤติกรรมกับผลการนำความรู้ไปใช้

หลักฐานประกอบ เช่น นโยบาย คำสั่ง กฎบัตร ตารางบทบาทและความรับผิดชอบ แผนพัฒนาบุคลากร และผลการประเมินวัฒนธรรมความเสี่ยง

2.7.2 ยุทธศาสตร์และการกำหนดวัตถุประสงค์ (Strategy and Objective-Setting)

ครอบคลุมหลักการที่ 6–9 ได้แก่ การวิเคราะห์บริบท การกำหนดระดับความเสี่ยงที่ยอมรับได้ การประเมินทางเลือกเชิงยุทธศาสตร์ และการกำหนดวัตถุประสงค์ มหาวิทยาลัยนำมาประยุกต์ใช้โดย

- วิเคราะห์บริบทภายในและภายนอก ผู้มีส่วนได้ส่วนเสีย แนวโน้ม และสมมติฐานที่มีผลต่อยุทธศาสตร์
- กำหนด RA และถ่ายทอดเป็นเกณฑ์ RT หรือเกณฑ์เชิงปฏิบัติที่ติดตามได้ ตามกระบวนการอนุมัติที่เกี่ยวข้อง
- เปรียบเทียบความเสี่ยง โอกาส ทรัพยากร และผลกระทบของทางเลือกก่อนตัดสินใจ
- กำหนดวัตถุประสงค์ เป้าหมาย ตัวชี้วัด และเจ้าของวัตถุประสงค์ให้ชัดเจน เพื่อใช้เป็นฐานในการระบุความเสี่ยง

หลักฐานประกอบ เช่น การวิเคราะห์บริบท แผนยุทธศาสตร์ การประเมินทางเลือก เอกสาร RA/RT ที่ได้รับอนุมัติ และบันทึกการตัดสินใจ

2.7.3 ผลการดำเนินงาน (Performance)

ครอบคลุมหลักการที่ 10–14 ได้แก่ การระบุความเสี่ยง การประเมินความรุนแรง การจัดลำดับความสำคัญ การตอบสนอง และการพัฒนามุมมองความเสี่ยงในภาพรวม

มหาวิทยาลัยนำมาประยุกต์ใช้โดย

- ระบุความเสี่ยงผ่านความสัมพันธ์ระหว่างสาเหตุ เหตุการณ์ และผลกระทบต่อวัตถุประสงค์

- ประเมินความเสี่ยงโดยธรรมชาติ การควบคุมที่มีอยู่ และความเสี่ยงคงเหลือ ณ วันที่ประเมิน พร้อมกำหนดเป้าหมายแยกต่างหาก
- จัดลำดับความสำคัญโดยพิจารณาคะแนน RA/RT เกณฑ์ยกระดับเป็นกรณีพิเศษ ความเร่งด่วน และความสำคัญเชิงยุทธศาสตร์
- เลือกแนวทางตอบสนองและจัดทำมาตรการ พร้อมผู้รับผิดชอบ ทรัพยากร กำหนดเวลา และหลักฐานที่ต้องส่งมอบ
- วิเคราะห์ความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัวของความเสี่ยง เพื่อเสนอประเด็นที่ต้องตัดสินใจระดับมหาวิทยาลัย โดยไม่ใช้การบวกคะแนนรายรายการแทนการวิเคราะห์ภาพรวม

หลักฐานประกอบ เช่น แบบ RISK-MJU-01 ทะเบียนความเสี่ยง ผลการทดสอบการควบคุม แผนบริหารความเสี่ยง และข้อมูลวิเคราะห์ความเสี่ยงในภาพรวม

2.7.4 การทบทวนและปรับปรุง (Review and Revision)

ครอบคลุมหลักการที่ 15–17 ได้แก่ การประเมินการเปลี่ยนแปลงสำคัญ การทบทวนความเสี่ยงและผลการดำเนินงาน และการปรับปรุง ERM มหาวิทยาลัยนำมาประยุกต์ใช้โดย

- ติดตามการเปลี่ยนแปลงด้านยุทธศาสตร์ กฎหมาย เทคโนโลยี ทรัพยากร โครงสร้าง และบริบทที่อาจเปลี่ยนสถานะความเสี่ยง
- เปรียบเทียบผลจริงกับวัตถุประสงค์ KPI KRI เกณฑ์ RA/RT และระดับความเสี่ยงเป้าหมาย
- ทบทวนประสิทธิผลของการควบคุมและมาตรการจากหลักฐาน โดยแยกความก้าวหน้าของกิจกรรมออกจากผลต่อความเสี่ยง
- นำเหตุการณ์ ข้อค้นพบ และบทเรียนมาปรับปรุงกรอบ เกณฑ์ กระบวนการ และความสามารถของบุคลากร พร้อมติดตามผลการแก้ไข

หลักฐานประกอบ เช่น รายงานติดตาม ทะเบียนความเสี่ยงฉบับทบทวน ผลการตรวจสอบ บทเรียนจากเหตุการณ์ และแผนปรับปรุงระบบ

2.7.5 สารสนเทศ การสื่อสาร และการรายงาน (Information, Communication, and Reporting)

ครอบคลุมหลักการที่ 18–20 ได้แก่ การใช้สารสนเทศและเทคโนโลยี การสื่อสารข้อมูลความเสี่ยง และการรายงานความเสี่ยง วัฒนธรรม และผลการดำเนินงาน มหาวิทยาลัยนำมาประยุกต์ใช้โดย

- กำหนดนิยาม แหล่งข้อมูล เจ้าของข้อมูล สิทธิการเข้าถึง และแนวทางตรวจสอบคุณภาพข้อมูล

- สื่อสารนโยบาย บทบาท เกณฑ์ และแนวทางตอบสนองให้ผู้เกี่ยวข้องเข้าใจและนำไปใช้ได้
- รายงานสถานะ แนวโน้ม เหตุการณ์ ประสิทธิผลของการควบคุม ความก้าวหน้าของมาตรการ และประเด็นที่ต้องตัดสินใจ
- จัดให้มีการรายงานตามรอบและการยกระดับรายงานเมื่อเข้าเกณฑ์ พร้อมบันทึกข้อจำกัดของข้อมูลและผลการตัดสินใจ

หลักฐานประกอบ เช่น นิยามตัวชี้วัด รายงานหรือ Dashboard บันทึกการสื่อสาร รายงานเหตุการณ์ และบันทึกการตัดสินใจ

หลักการนำไปประยุกต์ใช้

องค์ประกอบทั้ง 5 และหลักการทั้ง 20 ต้องใช้เชื่อมโยงกันตามบริบท โดยหลักฐานหนึ่งรายการอาจสนับสนุนได้หลายหลักการ

2.8 การประยุกต์ใช้หลักการบริหารความเสี่ยงตาม ISO 31000:2018

มหาวิทยาลัยนำหลักการ 8 ประการตามหัวข้อ 1.7 มาใช้ในการออกแบบ ดำเนินงาน และปรับปรุงระบบ เพื่อสนับสนุนการสร้างและคุ้มครองคุณค่า โดยมีแนวทางดังนี้

ตารางที่ 2-3 ตารางแสดงหลักการ ISO 31000:2018 และแนวทางการประยุกต์ใช้ของมหาวิทยาลัย

หลักการ	แนวทางการประยุกต์ใช้
บูรณาการ (Integrated)	ใช้ข้อมูลความเสี่ยงประกอบการกำหนดยุทธศาสตร์ แผน งบประมาณ โครงการ และการตัดสินใจ พร้อมกำหนดความรับผิดชอบในกระบวนการทำงาน
มีโครงสร้างและครอบคลุม (Structured and Comprehensive)	ใช้กระบวนการ คำศัพท์ เกณฑ์ และแบบฟอร์มที่สอดคล้องกัน ครอบคลุมความเสี่ยงสำคัญและความสัมพันธ์ระหว่างรายการ เพื่อให้ติดตามและเปรียบเทียบได้โดยคำนึงถึงบริบท
เหมาะสมกับบริบท (Customized)	ปรับรายละเอียด วิธีประเมิน และเครื่องมือตามวัตถุประสงค์ ภารกิจ ขนาด ความซับซ้อน และระดับความเสี่ยง โดยรักษาข้อกำหนดขั้นต่ำ
มีส่วนร่วม (Inclusive)	ให้ผู้เกี่ยวข้องและผู้มีส่วนได้ส่วนเสียร่วมให้ข้อมูล ประเมินทางเลือก และพิจารณาผลกระทบอย่างเหมาะสมและทันเวลา
มีพลวัต (Dynamic)	ติดตามบริบท ความเสี่ยงเกิดใหม่ KRI และ EWS พร้อมทบทวนความเสี่ยงและมาตรการเมื่อเกิดการเปลี่ยนแปลงสำคัญควบคู่กับรอบปกติ
ใช้สารสนเทศที่ดีที่สุดเท่าที่มี (Best Available Information)	ใช้ข้อมูลย้อนหลัง ปัจจุบัน การคาดการณ์ และความเห็นผู้เชี่ยวชาญ พร้อมระบุแหล่งข้อมูล คุณภาพ สมมติฐาน และข้อจำกัด

หลักการ	แนวทางการประยุกต์ใช้
คำนึงถึงปัจจัยมนุษย์และวัฒนธรรม (Human and Cultural Factors)	พิจารณาค่านิยม พฤติกรรม ทักษะ แรงจูงใจ อคติ และการสื่อสาร พร้อมส่งเสริมความรับผิดชอบและการรายงานโดยสุจริต
ปรับปรุงอย่างต่อเนื่อง (Continual Improvement)	ใช้ผลการติดตาม เหตุการณ์ ข้อร้องเรียน ผลตรวจสอบ การทดสอบแผน และบทเรียนมาปรับปรุงระบบ พร้อมกำหนดผู้รับผิดชอบและติดตามผล

หลักการ ISO 31000 และองค์ประกอบ COSO ERM ใช้สนับสนุนการออกแบบและประเมินคุณภาพของระบบ ส่วนกระบวนการปฏิบัติของมหาวิทยาลัยเป็นแนวทางดำเนินงานที่อธิบายไว้ในส่วนที่ 4 ให้ส่วนงานประยุกต์ใช้ร่วมกัน โดยเชื่อมโยงข้อมูลและหลักฐานตลอดกระบวนการ

2.9 ความเชื่อมโยงกับแผนยุทธศาสตร์มหาวิทยาลัย

มหาวิทยาลัยกำหนดให้การบริหารความเสี่ยงเชื่อมโยงกับการบริหารยุทธศาสตร์ ตั้งแต่การวิเคราะห์บริบท การกำหนดทางเลือก การนำแผนไปปฏิบัติ การติดตามผล และการทบทวน เพื่อให้ข้อมูลความเสี่ยงและโอกาสสนับสนุนการบรรลุเป้าประสงค์และการตัดสินใจ โดยมีแนวทางดังต่อไปนี้

1. **เชื่อมโยงความเสี่ยงกับวัตถุประสงค์และผลลัพธ์** ความเสี่ยงแต่ละรายการต้องระบุวัตถุประสงค์ เป้าประสงค์เชิงยุทธศาสตร์ ตัวชี้วัด หรือพันธกิจที่อาจได้รับผลกระทบ พร้อมอธิบายความเชื่อมโยงให้สามารถประเมินและติดตามได้
2. **พิจารณาความเสี่ยงตั้งแต่ขั้นกำหนดยุทธศาสตร์** การจัดทำหรือทบทวนแผนยุทธศาสตร์ต้องวิเคราะห์บริบท ผู้มีส่วนได้ส่วนเสีย สมมติฐาน ความเสี่ยง และโอกาสของทางเลือกต่าง ๆ โดยพิจารณาความสามารถในการรองรับความเสี่ยง (Risk Capacity) และกรอบ RA/RT ที่เกี่ยวข้องก่อนตัดสินใจ
3. **ประเมินความเสี่ยงก่อนอนุมัตินโยบายและโครงการสำคัญ** ข้อเสนอนโยบาย โครงการ การลงทุน หรือภาระผูกพันที่มีนัยสำคัญต้องแสดงความเสี่ยง ความคุ้มค่า ความพร้อมด้านทรัพยากร ข้อจำกัดตามกฎหมาย และผลกระทบต่อผู้มีส่วนได้ส่วนเสีย รวมทั้งความเสี่ยงที่อาจเพิ่มขึ้นหรือกระจุกตัวในภาพรวม เพื่อประกอบการพิจารณาของผู้มีอำนาจ
4. **กำหนดผู้รับผิดชอบและเกณฑ์ติดตาม** วัตถุประสงค์เชิงยุทธศาสตร์และโครงการสำคัญต้องมีเจ้าของวัตถุประสงค์และเจ้าของความเสี่ยงที่ชัดเจน พร้อมกำหนด KPI KRI เกณฑ์ที่ถ่ายทอดจาก RA/RT มาตรการตอบสนอง และเส้นทางรายงานตามความเหมาะสม ทั้งนี้ ไม่จำเป็นต้องกำหนดตัวชี้วัดใหม่หากข้อมูลที่มีอยู่สามารถใช้ติดตามความเสี่ยงได้อย่างเพียงพอ

5. พิจารณาความเสี่ยงในภาพรวมของมหาวิทยาลัย ความเสี่ยงที่กระทบหลายส่วนงาน มีความสัมพันธ์หรือการกระจุกตัวอย่างมีนัยสำคัญ เกินอำนาจจัดการของส่วนงาน หรือกระทบเป้าประสงค์และพันธกิจสำคัญ ต้องเสนอให้พิจารณาร่วมกันในระดับมหาวิทยาลัย การบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัย (University-level/Enterprise Risk) ให้ผ่านกระบวนการกลั่นกรองและพิจารณาตามอำนาจ โดยไม่ถือว่าการเกิน RT หรือคะแนนสูงทำให้เปลี่ยนเป็นความเสี่ยงระดับมหาวิทยาลัยโดยอัตโนมัติ

6. ติดตามความเสี่ยงควบคู่กับผลการดำเนินงาน รายงานผลยุทธศาสตร์ต้องเชื่อมโยงผลตาม KPI กับแนวโน้ม KRI สถานะเทียบ RA/RT ระดับความเสี่ยงคงเหลือ ประสิทธิผลของการควบคุมและผลการดำเนินมาตรการ พร้อมระบุปัญหาและประเด็นที่ต้องตัดสินใจ

7. ใช้ผลการติดตามปรับการดำเนินงานและการตัดสินใจ เมื่อผลการดำเนินงานเบี่ยงเบนจากเป้าหมาย KRI เข้าใกล้หรือเกินเกณฑ์ สมมติฐานเปลี่ยนแปลง หรือการควบคุมไม่เพียงพอ ให้เจ้าของวัตถุประสงค์และเจ้าของความเสี่ยงร่วมวิเคราะห์สาเหตุและทางเลือก เพื่อปรับแผน มาตรการหรือทรัพยากร และยกระดับรายงานตามเกณฑ์ โดยบันทึกเหตุผลและผลการตัดสินใจ

8. ทบทวนยุทธศาสตร์และความเสี่ยงร่วมกัน ทบทวนความสอดคล้องระหว่างยุทธศาสตร์ผลการดำเนินงาน และภาพรวมความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อบริบทเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งพิจารณาว่ายุทธศาสตร์และระดับความเสี่ยงที่ยอมรับได้ยังเหมาะสมกับทรัพยากรและความสามารถของมหาวิทยาลัยหรือไม่

การเชื่อมโยงข้อมูลให้ใช้รหัสหรือรายการอ้างอิงระหว่างเป้าประสงค์ ตัวชี้วัด แผนงานโครงการ และทะเบียนความเสี่ยง เพื่อให้ตรวจสอบย้อนกลับได้ และใช้ประกอบการติดตามผลในระดับส่วนงานและระดับมหาวิทยาลัย

2.10 ความเชื่อมโยงกับการควบคุมภายในและการให้ความเชื่อมั่น

การบริหารความเสี่ยงช่วยระบุและประเมินความไม่แน่นอนที่อาจส่งผลต่อวัตถุประสงค์ ส่วนการควบคุมภายในเป็นกระบวนการที่ผู้กำกับดูแล ฝ่ายบริหาร และบุคลากรร่วมดำเนินการผ่านนโยบาย ระบบ และกิจกรรม เพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลต่อวัตถุประสงค์ด้านการดำเนินงาน การรายงาน และการปฏิบัติตามข้อกำหนด การให้ความเชื่อมั่นช่วยประเมินความเพียงพอและประสิทธิผลของระบบดังกล่าวจากหลักฐานตามขอบเขตที่กำหนด

มหาวิทยาลัยใช้แนวทางความเสี่ยง–การควบคุม–การให้ความเชื่อมั่น (Risk–Control–Assurance) โดยเชื่อมโยงวัตถุประสงค์ ความเสี่ยง การควบคุม ผู้รับผิดชอบ หลักฐาน ผลการประเมินความเสี่ยงคงเหลือ และข้อค้นพบจากการให้ความเชื่อมั่น เพื่อนำไปปรับปรุงและสนับสนุนการตัดสินใจอย่างต่อเนื่อง

2.10.1 การประเมินการควบคุม

ให้เจ้าของความเสี่ยงและเจ้าของการควบคุมประเมินการควบคุมที่เกี่ยวข้องอย่างน้อย 3 มิติ ดังนี้

มิติการประเมิน	ประเด็นที่ต้องพิจารณา
ความเหมาะสมของการออกแบบ (Design Adequacy)	การควบคุมตอบสนองต่อสาเหตุหรือผลกระทบได้เพียงพอหรือไม่ มีผู้รับผิดชอบ ขอบเขต ขั้นตอน ความถี่ เกณฑ์การปฏิบัติ และหลักฐานที่ชัดเจนหรือไม่
การนำไปใช้ (Implementation)	มีการนำการควบคุมไปใช้จริงตามขอบเขตหรือไม่ ครอบคลุมหน่วยงาน กระบวนการ ระบบ และผู้เกี่ยวข้องตามที่กำหนดหรือไม่
ประสิทธิผลในการปฏิบัติงาน (Operating Effectiveness)	การควบคุมทำงานถูกต้อง สม่ำเสมอ และทันเวลาตลอดช่วงที่ประเมินหรือไม่ สามารถป้องกัน ลด ตรวจจับ หรือตอบสนองต่อความเสี่ยงได้ตามวัตถุประสงค์หรือไม่

ผลการประเมินต้องมีหลักฐานที่เพียงพอและตรวจสอบย้อนกลับได้ เช่น เอกสารอนุมัติ บันทึกการปฏิบัติงาน รายงานระบบ ผลการทดสอบ ตัวอย่างรายการ และข้อมูลข้อยกเว้นหรือข้อบกพร่อง พร้อมระบุช่วงเวลา ขอบเขต วิธีการ และข้อจำกัดของการประเมิน

การมีนโยบาย คู่มือ หรือคำสั่งเพียงอย่างเดียวไม่เพียงพอที่จะสรุปว่าการควบคุมมีประสิทธิผล หากการออกแบบไม่เหมาะสม ยังไม่ได้นำไปใช้ หรือไม่มีหลักฐานยืนยันการทำงาน ให้ประเมินความเสี่ยงคงเหลือตามข้อเท็จจริงอย่างระมัดระวัง และกำหนดมาตรการปรับปรุง ผู้รับผิดชอบ กำหนดเวลา และวิธีตรวจสอบผล

การลดระดับความเสี่ยงคงเหลือต้องอาศัยหลักฐานว่าการควบคุมช่วยเปลี่ยนโอกาสเกิดหรือผลกระทบ ไม่ใช้การหักคะแนนประสิทธิผลของการควบคุมออกจากคะแนน L × I โดยตรง ส่วนมาตรการที่ยังไม่ดำเนินการหรือยังไม่ยืนยันประสิทธิผลให้ใช้ประกอบการกำหนดความเสี่ยงคงเหลือเป้าหมาย และแยกจากผลประเมินปัจจุบัน

2.10.2 การให้ความเชื่อมั่นและความเป็นอิสระของการตรวจสอบภายใน

ฝ่ายบริหารรับผิดชอบจัดการความเสี่ยงและการควบคุม สายงานที่สองสนับสนุน ติดตาม และสอบทานตามหน้าที่ ส่วนกองตรวจสอบภายในให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรม ครอบคลุมการดำเนินงานของสายงานที่หนึ่งและสายงานที่สองตามกฎบัตรและแผนตรวจสอบที่เกี่ยวข้อง

กองตรวจสอบภายในสามารถให้ข้อเสนอแนะเกี่ยวกับกรอบ เกณฑ์ และแนวทางปรับปรุงได้ โดยต้องไม่รับผิดชอบแทนฝ่ายบริหารในการ

1. เป็นเจ้าของความเสี่ยงหรือเจ้าของการควบคุม
2. อนุมัติ RA/RT หรือยอมรับความเสี่ยง

3. ตัดสินใจเลือกหรือดำเนินมาตรการควบคุม
4. รับรองผลการบริหารความเสี่ยงในฐานะผู้รับผิดชอบดำเนินงาน

หากมีภารกิจเพิ่มเติมที่อาจกระทบต่อความเป็นอิสระหรือความเที่ยงธรรม ให้เปิดเผยต่อผู้มีหน้าที่กำกับดูแลการตรวจสอบภายใน และพิจารณาตามกฎบัตรและมาตรฐานที่เกี่ยวข้องก่อนรับภารกิจ โดยกำหนดขอบเขต ระยะเวลา สายการรายงาน และมาตรการคุ้มครองให้ชัดเจน พร้อมจัดให้มีการให้ความเชื่อมั่นจากผู้ที่เป็นอิสระสำหรับงานที่กองตรวจสอบภายในมีส่วนรับผิดชอบ ทั้งนี้ การอนุมัติภารกิจเพียงอย่างเดียวไม่ทดแทนมาตรการคุ้มครองดังกล่าว

2.10.3 การประสานและจัดทำแผนผังการให้ความเชื่อมั่น

ให้หน่วยงานบริหารความเสี่ยงประสานเจ้าของความเสี่ยง หน่วยงานในสายงานที่สอง กองตรวจสอบภายใน และผู้ให้ความเชื่อมั่นอื่น เพื่อจัดทำแผนผังการให้ความเชื่อมั่น (Assurance Map) สำหรับความเสี่ยงสำคัญระดับมหาวิทยาลัย โดยระบุอย่างน้อยดังนี้

1. วัตถุประสงค์ ความเสี่ยง และการควบคุมสำคัญ
2. เจ้าของความเสี่ยงและเจ้าของการควบคุม
3. หน่วยงานติดตามหรือสอบทานในสายงานที่สอง
4. แหล่งความเชื่อมั่นจากการตรวจสอบภายในและผู้ประเมินภายนอก
5. ขอบเขต เกณฑ์ วิธีการ และความถี่ของการประเมิน
6. ระดับความเป็นอิสระและข้อจำกัดของแหล่งความเชื่อมั่น
7. ข้อค้นพบ ช่องว่าง ความซ้ำซ้อน และผู้รับผิดชอบปรับปรุง

การประสานงานดังกล่าวไม่เปลี่ยนอำนาจอนุมัติแผนตรวจสอบหรือความรับผิดชอบของผู้ให้ความเชื่อมั่นแต่ละราย และต้องพิจารณาความน่าเชื่อถือของหลักฐานก่อนนำผลการประเมินมาใช้ร่วมกัน

ให้ส่วนงานประยุกต์ใช้ตามหลักความเหมาะสมตามสัดส่วน (Proportionality) โดยใช้ข้อมูลและหลักฐานจากการดำเนินงานที่มีอยู่ เชื่อมโยงกับแบบฟอร์มและระบบกลาง และเพิ่มรายละเอียดเฉพาะที่จำเป็นต่อการประเมินและการตัดสินใจ

2.11 ความเชื่อมโยงกับการพัฒนาองค์กรสู่ความเป็นเลิศ

มหาวิทยาลัยเชื่อมโยงการบริหารความเสี่ยงกับการพัฒนาองค์กรตามเกณฑ์คุณภาพการศึกษาเพื่อการดำเนินการที่เป็นเลิศ (Education Criteria for Performance Excellence: EdPEx) ฉบับที่มหาวิทยาลัยกำหนดใช้ โดยนำข้อมูลความเสี่ยงและโอกาสมาสนับสนุนการวางแผน การดำเนินงาน การเรียนรู้ และการปรับปรุงผลลัพธ์ ดังนี้

ตารางที่ 2-4 ***ตารางแสดงความเชื่อมโยงการบริหารความเสี่ยงกับการพัฒนาองค์กรตามเกณฑ์คุณภาพการศึกษาเพื่อการดำเนินการที่เป็นเลิศ (Education Criteria for Performance Excellence: EdPEx)***

องค์ประกอบ	แนวทางเชื่อมโยงการบริหารความเสี่ยง
1) **โครงร่างองค์กรและบริบท**	ใช้ข้อมูลพันธกิจ สภาพแวดล้อม ความสัมพันธ์กับผู้เกี่ยวข้อง ความท้าทาย ความได้เปรียบเชิงยุทธศาสตร์ และข้อจำกัด เป็นฐานในการระบุความเสี่ยงและโอกาส
2) **การนำองค์กร**	ใช้ข้อมูลความเสี่ยงประกอบการกำหนดทิศทาง การกำกับดูแล การส่งเสริมจริยธรรม และการติดตามความรับผิดชอบต่อผลลัพธ์ พร้อมสนับสนุนการรายงานข้อกังวลโดยสุจริต
3) **ยุทธศาสตร์**	พิจารณาความเสี่ยง โอกาส สมมติฐาน และกรอบ RA/RT ในการเลือกยุทธศาสตร์ กำหนดวัตถุประสงค์ จัดทำแผนปฏิบัติการ และจัดสรรทรัพยากร
4) **ผู้เรียนและลูกค้ากลุ่มอื่น**	ประเมินความเสี่ยงต่อการตอบสนองความต้องการ การเข้าถึงและคุณภาพบริการ ประสบการณ์ ความพึงพอใจ ความผูกพัน และความเชื่อมั่น โดยใช้ข้อมูลรับฟังและข้อร้องเรียนประกอบ
5) **การวัด การวิเคราะห์และการจัดการความรู้**	เชื่อมโยง KPI KRI และ EWS กับข้อมูลการควบคุมและผลการดำเนินมาตรการ พร้อมตรวจสอบคุณภาพข้อมูล วิเคราะห์แนวโน้ม และถ่ายทอดบทเรียนเพื่อสนับสนุนการตัดสินใจ
6) **บุคลากร**	ประเมินความเสี่ยงด้านกำลังคน สมรรถนะ ความผูกพัน สุขภาวะ ความปลอดภัย การสืบทอดตำแหน่ง และความพร้อมต่อการเปลี่ยนแปลง พร้อมติดตามผลของมาตรการพัฒนา
7) **การปฏิบัติการ**	เชื่อมโยงความเสี่ยงกับการออกแบบและบริหารกระบวนการสำคัญ การควบคุม ผู้ส่งมอบและคู่ความร่วมมือ เทคโนโลยี ความปลอดภัย และความต่อเนื่องของการดำเนินงาน
8) **ผลลัพธ์**	ใช้ผลการดำเนินงานและแนวโน้มความเสี่ยงร่วมกัน เพื่อประเมินการบรรลุวัตถุประสงค์ ประสิทธิผลของการควบคุม ความเชื่อมั่นของผู้เกี่ยวข้อง และความยั่งยืน พร้อมพิจารณาข้อมูลเปรียบเทียบที่เหมาะสม

ส่วนงานต้องนำข้อมูลความเสี่ยงและโอกาสมาใช้ในการทบทวนผลการดำเนินงาน วิเคราะห์ช่องว่าง และกำหนดการปรับปรุง โดยระบุผู้รับผิดชอบ กำหนดเวลา และผลลัพธ์ที่ต้องการ พร้อมติดตามว่าการปรับปรุงช่วยเพิ่มคุณภาพ ลดความเสี่ยง หรือเสริมความพร้อมได้เพียงใด

ให้ใช้ข้อมูลและหลักฐานจากระบบงานปกติร่วมกันระหว่างการบริหารความเสี่ยงและการประเมินคุณภาพ เช่น แผนงาน รายงานผล ตัวชี้วัด ข้อร้องเรียน ผลการทดสอบ และบันทึกการตัดสินใจ โดยเชื่อมโยงแหล่งอ้างอิงให้ตรวจสอบย้อนกลับได้ ทั้งนี้ การจัดทำแผนหรือดำเนินกิจกรรมครบถ้วนต้องมีหลักฐานผลลัพธ์ประกอบ จึงจะใช้สรุปประสิทธิผลของการพัฒนาได้อย่างเหมาะสม

2.12 ความเชื่อมโยงกับ ESG และการพัฒนาอย่างยั่งยืน

มหาวิทยาลัยกำหนดให้การบริหารความเสี่ยงพิจารณาปัจจัยและผลกระทบด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (Environmental, Social and Governance: ESG) ที่เกี่ยวข้องกับยุทธศาสตร์ พันธกิจ และการดำเนินงาน โดยพิจารณาทั้งผลกระทบต่อมหาวิทยาลัยและผลกระทบจากการดำเนินงานของมหาวิทยาลัยต่อผู้มีส่วนได้ส่วนเสียและสิ่งแวดล้อม

ตารางที่ 2-5 ***ตารางแสดงมิติ ESG และประเด็นที่ควรพิจารณาในการบริหารความเสี่ยง***

มิติ	ประเด็นที่ควรพิจารณา
สิ่งแวดล้อม (Environmental: E)	ความเสี่ยงจากสภาพภูมิอากาศและภัยพิบัติ ความเสี่ยงจากการเปลี่ยนผ่านด้านนโยบาย เทคโนโลยี และความต้องการของสังคม ความหลากหลายทางชีวภาพ การใช้พลังงาน น้ำ และทรัพยากร มลพิษ ของเสีย และผลกระทบจากการศึกษา การวิจัย และการดำเนินงานต่อสิ่งแวดล้อม
สังคม (Social: S)	สุขภาพ ความปลอดภัย สิทธิมนุษยชน ความเสมอภาค การไม่เลือกปฏิบัติ การป้องกันการคุกคาม ความเป็นอยู่ของนักศึกษาและบุคลากร การเข้าถึงการศึกษาและบริการ ความสัมพันธ์กับชุมชน และผลกระทบต่อกลุ่มเปราะบาง
ธรรมาภิบาล (Governance: G)	โครงสร้างและความรับผิดชอบในการกำกับดูแล จริยธรรม ความโปร่งใส การป้องกันการทุจริตและผลประโยชน์ทับซ้อน การปฏิบัติตามข้อกำหนด การคุ้มครองข้อมูล การกำกับดูแล AI และความน่าเชื่อถือของข้อมูลที่ใช้ตัดสินใจและรายงาน

2.12.1 การเชื่อมโยง ESG กับประเภทความเสี่ยง

ให้ใช้ ESG เป็นมิติประกอบการวิเคราะห์สาเหตุและผลกระทบ รวมทั้งเป็นป้ายกำกับข้ามประเภทความเสี่ยง (Cross-cutting Tag) โดยจำแนกประเภทหลักเป็น S O F C หรือ D ตามลักษณะของแต่ละประเด็น และใช้ทะเบียนความเสี่ยงกลางเพื่อเชื่อมโยงข้อมูล

รหัส **S** ในประเภทความเสี่ยงหมายถึง **Strategic Risk** ส่วน **S** ใน ESG หมายถึง **Social** ให้ระบุบริบทหรือใช้ป้ายกำกับ ESG-E, ESG-S และ ESG-G เพื่อป้องกันความสับสน

หากประเด็น ESG มีความสำคัญจนต้องบริหารแยกเป็นรายการ ให้ระบุวัตถุประสงค์ สาเหตุ เหตุการณ์ ผลกระทบ ประเภทหลัก และเจ้าของความเสี่ยง พร้อมกำหนด KRI เกณฑ์ที่สัมพันธ์กับ RA/RT มาตรการ หลักฐาน และเส้นทางรายงาน โดยหลีกเลี่ยงการบันทึกประเด็นเดียวกันซ้ำในหลายทะเบียน

2.12.2 การพิจารณาความสำคัญของประเด็น ESG

ให้มหาวิทยาลัยและส่วนงานพิจารณาอย่างน้อยดังต่อไปนี้

1. **ขนาดและความรุนแรงของผลกระทบ** รวมถึงผลกระทบสะสมและความเสียหายที่อาจไม่สามารถฟื้นคืนได้

2. **โอกาสเกิดและกรอบเวลา** ทั้งผลกระทบระยะสั้น ระยะกลาง และระยะยาว

3. **ขอบเขตของผู้ได้รับผลกระทบ** จำนวน กลุ่มเปราะบาง และความสามารถในการหลีกเลี่ยงหรือรับมือกับผลกระทบ

4. **ข้อกำหนดและพันธกรณี** กฎหมาย สัญญา นโยบาย และข้อผูกพันของมหาวิทยาลัยที่เกี่ยวข้อง

5. **ความต้องการและข้อกังวลของผู้มีส่วนได้ส่วนเสีย** โดยใช้ข้อมูลรับฟัง ข้อร้องเรียน และหลักฐานที่เหมาะสม

6. **ผลต่อมหาวิทยาลัยและพันธกิจ** ยุทธศาสตร์ คุณภาพการศึกษา การวิจัย การเงิน ชื่อเสียง และความต่อเนื่อง

7. **ความสามารถในการป้องกัน แก้ไข และเยียวยา** รวมถึงทรัพยากร ระยะเวลา และข้อจำกัดในการฟื้นฟู

2.12.3 การตอบสนองและติดตามผล

ประเด็น ESG ที่เข้าเกณฑ์สำคัญต้องมีมาตรการที่ตอบสนองต่อสาเหตุและผลกระทบ พร้อมผู้รับผิดชอบ กำหนดเวลา ตัวชี้วัด และหลักฐานผลการดำเนินงาน หากเข้าเกณฑ์เหตุที่ไม่ยอมรับหรือเกิดอันตรายร้ายแรง ให้ดำเนินการคุ้มครองผู้ได้รับผลกระทบและยกระดับรายงานทันทีตามแนวทางที่เกี่ยวข้อง โดยไม่รอรอบรายงานปกติ

การรายงานให้แสดงผลที่เกิดขึ้นจริง แนวโน้ม ข้อจำกัด และประเด็นที่ยังต้องปรับปรุง พร้อมเชื่อมโยงกับเป้าหมายความยั่งยืนที่มหาวิทยาลัยกำหนด โดยใช้ข้อมูลที่ตรวจสอบย้อนกลับได้และไม่สรุปผลสำเร็จเกินกว่าหลักฐานรองรับ

2.13 แนวปฏิบัติขั้นต่ำด้านการบริหารความเสี่ยง

ทุกส่วนงานต้องดำเนินการตามแนวปฏิบัติขั้นต่ำต่อไปนี้ โดยใช้หลักความเหมาะสมตามสัดส่วน (Proportionality) ให้สอดคล้องกับภารกิจ ขนาด ความซับซ้อน และระดับความเสี่ยง พร้อมใช้แบบ RISK-MJU-01 และทะเบียนความเสี่ยงเป็นหลักฐานเชื่อมโยงข้อมูล ทั้งนี้ รายการต่อไปนี้เป็นข้อกำหนดขั้นต่ำในการดำเนินงาน ให้ใช้ร่วมกับกระบวนการบริหารความเสี่ยงที่อธิบายในส่วนที่ 4

2.13.1 ข้อกำหนดขั้นต่ำในการดำเนินงาน

1. **กำหนดวัตถุประสงค์ ขอบเขต และบริบท** ระบุวัตถุประสงค์ ผลลัพธ์ เป้าหมายหรือตัวชี้วัด เจ้าของวัตถุประสงค์ ขอบเขตและกรอบเวลา พร้อมวิเคราะห์บริบทภายในและภายนอก ผู้มีส่วนได้ส่วนเสีย ข้อกำหนด และสมมติฐานที่เกี่ยวข้อง

2. **ระบุความเสี่ยงและผู้รับผิดชอบ** เขียนข้อความความเสี่ยงตามโครงสร้างสาเหตุ–เหตุการณ์–ผลกระทบ (Cause–Event–Impact) เชื่อมโยงกับวัตถุประสงค์ จำแนกประเภทหลัก S O F C หรือ D พร้อมระบุประเภทและมิติผลกระทบที่เกี่ยวข้อง และกำหนดเจ้าของความเสี่ยงให้ชัดเจน

3. ประเมินความเสี่ยงโดยธรรมชาติ ประเมินโอกาสเกิดและผลกระทบก่อนพิจารณาผลของการควบคุม โดยใช้เกณฑ์กลางและกรอบเวลาที่กำหนด พร้อมบันทึกข้อมูล หลักฐาน และสมมติฐานที่รองรับคะแนน

4. ระบุและประเมินการควบคุมที่มีอยู่ ระบุการควบคุม เจ้าของการควบคุม ขอบเขต ความถี่ และหลักฐาน พร้อมประเมินความเหมาะสมของการออกแบบ การนำไปใช้ และประสิทธิผลในการปฏิบัติงานตามหัวข้อ 2.10

5. ประเมินความเสี่ยงคงเหลือ ณ วันที่ประเมิน ประเมินจากผลของการควบคุมที่นำไปใช้และมีหลักฐานยืนยันการทำงานจริง หากหลักฐานไม่เพียงพอให้ระบุข้อจำกัดและประเมินอย่างระมัดระวัง โดยไม่ใช้มาตรการที่ยังอยู่ระหว่างวางแผนเป็นเหตุลดคะแนนปัจจุบัน

6. เปรียบเทียบกับกรอบการยอมรับและเลือกแนวทางตอบสนอง พิจารณาความเสี่ยงคงเหลือร่วมกับ RA/RT เกณฑ์ยกระดับเป็นกรณีพิเศษ กฎหมาย และขอบเขตอำนาจ แล้วเลือกแนวทางตอบสนอง พร้อมจัดทำแผนสำหรับความเสี่ยงที่เกินเกณฑ์หรือจำเป็นต้องปรับปรุง การยอมรับความเสี่ยงต้องมีผู้มีอำนาจพิจารณาและบันทึกเหตุผล เงื่อนไข และการติดตาม

7. กำหนดมาตรการและความเสี่ยงคงเหลือเป้าหมาย ระบุมาตรการ เจ้าของมาตรการ ทรัพยากร กำหนดเวลา ผลส่งมอบ และวิธีตรวจสอบประสิทธิผล พร้อมกำหนด Target Residual Risk และสมมติฐานรองรับ โดยแยกจากความเสี่ยงคงเหลือปัจจุบัน

8. กำหนดตัวชี้วัดและเงื่อนไขการดำเนินการ กำหนด KRI ที่สัมพันธ์กับความเสี่ยง โดยระบุนิยาม สูตรคำนวณ หน่วยวัด แหล่งข้อมูล เจ้าของข้อมูล ความถี่ และค่าฐาน รวมทั้งค่าเกณฑ์ที่ถ่ายทอดจาก RA ขอบเขต RT ช่วงเฝ้าระวัง และ Trigger/Action พร้อมผู้รับผิดชอบและเวลาตอบสนอง โดยช่วงค่าเกณฑ์ต้องไม่ทับซ้อนหรือมีช่องว่าง

9. ดำเนินมาตรการและติดตามตามระดับความเสี่ยง ดำเนินการควบคุมและมาตรการตามแผน ติดตามสถานะความเสี่ยงอย่างน้อยรายไตรมาส สำหรับความเสี่ยงระดับสูงมากให้ยกระดับรายงานทันทีเมื่อพบและติดตามอย่างน้อยรายเดือน หรือถี่ขึ้นตามสถานการณ์ เกณฑ์เฉพาะ หรือคำสั่งของผู้มีอำนาจ การติดตามดังกล่าวให้เชื่อมโยงกับรายงานรอบ 6 9 และ 12 เดือนตามที่มหาวิทยาลัยกำหนด

10. ตอบสนองและรายงานเหตุสำคัญทันที เมื่อเกิดเหตุที่ไม่ยอมรับ เหตุวิกฤต หรือเหตุที่อาจกระทบชีวิต ความปลอดภัย พันธกิจสำคัญ กฎหมาย ข้อมูล หรือผู้มีส่วนได้ส่วนเสียอย่างรุนแรง ให้ควบคุมผลกระทบและรายงานตามช่องทางและระยะเวลาที่กำหนด โดยไม่รอรอบรายงานปกติหรือผลการวิเคราะห์สาเหตุ

11. ทบทวนเมื่อบริบทหรือผลการดำเนินงานเปลี่ยนแปลง ทบทวนความเสี่ยงและการควบคุมเมื่อวัตถุประสงค์ ยุทธศาสตร์ กฎหมาย โครงสร้าง บุคลากร เทคโนโลยี ระบบงาน ผู้ให้บริการ

หรือสมมติฐานสำคัญเปลี่ยนแปลง รวมทั้งเมื่อเกิดเหตุการณ์ ข้อบกพร่อง หรือผลการดำเนินงานที่บ่งชี้ว่าการประเมินเดิมอาจไม่เหมาะสม

12. จัดเก็บหลักฐาน ยกระดับ และปรับปรุงอย่างต่อเนื่อง จัดเก็บหลักฐานการประเมิน การอนุมัติ การยอมรับความเสี่ยง การดำเนินมาตรการ และผลการติดตามให้ตรวจสอบย้อนกลับได้ตามข้อกำหนด เมื่อ KRI เกิน RT การควบคุมสำคัญไม่ทำงาน มาตรการล่าช้า หรือความเสี่ยงเพิ่มขึ้นอย่างมีนัยสำคัญ ให้วิเคราะห์สาเหตุ กำหนดการแก้ไข และยกระดับตามเกณฑ์ พร้อมติดตามผลจนได้ข้อยุติ

2.13.2 เกณฑ์ระดับความเสี่ยงและการดำเนินการขั้นต่ำ

ใช้คะแนนโอกาสเกิด (Likelihood: L) และผลกระทบ (Impact: I) ระดับ 1–5 ตามเกณฑ์ที่กำหนด โดยคำนวณดังนี้

คะแนนความเสี่ยง (Risk Score) = โอกาสเกิด (L) × ผลกระทบ (I)

คะแนน	ระดับความเสี่ยง	รหัสระดับ	แนวทางดำเนินการขั้นต่ำ
1–4	ต่ำ (Low)	L	รักษาการควบคุมและติดตามตามรอบปกติ การยอมรับต้องอยู่ภายในเกณฑ์และอำนาจที่กำหนด
5–9	ปานกลาง (Medium)	M	ทบทวนความเพียงพอของการควบคุม กำหนดมาตรการเพิ่มเติมตามความจำเป็น และติดตามโดยเจ้าของความเสี่ยง
10–15	สูง (High)	H	จัดทำหรือทบทวนแผนบริหารความเสี่ยง กำหนดผู้รับผิดชอบและเป้าหมาย พร้อมรายงานฝ่ายบริหารตามเกณฑ์
16–25	สูงมาก (Extreme)	E	ยกระดับรายงานทันทีเมื่อพบ เร่งดำเนินมาตรการ และติดตามอย่างใกล้ชิดตามสถานการณ์

คะแนนระดับต่ำหรือปานกลางไม่ทำให้ยอมรับความเสี่ยงได้โดยอัตโนมัติ ต้องพิจารณาสถานะ RA/RT ข้อกำหนดทางกฎหมาย เหตุที่ไม่ยอมรับ และเกณฑ์ยกระดับเป็นกรณีพิเศษร่วมด้วย

2.13.3 เกณฑ์ยกระดับเป็นกรณีพิเศษ

ให้ใช้เกณฑ์ยกระดับเป็นกรณีพิเศษ (Override Criteria) ร่วมกับคะแนนความเสี่ยง ดังนี้

1. **ผลกระทบระดับ 5** ให้ตอบสนองอย่างน้อยตามแนวทางความเสี่ยงระดับสูง แม้คะแนนรวมต่ำกว่า 10 และพิจารณาความเร่งด่วนตามลักษณะผลกระทบ

2. **เหตุที่ไม่ยอมรับ (Zero Tolerance Event)** ให้ระงับหรือควบคุมผลกระทบ ยกระดับรายงาน และดำเนินการด้วยความเร่งด่วนเทียบเท่าความเสี่ยงระดับสูงมากทันที โดยไม่รอคะแนนรวม ส่วนการประเมินความเสี่ยงคงเหลือหลังเหตุการณ์ให้ดำเนินการและบันทึกแยกตามข้อเท็จจริง

3. **KRI เกิน RT หรือการควบคุมสำคัญบกพร่อง** ให้ดำเนินการตาม Trigger วิเคราะห์ผลต่อความเสี่ยง และเสนอผู้มีอำนาจเมื่อเกินขอบเขตการตัดสินใจหรือเข้าเกณฑ์รายงาน โดยไม่รอรอบติดตามปกติ

4. ผลกระทบข้ามส่วนงานหรือมีความสำคัญเชิงยุทธศาสตร์ หากความเสี่ยงกระทบหลายส่วนงาน มีการกระจุกตัวสูง เกินอำนาจหรือทรัพยากรของส่วนงาน หรืออาจกระทบเป้าประสงค์และพันธกิจสำคัญ ให้เสนอพิจารณาการจัดการร่วมกันระดับมหาวิทยาลัย และพิจารณาบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัยตามกระบวนการที่กำหนด

การบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัยไม่เกิดขึ้นโดยอัตโนมัติจากคะแนนหรือ KRI เพียงรายการเดียว ต้องพิจารณาความสำคัญเชิงยุทธศาสตร์ ขอบเขตผลกระทบ ความสัมพันธ์ ความเร่งด่วน และอำนาจจัดการร่วมกัน การใช้ Override ให้บันทึกเหตุผล หลักฐาน ผู้เสนอ ผู้มีอำนาจพิจารณา วันที่ตัดสินใจ ระดับการตอบสนอง มาตรการ และกำหนดเวลาทบทวนไว้ในทะเบียนความเสี่ยง โดยคงคะแนน L × I ตามผลประเมินที่มีหลักฐานรองรับ หากมีข้อมูลใหม่จึงประเมินและบันทึกคะแนนใหม่ ทั้งนี้ การตอบสนองเร่งด่วนต้องไม่รอให้การบันทึกเอกสารเสร็จสิ้น

2.14 วัฒนธรรมความเสี่ยงองค์กร

มหาวิทยาลัยส่งเสริมวัฒนธรรมความเสี่ยงองค์กร (Risk Culture) เพื่อให้การตระหนักถึงความเสี่ยงและโอกาสเป็นส่วนหนึ่งของค่านิยม พฤติกรรม การปฏิบัติงาน และการตัดสินใจทุกระดับ โดยส่งเสริมความรับผิดชอบ การสื่อสารโดยสุจริต และการเรียนรู้ร่วมกัน ดังนี้

2.14.1 องค์ประกอบของวัฒนธรรมความเสี่ยง

1. ภาวะผู้นำและพฤติกรรมต้นแบบ (Tone from the Top) ผู้กำกับดูแลและผู้บริหารแสดงความมุ่งมั่นผ่านการใช้ข้อมูลความเสี่ยงประกอบการตัดสินใจ การสนับสนุนทรัพยากร การติดตามประเด็นสำคัญ และการรับผิดชอบต่อผลการตัดสินใจ รวมทั้งปฏิบัติตามค่านิยมและจริยธรรมอย่างสม่ำเสมอ

2. ความตระหนักด้านความเสี่ยง (Risk Awareness) บุคลากรเข้าใจวัตถุประสงค์และความเสี่ยงในงานของตน รู้จักการควบคุมที่เกี่ยวข้อง สัญญาณเตือน เกณฑ์การตอบสนอง และช่องทางรายงาน รวมทั้งเข้าใจผลกระทบที่อาจเกิดจากการปฏิบัติงานหรือการตัดสินใจ

3. ความเป็นเจ้าของความเสี่ยง (Risk Ownership) เจ้าของความเสี่ยงเข้าใจและปฏิบัติหน้าที่ที่ได้รับมอบหมาย โดยมีข้อมูลและทรัพยากรที่เหมาะสม ตัดสินใจภายในอำนาจ และยกระดับเมื่อเกินขอบเขต โดยประสานผู้เกี่ยวข้องและไม่ผลักความรับผิดชอบให้ผู้ประสานงานหรือหน่วยงานบริหารความเสี่ยง

4. ความรับผิดชอบตามบทบาท (Risk Accountability) ผู้เกี่ยวข้องรับผิดชอบต่อการตัดสินใจ การดำเนินการควบคุมและมาตรการ คุณภาพข้อมูล และผลลัพธ์ตามหน้าที่ พร้อมอธิบายเหตุผล รายงานข้อจำกัด และแก้ไขข้อบกพร่องอย่างทันเวลา

5. การสื่อสารอย่างเปิดเผยและปลอดภัย (Speak-up and Transparency) ส่งเสริมให้บุคลากรรายงานความเสี่ยง สัญญาณเตือน เหตุการณ์ ข้อผิดพลาด และข้อกังวลโดยสุจริต ผ่าน

ช่องทางที่เข้าถึงได้และเหมาะสม พร้อมรักษาความลับและดำเนินการคุ้มครองจากการตอบโต้ตามข้อกำหนดที่เกี่ยวข้อง ผู้รับรายงานต้องรับฟัง ประเมิน และติดตามเรื่องอย่างเป็นธรรม โดยไม่ด่วนสรุปความผิดจากการรายงาน

6. การตัดสินใจโดยคำนึงถึงความเสี่ยง (Risk-informed Decision-making) ผู้มีอำนาจใช้ข้อมูลความเสี่ยง โอกาส ทางเลือก สมมติฐาน ข้อจำกัด และกรอบ RA/RT ประกอบการอนุมัติ ปรับเปลี่ยน ชะลอ หรือยุติการดำเนินงาน พร้อมบันทึกเหตุผล เงื่อนไข และการติดตามผล

7. การเรียนรู้จากความเสี่ยง (Risk Learning) วิเคราะห์สาเหตุรากของเหตุการณ์ ข้อผิดพลาด เหตุการณ์เกือบเกิดความเสียหาย (Near Miss) ข้อร้องเรียน และข้อค้นพบจากการตรวจสอบ เพื่อปรับปรุงกระบวนการและป้องกันการเกิดซ้ำ พร้อมถ่ายทอดบทเรียนแก่ผู้เกี่ยวข้องโดยเคารพความเป็นส่วนตัวและกระบวนการพิจารณาข้อเท็จจริง

8. ความรู้และความสามารถด้านความเสี่ยง (Risk Competency) พัฒนาความรู้และทักษะของผู้กำกับดูแล ผู้บริหาร เจ้าของความเสี่ยง เจ้าของการควบคุม เจ้าของมาตรการ เจ้าของข้อมูล ผู้ประสานงาน และบุคลากรให้เหมาะสมกับบทบาท โดยติดตามความสามารถในการนำไปใช้จริงควบคู่กับการอบรม

9. การสอบทานและให้ข้อเสนอแนะอย่างสร้างสรรค์ (Constructive Challenge) เปิดโอกาสให้สายงานที่สองและผู้เกี่ยวข้องตั้งคำถาม ตรวจสอบข้อมูล ทบทวนสมมติฐาน และเสนอทางเลือกหรือข้อสังเกตโดยอาศัยหลักฐาน ผู้รับข้อเสนอแนะต้องพิจารณาอย่างเปิดกว้าง พร้อมชี้แจงหรือปรับปรุงตามความเหมาะสม

2.14.2 แนวทางส่งเสริมวัฒนธรรมความเสี่ยง

ให้ผู้บริหารส่วนงานกำหนดแนวทางส่งเสริมวัฒนธรรมความเสี่ยงที่เหมาะสมกับบริบท โดยเชื่อมโยงกับการบริหารงานปกติ เช่น การประชุมติดตามงาน การปฐมนิเทศ การพัฒนาบุคลากร การทบทวนเหตุการณ์ และการประเมินผลการดำเนินงาน พร้อมกำหนดผู้รับผิดชอบและติดตามการเปลี่ยนแปลงที่ต้องการ

การกำหนดเป้าหมายหรือแรงจูงใจต้องไม่ส่งเสริมให้ปกปิดเหตุการณ์ ลดคะแนนความเสี่ยงโดยไม่มีหลักฐาน หรือรายงานเฉพาะผลสำเร็จ ให้พิจารณาความถูกต้อง ความทันเวลา ความรับผิดชอบ และคุณภาพการแก้ไขร่วมกับผลลัพธ์

2.14.3 การประเมินวัฒนธรรมความเสี่ยง

ให้ใช้ข้อมูลหลายแหล่งทั้งเชิงปริมาณและเชิงคุณภาพ โดยพิจารณาความแตกต่างระหว่างส่วนงาน บทบาท และช่วงเวลา รวมถึงข้อมูลต่อไปนี้

ประเด็นประเมิน	ตัวอย่างข้อมูลหรือหลักฐาน
การรับรู้และความเข้าใจ	ผลสำรวจ การสัมภาษณ์ และความเข้าใจบทบาท เกณฑ์ และช่องทางรายงาน
การรายงานและการรับฟัง	ความทันเวลาในการรายงาน ความสะดวกของช่องทาง การตอบสนองต่อผู้รายงาน และข้อกังวลเกี่ยวกับการตอบโต้
ความเป็นเจ้าของและความรับผิดชอบ	การติดตามของเจ้าของความเสี่ยง การประสานแก้ไข และการยกระดับเมื่อเกินอำนาจหรือเข้าเกณฑ์
คุณภาพข้อมูลและการประเมิน	ความครบถ้วนของทะเบียนความเสี่ยง ความน่าเชื่อถือของหลักฐาน และเหตุผลรองรับคะแนนกับข้อสรุป
การใช้ข้อมูลในการตัดสินใจ	รายงานการประชุม บันทึกการพิจารณาทางเลือก การใช้ RA/RT และการติดตามผลการตัดสินใจ
ประสิทธิผลของการดำเนินงาน	ผลการทดสอบการควบคุม ความตรงเวลาของมาตรการ และการตอบสนองต่อ KRI หรือ EWS
การเรียนรู้และปรับปรุง	การวิเคราะห์สาเหตุราก การแก้ไขเชิงระบบ การถ่ายทอดบทเรียน และแนวโน้มการเกิดซ้ำ
ความสามารถตามบทบาท	ผลประเมินทักษะ คุณภาพชิ้นงาน และการนำความรู้ไปใช้ในการปฏิบัติงาน

การตีความจำนวนเหตุการณ์ต้องพิจารณาบริบทและคุณภาพการรายงานร่วมด้วย จำนวนรายงานที่เพิ่มขึ้นอาจสะท้อนความเชื่อมั่นในช่องทางและการเปิดเผยข้อมูลที่ดีขึ้น ส่วนจำนวนรายงานที่ลดลงอาจเกิดจากความเสี่ยงลดลงหรือการรายงานไม่ครบถ้วน จึงต้องใช้หลักฐานอื่นประกอบก่อนสรุป

ผลการประเมินให้ใช้กำหนดประเด็นพัฒนา ผู้รับผิดชอบ และระยะเวลา พร้อมติดตามว่าพฤติกรรม คุณภาพการตัดสินใจ ความโปร่งใส และผลลัพธ์เปลี่ยนแปลงอย่างไร โดยรักษาความลับและนำเสนอข้อมูลในระดับที่เหมาะสม ไม่ใช้จำนวนผู้เข้าอบรมหรือจำนวนกิจกรรมเพียงอย่างเดียวเป็นข้อสรุปว่าวัฒนธรรมความเสี่ยงมีประสิทธิผล

ส่วนที่ 3
โครงสร้างการกำกับดูแลและบทบาทหน้าที่ความรับผิดชอบ

3.1 หลักการกำกับดูแลการบริหารความเสี่ยง

มหาวิทยาลัยแม่โจ้บูรณาการการบริหารความเสี่ยงเข้ากับการกำกับดูแล การกำหนดยุทธศาสตร์ การบริหารผลการดำเนินงาน การจัดสรรทรัพยากร การควบคุมภายใน และการปฏิบัติตามกฎเกณฑ์ เพื่อสนับสนุนการตัดสินใจและการสร้าง รักษา และเพิ่มคุณค่า โดยกำหนดบทบาทความรับผิดชอบ และอำนาจตัดสินใจให้สอดคล้องกับกฎหมาย ข้อบังคับ กฎบัตร และคำสั่งที่มีผลใช้บังคับ ภายใต้หลักการดังต่อไปนี้

1. **การกำกับดูแลโดยสภามหาวิทยาลัย (Governing Body Oversight)** สภามหาวิทยาลัยกำหนดทิศทางและความคาดหวัง พิจารณาอนุมัตินโยบายและกรอบระดับความเสี่ยงที่ยอมรับได้ตามอำนาจหน้าที่ และกำกับติดตามฝ่ายบริหาร โดยได้รับข้อมูลความเสี่ยง การควบคุม และผลการให้ความเชื่อมั่นที่เพียงพอและทันเวลา พร้อมข้อจำกัดของข้อมูลและประเด็นที่ต้องตัดสินใจ

2. **ความรับผิดชอบของฝ่ายบริหาร (Management Accountability)** อธิการบดีและผู้บริหารนำนโยบายและกรอบที่ได้รับอนุมัติไปปฏิบัติ จัดให้มีระบบบริหารความเสี่ยงและการควบคุมที่เหมาะสม กำหนดผู้รับผิดชอบ จัดสรรทรัพยากร และติดตามผล โดยรับผิดชอบการตัดสินใจและผลการดำเนินงานภายในขอบเขตหน้าที่

3. **ความเป็นเจ้าของความเสี่ยง (Risk Ownership)** กำหนดเจ้าของวัตถุประสงค์ เจ้าของกระบวนการ และเจ้าของความเสี่ยงให้ชัดเจน พร้อมข้อมูล ทรัพยากร และอำนาจที่เหมาะสมกับบทบาท เจ้าของความเสี่ยงต้องติดตามและประสานการจัดการความเสี่ยง โดยไม่ผลักความรับผิดชอบให้หน่วยงานสนับสนุนหรือผู้ประสานงาน และต้องยกระดับเมื่อเกินอำนาจหรือความสามารถในการจัดการ

4. **การแบ่งและประสานบทบาทตามหลัก Three Lines** ฝ่ายบริหารในสายงานที่หนึ่งรับผิดชอบการดำเนินงานและจัดการความเสี่ยง สายงานที่สองสนับสนุน ให้คำปรึกษา ติดตาม และสอบทานตามหน้าที่ ส่วนกองตรวจสอบภายในในสายงานที่สามให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรม ทุกฝ่ายต้องประสานข้อมูลและการทำงาน โดยรักษาความรับผิดชอบและความเป็นอิสระตามบทบาท

5. **การตัดสินใจภายในขอบเขตอำนาจ (Decision within Delegated Authority)** การยอมรับความเสี่ยงต้องพิจารณา RA/RT ข้อกำหนดที่เกี่ยวข้อง และอำนาจที่ได้รับมอบหมาย พร้อมบันทึกเหตุผล หลักฐาน เงื่อนไข ระยะเวลาการยอมรับ และกำหนดทบทวน หากเกินเกณฑ์หรือเกิน

อำนาจต้องเสนอผู้มีอำนาจตามกระบวนการ ห้ามใช้การยอมรับความเสี่ยงเพื่ออนุญาตเหตุที่ไม่ยอมรับหรือการฝ่าฝืนกฎหมาย

6. การพิจารณาความเสี่ยงในภาพรวม (Portfolio View) พิจารณาความเสี่ยงรายประเด็นร่วมกับความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัวข้ามส่วนงาน เพื่อระบุประเด็นที่ต้องจัดการร่วมกันหรือใช้ทรัพยากรและการตัดสินใจระดับมหาวิทยาลัย โดยไม่ใช้การรวมคะแนนรายรายการแทนการวิเคราะห์ภาพรวม

7. ความโปร่งใสและการยกระดับอย่างทันเวลา (Transparency and Timely Escalation) รายงานข้อมูลตามข้อเท็จจริงอย่างครบถ้วนและทันเวลา พร้อมระบุความไม่แน่นอนและข้อจำกัด เมื่อเข้าเกณฑ์ต้องตอบสนองและยกระดับตามความเร่งด่วน โดยไม่ปกปิด บิดเบือน หรือรอรอบรายงานปกติสำหรับเหตุสำคัญ

8. คุณภาพข้อมูลและการตรวจสอบย้อนกลับ (Data Quality and Traceability)ข้อมูลที่ใช้ประเมิน ติดตาม และตัดสินใจต้องระบุแหล่งข้อมูล เจ้าของข้อมูล วันที่หรือช่วงเวลา นิยาม วิธีคำนวณ และหลักฐานรองรับ พร้อมควบคุมการแก้ไขและสิทธิการเข้าถึงตามความเหมาะสม เพื่อให้ตรวจสอบที่มาของคะแนน ข้อสรุป และการตัดสินใจได้

9. การประสานการให้ความเชื่อมั่น (Coordinated Assurance) ประสานขอบเขตข้อมูล และผลการประเมินระหว่างฝ่ายบริหาร สายงานที่สอง กองตรวจสอบภายใน และผู้ให้ความเชื่อมั่นอื่น เพื่อลดความซ้ำซ้อนและระบุช่องว่าง โดยพิจารณาความน่าเชื่อถือของแหล่งความเชื่อมั่นและไม่เปลี่ยนอำนาจหรือความเป็นอิสระของแต่ละฝ่าย

10. การทบทวนและปรับปรุงอย่างต่อเนื่อง (Continual Improvement) ใช้ผลการติดตาม เหตุการณ์ ข้อร้องเรียน ข้อค้นพบจากการตรวจสอบ การทดสอบแผน และบทเรียนมาทบทวนโครงสร้าง เกณฑ์ กระบวนการ และมาตรการ พร้อมกำหนดผู้รับผิดชอบและติดตามผลการปรับปรุง

การกำหนดบทบาทตามคู่มือต้องอ้างอิงเอกสารมอบหมายหน้าที่ที่มีผลใช้บังคับ และทบทวนเมื่อโครงสร้างหรือผู้รับผิดชอบเปลี่ยนแปลง ทั้งนี้ การระบุบทบาทในคู่มือไม่ก่อให้เกิดอำนาจอนุมัติหรืออำนาจยอมรับความเสี่ยงเพิ่มเติมจากที่กฎหมาย ข้อบังคับ หรือคำสั่งกำหนด

3.2 โครงสร้างการกำกับดูแลการบริหารความเสี่ยง

มหาวิทยาลัยจัดวางบทบาทการกำกับดูแล การบริหาร การปฏิบัติ และการให้ความเชื่อมั่นตามหลัก Three Lines โดยพิจารณาหน้าที่และความรับผิดชอบตามกฎหมาย ข้อบังคับ กฎบัตร และคำสั่งที่มีผลใช้บังคับ ให้ทุกฝ่ายประสานงานและแลกเปลี่ยนข้อมูลอย่างเหมาะสม พร้อมรักษาขอบเขตอำนาจและความเป็นอิสระตามบทบาท

ตารางที่ 3-1 ***ตารางแสดงกลุ่มบทบาท องค์ประกอบ และหน้าที่หลักในการกำกับดูแลความเสี่ยง***

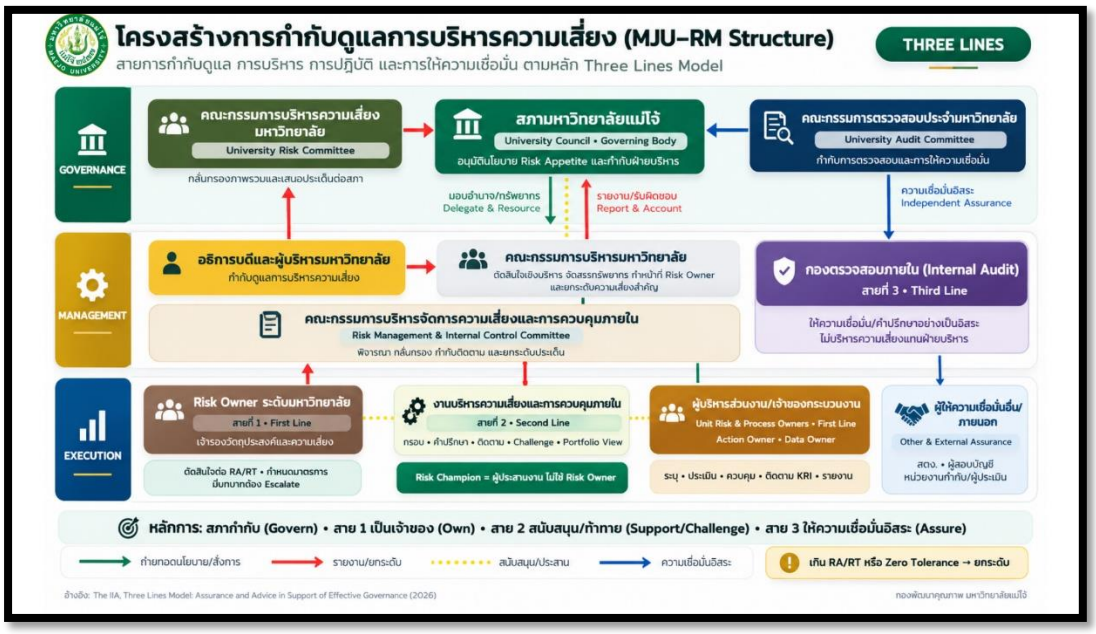
กลุ่มบทบาท	องค์ประกอบ	หน้าที่หลัก
ผู้กำกับดูแล (Governing Body)	สภามหาวิทยาลัย โดยมีคณะกรรมการตรวจสอบประจำมหาวิทยาลัย และคณะกรรมการที่ได้รับมอบหมายด้านความเสี่ยงสนับสนุนตามอำนาจหน้าที่	กำหนดทิศทาง พิจารณานโยบายและกรอบการยอมรับความเสี่ยง กำกับติดตามฝ่ายบริหาร และรับข้อมูลความเสี่ยง การควบคุม และผลการให้ความเชื่อมั่น โดยการอนุมัติหรือกลั่นกรองของแต่ละองค์กรให้เป็นไปตามอำนาจที่กำหนด
ฝ่ายบริหารระดับมหาวิทยาลัย (University Management)	อธิการบดี ผู้บริหารระดับมหาวิทยาลัย คณะกรรมการบริหารมหาวิทยาลัย และคณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน ตามขอบเขตที่ได้รับมอบหมาย	นำนโยบายไปปฏิบัติ กำหนดความรับผิดชอบ บริหารความเสี่ยงในภาพรวม จัดลำดับความสำคัญ จัดสรรทรัพยากร ตัดสินใจภายในอำนาจ และรายงานต่อผู้กำกับดูแล
บทบาทสายงานที่หนึ่ง (First Line Roles)	ผู้บริหารและผู้ปฏิบัติงานที่รับผิดชอบการดำเนินงาน รวมถึงเจ้าของวัตถุประสงค์ เจ้าของกระบวนการ เจ้าของความเสี่ยง เจ้าของการควบคุม เจ้าของมาตรการ และเจ้าของข้อมูลตามภารกิจ	รับผิดชอบผลการดำเนินงาน ระบุ ประเมิน จัดการ ติดตาม และรายงานความเสี่ยง ออกแบบและดำเนินการควบคุมกับมาตรการ พร้อมจัดเก็บหลักฐานและแก้ไขข้อบกพร่อง
บทบาทสายงานที่สอง (Second Line Roles)	งานบริหารความเสี่ยงและการควบคุมภายใน และผู้รับผิดชอบหน้าที่กำกับเฉพาะด้าน เช่น กฎหมาย การปฏิบัติตามกฎเกณฑ์ ความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล ความปลอดภัย และ BCM/BCP	พัฒนาหรือเสนอกรอบ มาตรฐาน เกณฑ์และเครื่องมือ ให้คำปรึกษา สนับสนุน ประสานงาน ติดตาม วิเคราะห์ และสอบทานอย่างสร้างสรรค์ โดยไม่ทำให้เจ้าของความเสี่ยงพ้นจากความรับผิดชอบ
บทบาทสายงานที่สาม (Third Line Roles)	กองตรวจสอบภายใน	ให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรมต่อความเพียงพอและประสิทธิผลของการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายใน รวมถึงการดำเนินงานของสายงานที่หนึ่งและสายงานที่สอง
ผู้ให้ความเชื่อมั่นอื่นและภายนอก (Other and External Assurance Providers)	ผู้สอบบัญชี ผู้ประเมินภายนอก หน่วยรับรอง ผู้เชี่ยวชาญอิสระ และหน่วยงานกำกับดูแล ตามลักษณะภารกิจ	ให้ความเชื่อมั่นหรือผลการประเมินตามขอบเขต อำนาจหน้าที่ และวิธีการของตน โดยมหาวิทยาลัยพิจารณาความ

กลุ่มบทบาท	องค์ประกอบ	หน้าที่หลัก
		น่าเชื่อถือ ความเป็นอิสระ และข้อจำกัด ก่อนนำผลมาใช้

หลักการใช้โครงสร้างและการประสานบทบาท

1. **แยกบทบาทกำกับดูแลออกจากบทบาทฝ่ายบริหาร** คณะกรรมการที่สนับสนุนการกำกับดูแลของสภามหาวิทยาลัยต้องมีหน้าที่และสายการรายงานตามเอกสารแต่งตั้งหรือมอบหมาย ส่วนคณะกรรมการฝ่ายบริหารทำหน้าที่อำนวยการ กลั่นกรอง ติดตาม หรือพิจารณาตามอำนาจ โดยไม่ถือเป็นผู้ให้ความเชื่อมั่นอย่างเป็นอิสระ
2. **พิจารณาบทบาทจากหน้าที่ที่ปฏิบัติจริง** สายงานที่หนึ่งและสายงานที่สองเป็นบทบาทภายใต้ฝ่ายบริหาร หน่วยงานหนึ่งอาจปฏิบัติทั้งสองบทบาทในกิจกรรมต่างกัน เช่น ดำเนินระบบเทคโนโลยีและกำกับมาตรฐานด้านความมั่นคงปลอดภัย จึงต้องระบุผู้รับผิดชอบและจัดการความขัดแย้งของบทบาทให้ชัดเจน
3. **คงความรับผิดชอบของเจ้าของความเสี่ยง** การสนับสนุนของสายงานที่สองหรือผู้ประสานงานไม่ทดแทนความรับผิดชอบของเจ้าของความเสี่ยง สายงานที่สองอาจมีอำนาจกำกับหรือตัดสินใจเฉพาะด้านตามที่ได้รับมอบหมาย และต้องปฏิบัติภายในขอบเขตนั้น
4. **รักษาความเป็นอิสระของการตรวจสอบภายใน** กองตรวจสอบภายในต้องไม่รับผิดชอบดำเนินงาน เป็นเจ้าของความเสี่ยง หรือบริหารการควบคุมแทนฝ่ายบริหาร การรายงาน การให้คำปรึกษา และภารกิจเพิ่มเติมให้เป็นไปตามกฎบัตรและมาตรการคุ้มครองความเป็นอิสระที่เกี่ยวข้อง
5. **ประสานแหล่งความเชื่อมั่นเพิ่มเติม** ผู้ให้ความเชื่อมั่นภายนอกเป็นแหล่งข้อมูลเพิ่มเติมจาก Three Lines ภายในมหาวิทยาลัย ให้ประสานขอบเขตและผลการประเมินผ่าน Assurance Map ตามความเหมาะสม โดยไม่เปลี่ยนอำนาจหน้าที่ของแต่ละฝ่าย
6. **ทบทวนโครงสร้างเมื่อมีการเปลี่ยนแปลง** เมื่อมีการเปลี่ยนแปลงโครงสร้าง คำสั่งแต่งตั้งหรือการมอบหมายหน้าที่ ให้ปรับข้อมูลผู้รับผิดชอบและเส้นทางรายงานให้เป็นปัจจุบัน การดำรงตำแหน่งผู้บริหารใหม่ไม่ทำให้เปลี่ยนองค์ประกอบคณะกรรมการโดยอัตโนมัติ เว้นแต่เอกสารแต่งตั้งกำหนดไว้หรือมีคำสั่งแก้ไข

ภาพที่ 3-1 ภาพแสดงโครงสร้างการกำกับดูแลการบริหารความเสี่ยง มหาวิทยาลัยแม่โจ้ (MJU–RM Structure)



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

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

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 ระดับความเสี่ยงคงเหลือ เป้าหมาย และความเพียงพอของทรัพยากรอย่างสร้างสรรค์

5. เสนอประเด็นที่ต้องการการตัดสินใจ การจัดสรรทรัพยากร หรือการกำกับเพิ่มเติมต่ออธิการบดีหรือสภามหาวิทยาลัยตามสายการรายงาน

6. รายงานต่อสภามหาวิทยาลัยตามรอบที่กำหนด และรายงานโดยไม่ชักช้าเมื่อเกิดเหตุการณ์สำคัญ

องค์ประกอบ อำนาจ วาระการดำรงตำแหน่ง การประชุม องค์ประชุม และสายการรายงานให้เป็นไปตามกฎบัตรหรือคำสั่งแต่งตั้งที่มีผลใช้บังคับ

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 และระดับความเสี่ยงคงเหลือเป้าหมาย เพื่อสั่งการหรือปรับการจัดสรรทรัพยากร

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 และคุณภาพข้อมูลพร้อมเสนอการยกระดับ

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 การบริหารความเสี่ยง และการควบคุมภายใน
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 เพื่อเชื่อมโยงบทบาทของผู้กำกับดูแล ฝ่ายบริหาร และการตรวจสอบภายใน ให้ทุกฝ่ายประสานงานและแลกเปลี่ยนข้อมูลอย่างเหมาะสม โดยรักษาความรับผิดชอบ อำนาจตัดสินใจ ความเป็นเจ้าของความเสี่ยง และความเป็นอิสระตามบทบาท

ตารางที่ 3-2 ***ตารางแสดงบทบาท ผู้เกี่ยวข้อง ความรับผิดชอบหลัก และขอบเขตการปฏิบัติ***

บทบาท	ผู้เกี่ยวข้อง	ความรับผิดชอบหลัก	ขอบเขตการปฏิบัติ
ผู้กำกับดูแล (Governing Body)	สภามหาวิทยาลัยและคณะกรรมการที่สนับสนุนการกำกับดูแลตามที่ได้รับมอบหมาย	กำหนดทิศทาง พิจารณานโยบายและกรอบการยอมรับความเสี่ยง กำกับติดตามฝ่ายบริหาร และรับข้อมูลความเสี่ยง การควบคุม และผลการให้ความเชื่อมั่น	ปฏิบัติตามอำนาจของแต่ละองค์กร แยกการกำกับดูแลออกจากการบริหารงานประจำ และไม่ทำให้ความรับผิดชอบของฝ่ายบริหารคลุมเครือ
สายงานที่หนึ่ง (First Line Roles)	ผู้บริหารและผู้ปฏิบัติงานที่รับผิดชอบการดำเนินงาน รวมถึงเจ้าของวัตถุประสงค์ กระบวนการ ความเสี่ยง การควบคุม มาตรการ และข้อมูล	ดำเนินงานให้บรรลุวัตถุประสงค์ บริหารความเสี่ยงและโอกาส ดำเนินการควบคุมและมาตรการ ติดตามรายงาน และแก้ไขข้อบกพร่อง	ตัดสินใจภายในอำนาจและยกระดับเมื่อเข้าเกณฑ์ ไม่ผลักความรับผิดชอบให้ผู้ประสานงาน สายงานที่สอง หรือกองตรวจสอบภายใน
สายงานที่สอง (Second Line Roles)	งานบริหารความเสี่ยงและการควบคุมภายใน และผู้ปฏิบัติหน้าที่กำกับเฉพาะด้าน เช่น กฎหมาย การ	พัฒนาหรือเสนอกรอบ เกณฑ์ และเครื่องมือ ให้คำปรึกษา สนับสนุน ติดตาม วิเคราะห์ สอบ	เป็นส่วนหนึ่งของฝ่ายบริหาร อาจมีอำนาจเฉพาะด้านตามที่ได้รับมอบหมาย แต่ไม่ทำให้เจ้าของความเสี่ยงพ้น

บทบาท	ผู้เกี่ยวข้อง	ความรับผิดชอบหลัก	ขอบเขตการปฏิบัติ
	ปฏิบัติตามกฎเกณฑ์ ไซเบอร์ PDPA ความปลอดภัย BCM/BCP คุณภาพ และการเงิน	ทานและให้ข้อเสนอแนะอย่างสร้างสรรค์ รวมทั้งรายงานภาพรวม	จากความรับผิดชอบ และต้องเปิดเผยข้อจำกัดในการประเมินงานที่ตนรับผิดชอบ
สายงานที่สาม (Third Line Roles)	กองตรวจสอบภายใน	ให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรมต่อการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายใน	ให้ข้อเสนอแนะได้ แต่ไม่อนุมัติ RA/RT ยอมรับความเสี่ยง เป็นเจ้าของทะเบียนความเสี่ยง หรือเลือกและดำเนินมาตรการแทนฝ่ายบริหาร
ผู้ให้ความเชื่อมั่นอื่นและภายนอก (Other and External Assurance Providers)	ผู้สอบบัญชี ผู้ประเมินภายนอก หน่วยรับรอง ผู้เชี่ยวชาญอิสระ และหน่วยงานกำกับดูแลตามภารกิจ	ให้ความเชื่อมั่นหรือผลการประเมินตามขอบเขต อำนาจหน้าที่ และวิธีการของตน	ระบุขอบเขต หลักฐาน ข้อจำกัด และระดับความเป็นอิสระให้ชัดเจน โดยเป็นแหล่งความเชื่อมั่นเพิ่มเติมจาก Three Lines ภายในมหาวิทยาลัย

สายงานที่หนึ่งและสายงานที่สองเป็นบทบาทภายใต้ฝ่ายบริหาร หน่วยงานหนึ่งอาจปฏิบัติทั้งสองบทบาทในกิจกรรมต่างกัน จึงต้องกำหนดผู้รับผิดชอบและแนวทางจัดการความขัดแย้งของบทบาทให้ชัดเจน ส่วนการประสานงานกับกองตรวจสอบภายในต้องไม่กระทบความเป็นอิสระและความเที่ยงธรรมในการประเมิน

หลักการทำงานร่วมกันคือ **ผู้กำกับดูแลกำหนดทิศทางและติดตาม ฝ่ายบริหารรับผิดชอบการดำเนินงานและความเสี่ยง สายงานที่สองสนับสนุนและสอบทาน และสายงานที่สามให้ความเชื่อมั่นอย่างเป็นอิสระ** โดยทุกฝ่ายใช้ข้อมูลร่วมกันตามสิทธิและหน้าที่ เพื่อสนับสนุนการตัดสินใจและการปรับปรุงอย่างต่อเนื่อง

3.5 ตารางบทบาทและความรับผิดชอบด้านการบริหารความเสี่ยง (Risk Management RACI Matrix)

มหาวิทยาลัยใช้ RACI เพื่อระบุผู้ดำเนินการ ผู้รับผิดชอบสูงสุด ผู้ให้คำปรึกษา และผู้รับทราบข้อมูลของแต่ละกิจกรรม โดยมีความหมายดังนี้

- R — **Responsible:** ผู้รับผิดชอบดำเนินกิจกรรมหรือจัดทำผลส่งมอบ
- A — **Accountable:** ผู้รับผิดชอบสูงสุดต่อผลลัพธ์ของกิจกรรมตามบทบาทที่ได้รับมอบหมาย ทั้งนี้ อำนาจอนุมัติต้องอ้างอิงเอกสารให้อำนาจแยกต่างหาก

- C — **Consulted:** ผู้ให้ข้อมูล คำปรึกษา หรือข้อเสนอแนะก่อนดำเนินการหรือตัดสินใจ
- I — **Informed:** ผู้ที่ต้องได้รับทราบความก้าวหน้า ผลการดำเนินงาน หรือผลการตัดสินใจ

แต่ละกิจกรรมหรือจุดตัดสินใจควรมี A หนึ่งบทบาทที่ชัดเจน หากต้องผ่านการพิจารณาหลายระดับ ให้แยกขั้นจัดทำ กลั่นกรอง และอนุมัติ พร้อมกำหนด A ของแต่ละขั้น โดย A อาจเป็นบุคคลหรือคณะกรรมการตามอำนาจหน้าที่

ตารางที่ 3-3 ***ตารางบทบาทและความรับผิดชอบด้านการบริหารความเสี่ยง***

กิจกรรม	ผู้ดำเนินการ R	ผู้รับผิดชอบสูงสุด A	ผู้ให้คำปรึกษา C	ผู้รับทราบ I
จัดทำข้อเสนอนโยบายและกรอบการบริหารความเสี่ยง	งานบริหารความเสี่ยงและการควบคุมภายในร่วมกับผู้เกี่ยวข้อง	ผู้บริหารที่ได้รับมอบหมายให้รับผิดชอบการจัดทำข้อเสนอ	ส่วนงานและหน่วยงานเฉพาะด้าน	อธิการบดีและคณะกรรมการที่เกี่ยวข้องตามขั้นตอน
กลั่นกรองข้อเสนอนโยบายและกรอบ	ฝ่ายเลขานุการจัดเตรียมข้อมูลและดำเนินการตามข้อพิจารณา	คณะกรรมการที่มีหน้าที่กลั่นกรองตามคำสั่ง	ฝ่ายบริหารและผู้เชี่ยวชาญที่เกี่ยวข้อง	ผู้มีอำนาจพิจารณาขั้นต่อไป
พิจารณาอนุมัตินโยบายหรือกรอบ	ฝ่ายบริหารและฝ่ายเลขานุการเสนอเรื่องตามขั้นตอน	ผู้มีอำนาจอนุมัติในเรื่องนั้น เช่น สภามหาวิทยาลัยสำหรับเรื่องที่อยู่ในอำนาจ	คณะกรรมการหรือหน่วยงานที่มีหน้าที่ให้ความเห็น	ผู้บริหารและส่วนงานที่ต้องนำไปปฏิบัติ
ประเมินความเสี่ยงและจัดทำแผนส่วนงาน	Risk Owner ร่วมกับผู้รับผิดชอบกระบวนการและผู้ประสานงาน	หัวหน้าส่วนงานหรือผู้ได้รับมอบหมายตามอำนาจ	งานบริหารความเสี่ยงและหน่วยงานเฉพาะด้าน	ผู้บริหารกำกับส่วนงานและผู้เกี่ยวข้อง
ดำเนินการควบคุมและมาตรการ	Control Owner และ Action Owner ตามกิจกรรม	ผู้รับผิดชอบสูงสุดของกิจกรรมตามที่ได้รับมอบหมาย	Risk Owner, Data Owner และผู้เชี่ยวชาญที่เกี่ยวข้อง	ผู้บริหารส่วนงานและงานบริหารความเสี่ยงตามรอบ
จัดทำและตรวจสอบข้อมูลตัวชี้วัด	ผู้จัดเก็บหรือจัดทำข้อมูลตามที่ได้รับมอบหมาย	Data Owner ของชุดข้อมูล	Risk Owner และผู้ดูแลระบบ	ผู้ใช้ข้อมูลและผู้รับรายงานตามสิทธิ
เสนอและพิจารณายอมรับความเสี่ยง	Risk Owner จัดทำข้อมูล เหตุผล	ผู้มีอำนาจยอมรับในแต่ละกรณี (A*)	ผู้บริหารกำกับงานและหน่วยงานเฉพาะด้าน	งานบริหารความเสี่ยงและ

กิจกรรม	ผู้ดำเนินการ R	ผู้รับผิดชอบสูงสุด A	ผู้ให้คำปรึกษา C	ผู้รับทราบ I
	ทางเลือก และ เงื่อนไข			ผู้เกี่ยวข้องตามสายรายงาน
รายงานและยกระดับความเสี่ยง	Risk Owner หรือผู้รับผิดชอบรายงานตามเกณฑ์	ผู้รับผิดชอบสูงสุดในการส่งรายงานของระดับนั้น	งานบริหารความเสี่ยงและหน่วยงานที่เกี่ยวข้อง	ผู้มีอำนาจตัดสินใจระดับถัดไปตามเส้นทางรายงาน
รวบรวมและจัดทำรายงานภาพรวม	งานบริหารความเสี่ยงรวบรวมและวิเคราะห์ โดยเจ้าของข้อมูลและ Risk Owner ตรวจสอบข้อมูลในส่วนที่รับผิดชอบ	ผู้บริหารที่ได้รับมอบหมายให้รับผิดชอบรายงานภาพรวม	ส่วนงานและหน่วยงานเฉพาะด้าน	อธิการบดีและคณะกรรมการที่เกี่ยวข้อง
กลั่นกรองและรายงานต่อสภามหาวิทยาลัย	ฝ่ายเลขานุการจัดเตรียมรายงานและข้อมูลประกอบ	คณะกรรมการหรือผู้มีหน้าที่รายงานตามข้อบังคับและคำสั่ง	ฝ่ายบริหารและเจ้าของความเสี่ยงที่เกี่ยวข้อง	สภามหาวิทยาลัยและผู้เกี่ยวข้องตามมติ
ดำเนินงานให้ความเชื่อมั่นอย่างเป็นอิสระ	ผู้ตรวจสอบภายในตามแผนและการมอบหมาย	หัวหน้าหน่วยงานตรวจสอบภายในตามกฎบัตร	ผู้รับผิดชอบงานที่ตรวจสอบให้ข้อมูลและชี้แจง	คณะกรรมการตรวจสอบ ผู้กำกับดูแล และฝ่ายบริหารตามกฎบัตร
แก้ไขข้อค้นพบและข้อบกพร่อง	เจ้าของมาตรการและเจ้าของการควบคุม	ผู้บริหารที่รับผิดชอบเรื่องนั้น	Risk Owner และหน่วยงานเฉพาะด้าน	กองตรวจสอบภายในและผู้กำกับติดตามตามขอบเขต

<u>หมายเหตุประกอบการใช้ RACI</u>

1. **A*** หมายถึง ผู้มีอำนาจยอมรับความเสี่ยงที่แตกต่างกันตามระดับความเสี่ยง ขอบเขตผลกระทบ และอำนาจที่ได้รับมอบหมาย ต้องระบุผู้มีอำนาจของแต่ละกรณีให้ชัดเจน โดยอาจเป็นบุคคลหรือองค์กรตามเอกสารให้อำนาจ

2. การยอมรับความเสี่ยงให้ใช้ตารางอำนาจยอมรับและยกระดับความเสี่ยง (Risk Acceptance and Escalation Authority Matrix) ร่วมกับ RA/RT และข้อกำหนดที่เกี่ยวข้อง หากเกินเกณฑ์ต้องเสนอพิจารณาตามกระบวนการ โดยไม่อนุญาตให้ฝ่าฝืนกฎหมายหรือยอมรับเหตุที่ไม่ยอมรับ

3. Risk Owner รับผิดชอบการบริหารความเสี่ยงที่ได้รับมอบหมาย ส่วนผู้บริหารส่วนงานยังคงรับผิดชอบผลการดำเนินงานและระบบบริหารความเสี่ยงของส่วนงาน การกำหนด RACI ไม่ทำให้ความรับผิดชอบตามกฎหมายหรือคำสั่งสิ้นสุดลง

4. Data Owner รับผิดชอบคุณภาพและนิยามของข้อมูล ส่วน Risk Owner รับผิดชอบการตีความผลและการตอบสนองภายในอำนาจ งานบริหารความเสี่ยงทำหน้าที่รวบรวม วิเคราะห์ และสอบทาน โดยไม่รับรองข้อมูลแทนผู้รับผิดชอบต้นทาง

5. กองตรวจสอบภายในติดตามและรายงานสถานะการแก้ไขอย่างเป็นอิสระ ส่วนฝ่ายบริหารและเจ้าของมาตรการรับผิดชอบดำเนินการแก้ไข การกำกับงานตรวจสอบของคณะกรรมการตรวจสอบไม่ทำให้คณะกรรมการเป็นผู้รับผิดชอบดำเนินงานตรวจสอบ

6. บทบาทและสายการรายงานของคณะกรรมการแต่ละชุดต้องยึดข้อบังคับ กฎบัตร และคำสั่งแต่งตั้ง การใช้ชื่อคณะกรรมการคล้ายกันไม่ทำให้มีอำนาจหรือหน้าที่เหมือนกัน

7. ตารางนี้เป็นกรอบสำหรับกำหนดความรับผิดชอบ ให้ระบุชื่อผู้ดำรงตำแหน่งและเอกสารอ้างอิงในการนำไปใช้จริง พร้อมทบทวนเมื่อมีการเปลี่ยนแปลง โดย RACI ไม่ก่อให้เกิดอำนาจอนุมัติหรือมอบอำนาจเพิ่มเติมจากเอกสารที่มีผลใช้บังคับ

3.6 สายการรายงานและการยกระดับความเสี่ยง

มหาวิทยาลัยกำหนดการรายงานให้สอดคล้องกับความรุนแรง ความเร่งด่วน ขอบเขตผลกระทบ และอำนาจตัดสินใจ โดยแบ่งเป็น 2 ลักษณะ ได้แก่

1. **การรายงานความเสี่ยงตามรอบ (Periodic Risk Reporting)** ใช้ติดตามระดับความเสี่ยง แนวโน้ม KRI สถานะเทียบ RA/RT ประสิทธิผลของการควบคุม และผลการดำเนินมาตรการตามรอบที่กำหนดฃ

2. **การรายงานและยกระดับนอกวงรอบ (Ad hoc Reporting and Escalation)** ใช้เมื่อเกิดเหตุการณ์หรือภาวะวิกฤต รวมถึงเมื่อความเสี่ยงหรือสัญญาณเตือนเข้าเกณฑ์ที่ต้องตัดสินใจ แม้ยังไม่เกิดความเสียหาย โดยไม่รอรายงานตามรอบ

3.6.1 สายการรายงานหลัก

สายการรายงาน	แนวทาง
ระดับส่วนงาน	ผู้พบเหตุ ผู้รับผิดชอบงาน หรือเจ้าของข้อมูล รายงานต่อผู้บังคับบัญชาหรือเจ้าของความเสี่ยง และหัวหน้าส่วนงานตามเกณฑ์
ระดับมหาวิทยาลัย	หัวหน้าส่วนงานหรือเจ้าของความเสี่ยงรายงานต่อผู้บริหารที่กำกับ อธิการบดี หรือคณะกรรมการฝ่ายบริหารตามอำนาจ พร้อมส่งข้อมูลให้งานบริหารความเสี่ยงและการควบคุมภายในเพื่อประสานและรวบรวมภาพรวม
ระดับผู้กำกับดูแล	ฝ่ายบริหารและคณะกรรมการที่มีหน้าที่เสนอหรือรายงาน ดำเนินการต่อสภามหาวิทยาลัยหรือคณะกรรมการที่เกี่ยวข้องตามข้อบังคับ คำสั่ง และลักษณะเรื่อง

สายการตรวจสอบภายใน	กองตรวจสอบภายในรายงานต่อคณะกรรมการตรวจสอบและผู้กำกับดูแลตามกฎบัตร โดยรักษาความเป็นอิสระจากความรับผิดชอบในการบริหารความเสี่ยงของฝ่ายบริหาร
สายการรายงานเฉพาะด้าน	รายงานต่อผู้รับผิดชอบด้านกฎหมาย ไซเบอร์ PDPA ความปลอดภัย BCM/BCP การสื่อสารภาวะวิกฤต หรือหน่วยงานภายนอก ตามข้อกำหนดและแผนที่เกี่ยวข้อง

สำหรับเรื่องเร่งด่วน ให้รายงานตรงต่อผู้มีอำนาจตัดสินใจหรือผู้รับผิดชอบเผชิญเหตุ พร้อมแจ้งผู้เกี่ยวข้องตามความจำเป็น การส่งข้อมูลผ่านงานบริหารความเสี่ยงและการควบคุมภายในต้องไม่เป็นเงื่อนไขที่ทำให้การตอบสนองล่าช้า

3.6.2 หลักการรายงานและตอบสนองต่อเหตุการณ์สำคัญ การรายงานต้องดำเนินควบคู่กับการตอบสนองตามสถานการณ์ โดยผู้พบเหตุและผู้รับผิดชอบต้อง

1. คุ้มครองชีวิต สุขภาพ และความปลอดภัยเป็นลำดับแรก
2. แจ้งผู้รับผิดชอบเผชิญเหตุหรือหน่วยฉุกเฉินที่เกี่ยวข้อง และระงับหรือจำกัดความเสียหายเท่าที่ทำได้อย่างปลอดภัยภายในหน้าที่และความสามารถ
3. คุ้มครองข้อมูล ระบบ ทรัพย์สิน และความต่อเนื่องของพันธกิจ
4. รักษาหลักฐานและบันทึกลำดับเหตุการณ์โดยไม่ขัดขวางการช่วยเหลือหรือระงับเหตุ
5. รายงานข้อเท็จจริงที่ยืนยันได้ แยกจากข้อสันนิษฐาน พร้อมระบุข้อมูลที่ยังต้องตรวจสอบ
6. สื่อสารผ่านผู้ได้รับมอบหมาย โดยรักษาความลับและสิทธิของผู้เกี่ยวข้อง
7. ดำเนินการแก้ไข เยียวยา ฟื้นฟู และป้องกันการเกิดซ้ำตามอำนาจหน้าที่

เมื่อเกิดเหตุที่ไม่ยอมรับ เหตุวิกฤต หรือภัยคุกคามร้ายแรง ให้รายงานผู้มีอำนาจและหน่วยงานเฉพาะด้านทันที โดยไม่รอข้อมูลครบถ้วนหรือผลการวิเคราะห์สาเหตุ แล้วปรับปรุงรายงานเมื่อได้รับข้อมูลเพิ่มเติม

3.6.3 ตารางการรายงานและการยกระดับความเสี่ยง

ตารางที่ 3-4 ***ตารางแสดงเกณฑ์กลางการรายงานและการยกระดับความเสี่ยง***

เหตุหรือเงื่อนไข	เวลารายงาน	ผู้รับรายงานและการประสานงาน	สาระขั้นต่ำ
เหตุที่ไม่ยอมรับ เหตุวิกฤต หรือภัยคุกคามร้ายแรงต่อชีวิต ความปลอดภัย ข้อมูล หรือพันธกิจสำคัญ	แจ้งทันที และจัดทำรายงานเบื้องต้นภายใน 24 ชั่วโมง	ผู้รับผิดชอบเผชิญเหตุ หัวหน้าส่วนงาน และผู้มีอำนาจระดับมหาวิทยาลัย พร้อมแจ้งหน่วยงานเฉพาะด้านและผู้กำกับดูแลตามเกณฑ์	ข้อเท็จจริง เวลาและสถานที่ ผลกระทบ การระงับเหตุ ผู้รับผิดชอบ หลักฐาน และการตัดสินใจที่ต้องการ

เหตุหรือเงื่อนไข	เวลารายงาน	ผู้รับรายงานและการประสานงาน	สาระขั้นต่ำ
ความเสี่ยงคงเหลือระดับสูงมาก 16–25	แจ้งทันทีเมื่อพบ และส่งข้อมูลเบื้องต้นภายใน 24 ชั่วโมง	หัวหน้าส่วนงานและผู้บริหารที่มีอำนาจ พร้อมแจ้งงานบริหารความเสี่ยงและการควบคุมภายใน	คะแนนและเหตุผล สาเหตุ ช่องว่างการควบคุม มาตรการเร่งด่วน ทรัพยากร และเป้าหมาย
ความเสี่ยงระดับสูง 10–15 หรือผลกระทบระดับ 5 ที่คะแนนต่ำกว่า 10	ภายใน 3 วันทำการ หรือเร็วกว่าตามความรุนแรงและ Trigger	หัวหน้าส่วนงานและผู้บริหารที่กำกับ พร้อมส่งข้อมูลให้งานบริหารความเสี่ยงและการควบคุมภายใน	ผลกระทบ หลักฐานการประเมิน สถานะ RA/RT แผนตอบสนอง และประเด็นที่ต้องตัดสินใจ
KRI เกิน RT การควบคุมสำคัญไม่ทำงาน หรือมาตรการสำคัญล่าช้า	ตาม Trigger โดยไม่เกิน 3 วันทำการ หากเข้าเกณฑ์เร่งด่วนให้ใช้เวลาของเกณฑ์นั้น	เจ้าของความเสี่ยง หัวหน้าส่วนงาน และผู้มีอำนาจที่เกี่ยวข้อง	ข้อมูลและแนวโน้ม สาเหตุ ผลต่อความเสี่ยง มาตรการแก้ไข ผู้รับผิดชอบ และกำหนดเวลา
ความเสี่ยงระดับปานกลาง 5–9	อย่างน้อยรายไตรมาส หรือตามรอบที่ถี่กว่า	หัวหน้าส่วนงาน และรายงานภาพรวมตามรอบมหาวิทยาลัย	KRI การควบคุม ผลการดำเนินมาตรการ แนวโน้ม และข้อเสนอ
ความเสี่ยงระดับต่ำ 1–4	ตามรอบบริหารงานปกติ โดยทบทวนอย่างน้อยรายไตรมาส	เจ้าของความเสี่ยงและผู้บริหารส่วนงานตามความเหมาะสม	การเปลี่ยนแปลงสำคัญ และหลักฐานว่าการควบคุมยังทำงาน

กรณีเข้าได้หลายเงื่อนไข ให้ใช้เกณฑ์ที่เร่งด่วนกว่า การประเมินว่าผลกระทบอาจอยู่ระดับ 5 โดยยังไม่เกิดเหตุ ให้รายงานตามเกณฑ์ความเสี่ยงและความเร่งด่วน ส่วนเหตุที่เกิดขึ้นจริงหรือภัยคุกคามฉุกเฉินต้องแจ้งทันที

ระยะเวลา 24 ชั่วโมงให้นับต่อเนื่องจากเวลาที่พบเหตุหรือรับทราบว่าเข้าเกณฑ์ ส่วน 3 วันทำการให้นับตามปฏิทินทำการของมหาวิทยาลัย หากข้อมูลยังไม่ครบ ให้รายงานเบื้องต้นพร้อมข้อจำกัดและกำหนดการส่งข้อมูลเพิ่มเติม โดยไม่ใช้การรอตรวจสอบเป็นเหตุเลื่อนรายงาน

เกณฑ์เวลาข้างต้นให้ใช้เมื่อได้รับอนุมัติเป็นเกณฑ์กลางของมหาวิทยาลัย หากกฎหมาย แผนฉุกเฉิน หรือข้อกำหนดเฉพาะกำหนดผู้รับรายงาน วิธีการ หรือเวลาที่แตกต่าง ให้ปฏิบัติตามข้อกำหนดนั้นด้วย และใช้เวลาที่เข้มงวดกว่าสำหรับหน้าที่รายงานเดียวกัน

3.6.4 การติดตามและปิดเหตุ

ภายหลังรายงานเบื้องต้น เจ้าของความเสี่ยงและผู้รับผิดชอบจัดการเหตุต้อง

1. รายงานความคืบหน้าตามความถี่ที่กำหนด พร้อมปรับปรุงข้อเท็จจริงและผลกระทบ
2. ประเมินความเสียหาย การเยียวยา และความเสี่ยงคงเหลือ
3. วิเคราะห์สาเหตุรากและจัดทำมาตรการแก้ไขและป้องกัน (CAPA)
4. กำหนดผู้รับผิดชอบ กำหนดเวลา และหลักฐานยืนยันผลการแก้ไข
5. ตรวจสอบความพร้อมก่อนฟื้นคืนบริการหรือกลับสู่การดำเนินงานปกติตามแผนที่เกี่ยวข้อง
6. จัดทำรายงานสรุป บทเรียน และรายการที่ต้องติดตามต่อ
7. เสนอปิดเหตุต่อผู้มีอำนาจตามแผนหรือขั้นตอนที่กำหนด

การปิดเหตุหมายถึงการยุติสถานะการจัดการเหตุการณ์ตามเกณฑ์ ไม่ทำให้ความเสี่ยงเป็นศูนย์ และไม่ยุติหน้าที่ติดตามมาตรการ การสอบสวน การเยียวยา หรือความรับผิดตามข้อกำหนดที่ยังคงมีอยู่

3.6.5 การเสนอพิจารณาเป็นความเสี่ยงระดับมหาวิทยาลัย

ให้เสนอพิจารณาการจัดการร่วมกันระดับมหาวิทยาลัยเมื่อความเสี่ยงมีลักษณะอย่างน้อยประการหนึ่ง ได้แก่

- กระทบเป้าประสงค์เชิงยุทธศาสตร์หรือพันธกิจสำคัญอย่างมีนัยสำคัญ
- กระทบหลายส่วนงาน หรือเกินความสามารถและทรัพยากรของส่วนงาน
- เกินเกณฑ์ RA/RT ที่เกี่ยวข้องหรือเกินอำนาจยอมรับของส่วนงาน
- มีความสัมพันธ์หรือการกระจุกตัวที่อาจขยายผลกระทบ
- ต้องใช้ทรัพยากรหรือการตัดสินใจระดับมหาวิทยาลัย
- อาจกระทบชีวิต ความปลอดภัย กฎหมาย ชื่อเสียง หรือความเชื่อมั่นอย่างมีนัยสำคัญ

การบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัยต้องผ่านการกลั่นกรองและพิจารณาตามอำนาจ โดยไม่เกิดขึ้นอัตโนมัติจากคะแนนหรือ KRI เพียงรายการเดียว ระหว่างการพิจารณาเจ้าของความเสี่ยงเดิมยังต้องดำเนินการตอบสนองและติดตามต่อไป จนมีการมอบหมายความรับผิดชอบใหม่อย่างชัดเจน

3.7 หลักการความรับผิดชอบร่วมกัน

การบริหารความเสี่ยงเป็นความรับผิดชอบของบุคลากรทุกระดับตามบทบาท โดยต้องกำหนดความเป็นเจ้าของ อำนาจตัดสินใจ และความรับผิดชอบต่อผลลัพธ์ให้ชัดเจน ดังนี้

1. **มีเจ้าของความเสี่ยงหลักที่ชัดเจน** ความเสี่ยงแต่ละรายการต้องระบุเจ้าของความเสี่ยงหลัก (Lead Risk Owner) หนึ่งบทบาท รับผิดชอบการประสานภาพรวม ติดตาม และรายงาน โดยมี

อำนาจเหมาะสมกับหน้าที่ หากต้องใช้ทรัพยากรหรือการตัดสินใจเกินอำนาจให้เสนอผู้มีอำนาจตามสายรายงาน

2. **ประสานความเสี่ยงข้ามส่วนงาน** หากมีหลายส่วนงานร่วมรับผิดชอบ ให้ระบุ Lead Risk Owner เจ้าของความเสี่ยงร่วม ผู้รับผิดชอบสูงสุดในแต่ละจุดตัดสินใจ และกลไกประสานงาน โดยไม่ลดทอนความรับผิดชอบของแต่ละส่วนงาน

3. **ระบุเจ้าของการควบคุม** การควบคุมสำคัญแต่ละรายการต้องมี Control Owner พร้อมขอบเขต ความถี่ วิธีปฏิบัติ และหลักฐานที่ต้องจัดเก็บ

4. **ระบุเจ้าของมาตรการ** มาตรการเพิ่มเติมต้องมี Action Owner ทรัพยากร ผลส่งมอบ กำหนดเวลา และวิธีตรวจสอบผล โดยรายงานทันทีเมื่อมีข้อจำกัดที่อาจทำให้ไม่บรรลุเป้าหมาย

5. **ระบุเจ้าของข้อมูล** KRI ทุกตัวต้องมี Data Owner รับผิดชอบนิยาม คุณภาพ และความทันเวลาของข้อมูล ส่วน Risk Owner รับผิดชอบการตีความและการตอบสนองภายในอำนาจ

6. **แยกบทบาทผู้ประสานงานและผู้ส่งเสริมความเสี่ยง** Risk Coordinator สนับสนุนการจัดทำข้อมูล ติดตาม และรายงาน ส่วน Risk Champion ส่งเสริมความเข้าใจและการมีส่วนร่วม บุคคลเดียวอาจทำทั้งสองบทบาทได้ตามการมอบหมาย แต่ไม่เป็นเจ้าของความเสี่ยงแทนโดยอัตโนมัติ

7. **ส่งเสริมการรายงานโดยสุจริตและการจัดการอย่างเป็นธรรม** บุคลากรรายงานข้อมูลความเสี่ยง สัญญาณเตือน เหตุการณ์ และข้อผิดพลาดอย่างถูกต้องและทันเวลา ผู้บริหารต้องรับฟัง รักษาความลับ และดำเนินการคุ้มครองผู้รายงานตามข้อกำหนด พร้อมใช้ข้อมูลระงับเหตุ แก้ไขสาเหตุ และปรับปรุงระบบ โดยพิจารณาความรับผิดจากข้อเท็จจริงและกระบวนการที่เป็นธรรม

การมอบหมายงานหรือประสานความร่วมมือไม่ทำให้ความรับผิดชอบตามกฎหมาย ข้อบังคับ หรือคำสั่งสิ้นสุดลง และต้องไม่ทำให้หน้าที่รายงานหรือการตอบสนองต่อความเสี่ยงขาดผู้รับผิดชอบ

3.8 อำนาจการยอมรับความเสี่ยง

การยอมรับความเสี่ยง (Risk Acceptance) หมายถึง การตัดสินใจโดยผู้มีอำนาจให้คงความเสี่ยงคงเหลือไว้ภายใต้เหตุผล การควบคุม เงื่อนไข และระยะเวลาที่กำหนด อาจเป็นการยอมรับเมื่อการควบคุมที่มีอยู่เพียงพอ หรือการยอมรับชั่วคราวระหว่างดำเนินมาตรการเพิ่มเติม โดยต้องพิจารณาทางเลือกและผลกระทบอย่างรอบด้าน

การยอมรับต้องอ้างอิง **ความเสี่ยงคงเหลือ ณ วันที่ตัดสินใจ** และสถานะเทียบกับ RA/RT โดยไม่ใช้ความเสี่ยงคงเหลือเป้าหมายแทนผลประเมินปัจจุบัน เจ้าของความเสี่ยงยังคงรับผิดชอบการจัดการ ติดตาม และรายงาน ส่วนผู้อนุมัติรับผิดชอบการตัดสินใจภายในอำนาจของตน การยอมรับความเสี่ยงไม่ยกเว้นหน้าที่ตามกฎหมาย ไม่อนุญาตเหตุที่ไม่ยอมรับ และไม่ยุติการควบคุม การติดตาม หรือการรายงาน การพิจารณาต้องใช้ข้อมูลและหลักฐานร่วมกับคะแนนความเสี่ยงเสมอ

3.8.1 กรอบการพิจารณาและอำนาจการยอมรับ

ตารางที่ 3-5 ***ตารางแสดงข้อเสนอกรอบอำนาจการยอมรับความเสี่ยงและเงื่อนไขขั้นต่ำ***

ระดับความเสี่ยงคงเหลือ	กรอบอำนาจที่เสนอ	เงื่อนไขขั้นต่ำ
ต่ำ 1–4 (L)	เจ้าของความเสี่ยงหรือหัวหน้าส่วนงาน เฉพาะกรณีที่ได้รับมอบอำนาจ	อยู่ภายใน RA/RT ไม่มีข้อห้ามหรือเหตุที่ไม่ยอมรับ มีหลักฐานการควบคุม และกำหนดการติดตาม
ปานกลาง 5–9 (M)	หัวหน้าส่วนงานหรือผู้บริหารที่ได้รับมอบอำนาจ	มีเหตุผลและหลักฐานรองรับ พิจารณา RA/RT และข้อกำหนดที่เกี่ยวข้อง พร้อมกำหนด KRI เงื่อนไขการยอมรับ และวันทบทวน
สูง 10–15 (H)	อธิการบดีหรือผู้บริหารระดับมหาวิทยาลัยที่ได้รับมอบอำนาจ โดยผ่านการกลั่นกรองตามขั้นตอน	หากเกิน RA/RT ให้เสนอพิจารณาเป็นกรณีเฉพาะตามอำนาจ พร้อมแผนลดความเสี่ยง เป้าหมาย ผู้รับผิดชอบ ทรัพยากร วันสิ้นสุด และการรายงาน
สูงมาก 16–25 (E)	ยกระดับทันที การคงความเสี่ยงไว้ชั่วคราวต้องเสนอผู้มีอำนาจที่กำหนดไว้โดยชัดแจ้ง และรายงานผู้กำกับดูแลตามเกณฑ์	ใช้เฉพาะกรณีจำเป็นที่มีเหตุผลรองรับ เช่น การหยุดทันทีอาจก่อผลกระทบรุนแรงกว่า ต้องมีมาตรการชดเชยหรือแผนฉุกเฉิน การติดตามใกล้ชิด วันสิ้นสุด และเงื่อนไขหยุดหรือยกระดับ

ตารางนี้เป็น **ข้อเสนอเพื่อพิจารณากำหนดอำนาจ** ให้ใช้เมื่อได้รับอนุมัติและมีเอกสารมอบอำนาจรองรับ ระหว่างนั้นให้ยึดอำนาจที่มีผลใช้บังคับ หากไม่ชัดเจนต้องเสนอให้ผู้มีอำนาจพิจารณา ไม่ถือว่าตำแหน่งหรือคะแนนความเสี่ยงให้อำนาจยอมรับโดยอัตโนมัติ

กรณีเข้าเกณฑ์ Override ให้ใช้ระดับการตอบสนองและอำนาจพิจารณาที่เข้มงวดกว่าตามเกณฑ์ โดยคงคะแนน L × I ตามหลักฐานการประเมิน การอนุมัติให้ดำเนินงานชั่วคราวไม่ทำให้สถานะความเสี่ยงที่เกิน RA/RT เปลี่ยนเป็นอยู่ภายในเกณฑ์

3.8.2 ข้อมูลประกอบการพิจารณา

ผู้มีอำนาจต้องพิจารณาอย่างน้อยดังต่อไปนี้

1. ความเสี่ยงคงเหลือ สถานะ RA/RT และความสามารถในการรองรับความเสี่ยง (Risk Capacity)
2. ข้อกำหนดทางกฎหมาย สัญญา ข้อผูกพัน และข้อห้ามที่เกี่ยวข้อง
3. ความเพียงพอและประสิทธิผลของการควบคุม รวมถึงข้อจำกัดของหลักฐาน
4. ผลต่อยุทธศาสตร์ พันธกิจสำคัญ และความต่อเนื่องของการดำเนินงาน

5. ความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัวของความเสี่ยง
6. ผลต่อชีวิต ความปลอดภัย ข้อมูล ชื่อเสียง และผู้มีส่วนได้ส่วนเสีย
7. ทางเลือก ต้นทุน ประโยชน์ และผลกระทบจากการดำเนินการ การชะลอ หรือการหยุดดำเนินการ
8. ความจำเป็น ระยะเวลาที่ต้องคงความเสี่ยงไว้ และความพร้อมของมาตรการเพิ่มเติม

การพิจารณาให้ดำเนินการภายในอำนาจที่มีอยู่ หากเกินอำนาจ ขัดกับข้อห้าม หรือไม่มีเงื่อนไขรองรับ ให้ยกระดับเสนอผู้มีอำนาจหรือเลือกแนวทางตอบสนองอื่นตามความเหมาะสม

3.8.3 หลักฐานการยอมรับความเสี่ยง

ให้บันทึกการยอมรับในแบบบันทึกหรือระบบที่เชื่อมโยงกับทะเบียนความเสี่ยง โดยระบุอย่างน้อย

1. รหัสและรายละเอียดความเสี่ยง วัตถุประสงค์ที่ได้รับผลกระทบ และเจ้าของความเสี่ยง
2. Inherent Risk และ Residual Risk พร้อมวันที่ประเมินและหลักฐานรองรับ
3. สถานะเทียบ RA/RT และเกณฑ์ Override ที่เกี่ยวข้อง
4. การควบคุมที่มีอยู่ ผลการประเมินประสิทธิผล และข้อบกพร่อง
5. ทางเลือกที่พิจารณา เหตุผลที่เลือกยอมรับ และผลกระทบของแต่ละทางเลือก
6. มาตรการเพิ่มเติมหรือมาตรการชดเชย แผนฉุกเฉิน และ Target Residual Risk หากมี
7. KRI ความถี่การติดตาม Trigger และเงื่อนไขหยุด ชะลอ หรือยกระดับ
8. ผู้เสนอ ผู้ให้ความเห็น ผู้อนุมัติ และเอกสารอ้างอิงอำนาจ
9. วันที่มีผล ระยะเวลาการยอมรับ วันทบทวน และวันสิ้นสุด
10. เงื่อนไขการอนุมัติและผู้รับผิดชอบติดตามแต่ละเงื่อนไข

3.8.4 การทบทวนและสิ้นสุดการยอมรับ

การยอมรับความเสี่ยงระดับสูงหรือสูงมากต้องมีวันสิ้นสุด (Expiry/Sunset Date) และเสนอพิจารณาใหม่ก่อนครบกำหนดหากยังจำเป็นต้องคงความเสี่ยงไว้ โดยใช้ผลประเมินและหลักฐานปัจจุบัน การยอมรับไม่ต่ออายุโดยอัตโนมัติ

ให้ทบทวนก่อนกำหนดเมื่อ KRI เข้าเกณฑ์ยกระดับ การควบคุมสำคัญไม่ทำงาน เกิดเหตุการณ์ สมมติฐานเปลี่ยนแปลง หรือไม่สามารถปฏิบัติตามเงื่อนไขอนุมัติ เจ้าของความเสี่ยงต้องรายงานและเสนอแนวทางต่อผู้มีอำนาจทันทีตามความเร่งด่วน

3.8.5 ข้อจำกัดสำหรับเหตุที่ไม่ยอมรับ

เหตุที่ไม่ยอมรับ (Zero Tolerance Event) ไม่อยู่ในกรอบอำนาจการยอมรับตามตารางนี้ การอนุมัติความเสี่ยงไม่สามารถใช้อนุญาตการกระทำผิดกฎหมาย การทุจริต หรือการฝ่าฝืนข้อห้ามของมหาวิทยาลัยได้

เมื่อพบเหตุหรือข้อมูลที่มีมูล ให้คุ้มครองผู้ได้รับผลกระทบ ระงับหรือจำกัดความเสียหาย รายงาน รักษาหลักฐาน และตรวจสอบข้อเท็จจริงตามอำนาจหน้าที่ พร้อมแก้ไข เยียวยา และดำเนินการตามกระบวนการที่เกี่ยวข้องโดยไม่ชักช้า โดยไม่ด่วนสรุปความผิดก่อนการพิจารณาข้อเท็จจริง

Zero Tolerance หมายถึงมหาวิทยาลัยไม่ยอมรับการกระทำ การเพิกเฉย หรือการปล่อยให้เหตุดำเนินต่อโดยไม่จัดการ แม้โอกาสเกิดเหตุจะไม่สามารถลดลงเป็นศูนย์ได้ทั้งหมด จึงต้องคงการป้องกัน การตรวจจับ และความพร้อมในการตอบสนองอย่างต่อเนื่อง

3.9 เกณฑ์การยกระดับความเสี่ยง

การยกระดับความเสี่ยง (Risk Escalation) หมายถึง การส่งต่อข้อมูลความเสี่ยงหรือเหตุการณ์ไปยังผู้มีอำนาจตัดสินใจในระดับสูงขึ้น เพื่อพิจารณาสั่งการ จัดสรรทรัพยากร หรือกำหนดมาตรการ เมื่อระดับความเสี่ยง ความเร่งด่วน ขอบเขตผลกระทบ หรือการดำเนินการที่จำเป็นเกินอำนาจหรือขีดความสามารถของผู้รับผิดชอบระดับเดิม หรือเข้าเงื่อนไขการยกระดับที่มหาวิทยาลัยกำหนด

การยกระดับต้องพิจารณาทั้งความเสี่ยงคงเหลือ สถานะระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) ประสิทธิผลของการควบคุม สัญญาณเตือน และข้อเท็จจริงของเหตุการณ์ โดยไม่ใช้คะแนนความเสี่ยงเป็นเกณฑ์เพียงอย่างเดียว

3.9.1 เงื่อนไขการยกระดับความเสี่ยง

ให้เจ้าของความเสี่ยงหรือผู้รับผิดชอบยกระดับเมื่อเข้าเงื่อนไขอย่างน้อยหนึ่งข้อ ดังต่อไปนี้

1. **ความเสี่ยงคงเหลืออยู่ในระดับสูงหรือสูงมาก:** มีคะแนนความเสี่ยงคงเหลือระดับสูง 10–15 หรือระดับสูงมาก 16–25 หรือเพิ่มขึ้นจนต้องได้รับการพิจารณาจากผู้มีอำนาจในระดับสูงขึ้น ทั้งนี้ความเสี่ยงโดยธรรมชาติที่อยู่ในระดับสูงหรือสูงมากต้องได้รับการพิจารณาความเพียงพอของการควบคุมและความจำเป็นในการยกระดับตามบริบทด้วย
2. **ผลกระทบรุนแรงหรือเข้าเกณฑ์ยกระดับเป็นกรณีพิเศษ:** มีผลกระทบระดับ 5 หรือเข้าเกณฑ์ยกระดับเป็นกรณีพิเศษ (Override Criteria) ตามข้อ 2.13 โดยให้ใช้ระดับการตอบสนองที่กำหนด แม้คะแนนรวมจะอยู่ในระดับต่ำกว่า และบันทึกคะแนนความเสี่ยงแยกจากระดับการตอบสนอง
3. **KRI เกิน RT หรือเข้าเงื่อนไขเตือนที่ต้องยกระดับ:** ตัวชี้วัดความเสี่ยงที่สำคัญ (KRI) เกิน RT หรือเข้าเงื่อนไขการยกระดับในช่วงเฝ้าระวังที่กำหนดไว้ รวมถึงมีข้อมูลหรือการคาดการณ์ที่น่าเชื่อถือว่าจะเกิน RT ก่อนรอบติดตามถัดไป ทั้งนี้ การเข้าสู่ช่วงเฝ้าระวังให้ดำเนินการตาม Trigger/Action ของ KRI แต่ละตัว และไม่ถือว่าต้องยกระดับทุกกรณีโดยอัตโนมัติ

4. **เหตุ Zero Tolerance เหตุวิกฤต หรือเหตุการณ์สำคัญ:** พบเหตุหรือข้อสงสัยที่มีมูลเกี่ยวกับเหตุ Zero Tolerance เหตุวิกฤต หรือเหตุการณ์เกือบเกิดความเสียหาย (Near Miss) ซึ่งสะท้อนช่องโหว่สำคัญและอาจก่อให้เกิดผลกระทบรุนแรงหากเกิดขึ้นจริง โดยต้องดำเนินการคุ้มครองและระงับเหตุโดยไม่รอผลการตรวจสอบข้อเท็จจริงให้แล้วเสร็จ

5. **ผลกระทบข้ามส่วนงานหรือเชิงยุทธศาสตร์:** ความเสี่ยงกระทบหรืออาจกระทบหลายส่วนงาน วัตถุประสงค์เชิงยุทธศาสตร์ พันธกิจสำคัญ หรือภาพรวมความเสี่ยงของมหาวิทยาลัย และจำเป็นต้องได้รับการประสานงานหรือการตัดสินใจในระดับมหาวิทยาลัย

6. **การควบคุมหรือมาตรการไม่มีประสิทธิผล:** การควบคุมสำคัญไม่ทำงาน มีข้อบกพร่องที่มีนัยสำคัญ หรือมาตรการสำคัญล่าช้า จนคาดว่าจะไม่สามารถลดความเสี่ยงให้ถึงระดับความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk) ภายในเวลาที่กำหนด

7. **เกินอำนาจหรือขีดความสามารถของเจ้าของความเสี่ยง:** ต้องใช้ทรัพยากร อำนาจตัดสินใจ การประสานงาน หรือการสื่อสารเกินขอบเขตของเจ้าของความเสี่ยงหรือส่วนงาน หรือไม่สามารถดำเนินมาตรการที่จำเป็นได้ภายในอำนาจที่ได้รับมอบหมาย

8. **ผลกระทบต่อมิติสำคัญอย่างมีนัยสำคัญ:** กระทบหรืออาจกระทบชีวิต สุขภาพและความปลอดภัย ชื่อเสียงและความเชื่อมั่น ฐานะการเงิน การปฏิบัติตามกฎหมาย ความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล ความต่อเนื่องของพันธกิจ สิ่งแวดล้อม หรือผู้มีส่วนได้ส่วนเสียอย่างมีนัยสำคัญ

9. **ความเสี่ยงเกิดใหม่ที่อาจมีผลกระทบสูง:** เป็นความเสี่ยงเกิดใหม่ที่ข้อมูลยังมีจำกัด มีความไม่แน่นอนสูง หรือเปลี่ยนแปลงอย่างรวดเร็ว และอาจมีผลกระทบสูง โดยข้อจำกัดของข้อมูลต้องไม่เป็นเหตุให้ชะลอการรายงานหรือการเตรียมมาตรการที่จำเป็น

10. **ความสัมพันธ์หรือการกระจุกตัวของความเสี่ยง:** ความเสี่ยงหลายรายการมีสาเหตุ ระบบ ข้อมูล ผู้ให้บริการ ทรัพยากร หรือผลกระทบร่วมกัน ซึ่งอาจทำให้ผลกระทบรวมรุนแรงกว่าการประเมินความเสี่ยงแต่ละรายการแยกกัน

11. **ข้อกำหนดตามกฎหมายหรือข้อผูกพัน:** กฎหมาย ระเบียบ สัญญา หรือหน่วยงานกำกับดูแลกำหนดให้ต้องแจ้ง รายงาน หรือดำเนินการภายในระยะเวลาที่กำหนด โดยต้องรายงานต่อผู้รับที่กำหนดไว้ตามข้อกำหนดนั้น ควบคู่กับการรายงานภายในมหาวิทยาลัย

12. **ความเห็นต่างที่ยังไม่ยุติ:** มีความเห็นต่างอย่างมีนัยสำคัญเกี่ยวกับระดับความเสี่ยง ประสิทธิผลของการควบคุม การยอมรับความเสี่ยง หรือความเพียงพอของมาตรการ และไม่สามารถยุติได้ในระดับเดิม ให้เสนอข้อมูล เหตุผล และความเห็นของแต่ละฝ่ายต่อผู้มีอำนาจพิจารณา โดยไม่ชะลอการดำเนินมาตรการคุ้มครองที่จำเป็น

3.9.2 หลักการยกระดับความเสี่ยง

1. **รายงานตามความเร่งด่วน:** ดำเนินการตามเวลาและเส้นทางที่กำหนดในตารางการรายงานและการยกระดับความเสี่ยง (Reporting and Escalation Matrix) ตามข้อ 3.6 โดยเหตุ Zero Tolerance เหตุวิกฤต และความเสี่ยงคงเหลือระดับสูงมากต้องแจ้งทันที และจัดทำรายงานตามระยะเวลาที่กำหนด

2. **รักษาความรับผิดชอบของเจ้าของความเสี่ยง:** การรายงานหรือยกระดับไม่ทำให้เจ้าของความเสี่ยงพ้นจากหน้าที่บริหารความเสี่ยง ระงับหรือจำกัดความเสียหายในขอบเขตอำนาจ ดำเนินมาตรการ และติดตามผล เว้นแต่มีการมอบหมายหรือเปลี่ยนเจ้าของความเสี่ยงอย่างเป็นทางการ

3. **รายงานตรงเมื่อจำเป็น:** กรณีฉุกเฉินหรือเหตุรุนแรง ให้รายงานตรงต่อผู้มีอำนาจตัดสินใจหรือผู้บัญชาการเหตุการณ์ พร้อมแจ้งหน่วยบริหารความเสี่ยงและหน่วยงานเฉพาะด้านที่เกี่ยวข้อง โดยไม่ให้กระบวนการรวบรวมหรือกลั่นกรองข้อมูลทำให้การตอบสนองล่าช้า

4. **ระบุสิ่งที่ต้องการให้ตัดสินใจ:** การยกระดับต้องระบุประเด็นที่ต้องพิจารณา ทางเลือกมาตรการเร่งด่วน ทรัพยากรที่จำเป็น และเวลาที่ต้องได้รับการตัดสินใจให้ชัดเจน หากข้อมูลยังไม่ครบถ้วน ให้แยกข้อเท็จจริงที่ยืนยันแล้ว ข้อสันนิษฐาน และข้อมูลที่อยู่ระหว่างตรวจสอบ

5. **ติดตามให้ได้รับการตอบสนอง:** หน่วยบริหารความเสี่ยงทำหน้าที่ประสานและติดตามการยกระดับตามบทบาท หากไม่ได้รับการตอบสนองภายในเวลาที่จำเป็น เจ้าของความเสี่ยงต้องติดตามหรือยกระดับต่อไปตามช่องทางที่กำหนด พร้อมบันทึกการดำเนินการ

6. **แยกการยกระดับออกจากการบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัย:** การยกระดับรายงานไม่ทำให้ความเสี่ยงเป็นความเสี่ยงระดับมหาวิทยาลัย (University-level/Enterprise Risk) โดยอัตโนมัติ การบรรจุต้องผ่านการกลั่นกรองและอนุมัติตามอำนาจที่กำหนด ระหว่างการพิจารณาเจ้าของความเสี่ยงเดิมยังคงรับผิดชอบจนกว่าจะมีการมอบหมายอย่างเป็นทางการ

7. **ปฏิบัติตามข้อกำหนดเฉพาะ:** หากกฎหมาย แผนฉุกเฉิน แผนเผชิญเหตุ หรือข้อกำหนดเฉพาะด้านกำหนดเวลาที่สั้นกว่า ให้ใช้เวลาที่สั้นกว่า และปฏิบัติตามเส้นทาง ผู้รับรายงาน และสาระการรายงานที่ข้อกำหนดนั้นระบุ การรายงานภายในไม่ทดแทนการแจ้งหน่วยงานภายนอกตามกฎหมาย

8. **ดำเนินการภายในอำนาจ:** การยกระดับไม่ถือเป็นการอนุมัติให้ยอมรับความเสี่ยง ไม่เปลี่ยนแปลง RA/RT และไม่ให้อำนาจดำเนินการเพิ่มเติมโดยอัตโนมัติ การตัดสินใจและการยอมรับความเสี่ยงต้องเป็นไปตามกฎหมาย การมอบอำนาจ และข้อ 3.9

3.9.3 ข้อมูลและหลักฐานที่ต้องบันทึก

ให้บันทึกการยกระดับในทะเบียนความเสี่ยง (Risk Register) หรือบันทึกเหตุการณ์และการยกระดับ (Incident/Escalation Record) ตามลักษณะของเรื่อง โดยเชื่อมโยงรหัสความเสี่ยงหรือรหัสเหตุการณ์เพื่อให้ตรวจสอบย้อนกลับได้ และมีข้อมูลอย่างน้อยดังต่อไปนี้

1. **ข้อมูลการรายงาน:** วันที่และเวลาที่พบหรือรับทราบ วันที่และเวลาที่รายงาน ผู้รายงาน ผู้รับรายงาน และช่องทางที่ใช้

2. **เหตุผลในการยกระดับ:** เงื่อนไขหรือเกณฑ์ที่เข้า รวมถึงเหตุผลการใช้ Override หากมี

3. **ข้อเท็จจริงและแหล่งข้อมูล:** รายละเอียดสถานการณ์ หลักฐาน แหล่งข้อมูล สมมติฐาน และข้อจำกัดของข้อมูล

4. **วัตถุประสงค์และขอบเขตผลกระทบ:** วัตถุประสงค์ พันธกิจ ส่วนงาน และผู้มีส่วนได้ส่วนเสียที่ได้รับหรืออาจได้รับผลกระทบ

5. **ผลการประเมินความเสี่ยง:** ระดับความเสี่ยงคงเหลือ ณ วันที่ประเมิน สถานะ RA/RT ค่าและแนวโน้ม KRI ตลอดจนระดับการตอบสนองตาม Override หากเกี่ยวข้อง กรณีเหตุฉุกเฉินที่ยังประเมินไม่ครบ ให้ระบุผลกระทบเบื้องต้นและกำหนดเวลาประเมินเพิ่มเติม

6. **การควบคุมและมาตรการที่ดำเนินการแล้ว:** สถานะและประสิทธิผลของการควบคุม ช่องว่างที่พบ การระงับเหตุ และมาตรการเร่งด่วน

7. **ประเด็นที่ต้องตัดสินใจ:** ทางเลือก ข้อเสนอ ผลกระทบจากการดำเนินการหรือไม่ดำเนินการ และกำหนดเวลาที่ต้องได้รับการตัดสินใจ

8. **ผู้รับผิดชอบและทรัพยากร:** เจ้าของความเสี่ยง ผู้รับผิดชอบจัดการเหตุ เจ้าของมาตรการ และทรัพยากรหรือการสนับสนุนที่ต้องการ

9. **ผลการพิจารณา:** ผู้มีอำนาจพิจารณา วันที่ตัดสินใจ ข้อสั่งการ เหตุผล เงื่อนไข และผู้รับผิดชอบนำข้อสั่งการไปปฏิบัติ

10. **การติดตามและปิดประเด็น:** รอบรายงานครั้งถัดไป กำหนดแล้วเสร็จ หลักฐานที่ใช้ยืนยันผล เงื่อนไขการยกระดับเพิ่มเติม และผู้มีอำนาจอนุมัติการปิดประเด็น

การปิดประเด็นการยกระดับต้องมีหลักฐานว่าข้อสั่งการได้รับการดำเนินการ และความเสี่ยงหรือเหตุการณ์ได้รับการจัดการตามเงื่อนไขที่กำหนด ทั้งนี้ การปิดประเด็นไม่ทำให้ความเสี่ยงสิ้นสุดลงโดยอัตโนมัติ และไม่ยุติหน้าที่ติดตามมาตรการ การเยียวยา หรือการดำเนินการตามกฎหมายที่ยังคงค้างอยู่

ส่วนที่ 4

กรอบและกระบวนการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้

4.1 หลักการของกรอบการบริหารความเสี่ยงองค์กร

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

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

หลักการตาม ISO 31000:2018 และองค์ประกอบตาม COSO ERM 2017 มีรายละเอียดในข้อ 1.6 และข้อ 1.7 ส่วนแนวทางการประยุกต์ใช้มีรายละเอียดในข้อ 2.8 และข้อ 2.7 ตามลำดับ มหาวิทยาลัยนำหลักการและองค์ประกอบดังกล่าวมาใช้ในการออกแบบกรอบการบริหารความเสี่ยง โดยยึดหลักปฏิบัติสำคัญดังต่อไปนี้

1. เริ่มต้นจากวัตถุประสงค์ (Objective-driven) ความเสี่ยงทุกเรื่องต้องเชื่อมโยงกับวัตถุประสงค์ ผลลัพธ์ ตัวชี้วัดผลการดำเนินงาน หรือพันธกิจที่ต้องคุ้มครองอย่างชัดเจน โดยระบุว่าความไม่แน่นอนอาจทำให้ผลลัพธ์เบี่ยงเบนจากเป้าหมายอย่างไร เพื่อให้การประเมินและการเลือกมาตรการตอบสนองมีจุดอ้างอิงที่ชัดเจน

2. ใช้ระบบที่บูรณาการและรองรับหลายกรอบอ้างอิง (One Integrated System, Multiple Frameworks) ใช้กระบวนการกลาง คำศัพท์ เกณฑ์ เครื่องมือ ข้อมูล และหลักฐานร่วมกันเท่าที่เหมาะสม เพื่อเชื่อมโยงการบริหารความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎเกณฑ์ การบริหารความต่อเนื่องขององค์กรและแผนความต่อเนื่องในการดำเนินงาน (BCM/BCP)

การพัฒนาองค์กรตามเกณฑ์ EdPEx มิติ ESG และการให้ความเชื่อมั่น โดยรักษาข้อกำหนดเฉพาะ อำนาจหน้าที่ และความเป็นอิสระของแต่ละบทบาท

3. บูรณาการกับการบริหารและการตัดสินใจ (Integrated into Management and Decision-making) พิจารณาความเสี่ยงและโอกาสตลอดวงจรการกำหนดและทบทวนยุทธศาสตร์ การจัดทำแผนงานและงบประมาณ การอนุมัติโครงการและการลงทุน การดำเนินงาน และการติดตามผล รวมทั้งใช้ข้อมูลความเสี่ยงประกอบการเลือกทางเลือก จัดลำดับความสำคัญ และจัดสรรทรัพยากร

4. ใช้มาตรฐานร่วมและประยุกต์ใช้ตามสัดส่วน (Common Standards and Proportionality) ใช้กระบวนการ คำศัพท์ และเกณฑ์กลางทั่วทั้งมหาวิทยาลัย โดยปรับระดับรายละเอียด ความถี่ และความเข้มข้นของการดำเนินงานให้เหมาะสมกับภารกิจ ขนาด ความซับซ้อน และระดับความเสี่ยงของแต่ละส่วนงาน การปรับใช้ต้องไม่ลดทอนข้อกำหนดขั้นต่ำ หน้าที่ตามกฎหมาย หรือเงื่อนไขการรายงานและการยกระดับที่กำหนดไว้

5. กำหนดความเป็นเจ้าของและอำนาจตัดสินใจให้ชัดเจน (Clear Ownership and Decision Rights) กำหนดเจ้าของวัตถุประสงค์ (Objective Owner) เจ้าของความเสี่ยง (Risk Owner) เจ้าของการควบคุม (Control Owner) เจ้าของมาตรการ (Action Owner) และเจ้าของข้อมูล (Data Owner) พร้อมขอบเขตความรับผิดชอบ อำนาจตัดสินใจ ทรัพยากร และเส้นทางการรายงานตามหลัก Three Lines หากการจัดการเกินอำนาจหรือขีดความสามารถของผู้รับผิดชอบ ต้องยกระดับต่อผู้มีอำนาจโดยไม่ชักช้า

6. ใช้ข้อมูลและหลักฐานที่เชื่อถือได้ (Evidence-based and Data-driven) ใช้สารสนเทศที่ดีที่สุดเท่าที่มี โดยพิจารณาความถูกต้อง ความครบถ้วน ความทันเวลา และความสามารถในการตรวจสอบย้อนกลับ พร้อมระบุแหล่งข้อมูล เจ้าของข้อมูล สมมติฐาน ข้อจำกัด และความไม่แน่นอนอย่างชัดเจน หากข้อมูลยังไม่เพียงพอ ให้บันทึกข้อจำกัดและกำหนดแนวทางหาข้อมูลเพิ่มเติมโดยไม่ชะลอการตอบสนองที่จำเป็น

7. บริหารเชิงรุกและมองไปข้างหน้า (Proactive and Forward-looking) ใช้ตัวชี้วัดความเสี่ยงที่สำคัญ (KRI) สัญญาณเตือนล่วงหน้า (EWS) การวิเคราะห์แนวโน้ม การวิเคราะห์สถานการณ์ และการติดตามความเสี่ยงเกิดใหม่ เพื่อเตรียมมาตรการก่อนเกิดผลกระทบอย่างมีนัยสำคัญ รวมทั้งพิจารณาความสัมพันธ์ ผลกระทบร่วม และการกระจุกตัวของความเสี่ยงในภาพรวมมหาวิทยาลัย

8. บริหารทั้งภัยคุกคามและโอกาส (Threat and Opportunity Management) พิจารณาทั้งความไม่แน่นอนที่อาจก่อให้เกิดความเสียหายและความไม่แน่นอนที่อาจนำไปสู่ผลลัพธ์ที่ดีกว่าคาด โดยประเมินทางเลือก ประโยชน์ ต้นทุน และความเสี่ยงที่เกี่ยวข้องกับการใช้ประโยชน์จากโอกาส ภายใต้ความสามารถในการรองรับความเสี่ยง (Risk Capacity) กรอบ RA/RT ข้อจำกัดตามกฎหมาย และอำนาจตัดสินใจที่ได้รับมอบหมาย

9. เชื่อมโยงความเสี่ยง–การควบคุม–การให้ความเชื่อมั่น (Risk–Control–Assurance) ประเมินความเสี่ยงควบคู่กับความเหมาะสมของการออกแบบการควบคุม การนำไปใช้ และประสิทธิผลในการปฏิบัติงาน พร้อมระบุหลักฐานและแหล่งการให้ความเชื่อมั่นให้ชัดเจน การประเมินความเสี่ยงคงเหลือต้องสะท้อนสภาพจริง ณ วันที่ประเมิน และแยกจากระดับความเสี่ยงคงเหลือเป้าหมายที่คาดว่าจะบรรลุหลังดำเนินมาตรการเพิ่มเติม

10. ทบทวน เรียนรู้ และปรับปรุงอย่างต่อเนื่อง (Learning and Continual Improvement) ใช้ผลการติดตาม ผลการดำเนินงาน เหตุการณ์จริง ข้อร้องเรียน เหตุการณ์เกือบเกิดความเสียหาย (Near Miss) ผลการตรวจสอบ ผลการทดสอบแผน และบทเรียนที่ได้รับ มาทบทวนสมมติฐานและปรับปรุงกรอบ กระบวนการ เกณฑ์ การควบคุม คุณภาพข้อมูล และความสามารถของบุคลากร ทั้งตามรอบที่กำหนดและเมื่อบริบทเปลี่ยนแปลงอย่างมีนัยสำคัญ

หลักปฏิบัติทั้ง 10 ประการเป็นแนวทางในการออกแบบและใช้กรอบการบริหารความเสี่ยงร่วมกัน มิใช่ขั้นตอนที่ต้องดำเนินการตามลำดับ ส่วนกระบวนการบริหารความเสี่ยงให้ดำเนินการตามขั้นตอนที่กำหนดไว้ในคู่มือ โดยมีการสื่อสาร การมีส่วนร่วม และการติดตามทบทวนตลอดกระบวนการ

ทุกส่วนงานต้องนำกรอบนี้ไปใช้ในการบริหารงานประจำและการตัดสินใจ โดยเชื่อมโยงข้อมูลความเสี่ยงกับผลการดำเนินงาน และจัดเก็บหลักฐานให้สามารถตรวจสอบย้อนกลับได้ว่า ความเสี่ยงเกี่ยวข้องกับเป้าหมายใด มีผู้รับผิดชอบใคร ได้ดำเนินมาตรการใด และข้อมูลความเสี่ยงนำไปสู่การตัดสินใจหรือการปรับปรุงอย่างไร

ภาพที่ 4-1 ภาพแสดงกรอบการบริหารความเสี่ยงองค์กร มหาวิทยาลัยแม่โจ้ (MJU Enterprise Risk Management Framework)

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

4.2 วัตถุประสงค์ของกรอบการบริหารความเสี่ยง

กรอบการบริหารความเสี่ยงมีวัตถุประสงค์เพื่อถ่ายทอดนโยบายและหลักการกำกับดูแลไปสู่การปฏิบัติ โดยกำหนดกระบวนการ บทบาท เกณฑ์ เครื่องมือ และข้อมูลที่เชื่อมโยงกัน เพื่อให้ทุกส่วนงานบริหารความเสี่ยงและโอกาสตามมาตรฐานร่วมของมหาวิทยาลัย และประยุกต์ใช้ได้อย่างเหมาะสมตามสัดส่วน โดยมีวัตถุประสงค์ดังต่อไปนี้

1. ถ่ายทอดนโยบายสู่การปฏิบัติ: นำนโยบาย กรอบระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) และหลักการกำกับดูแล มาจัดทำเป็นกระบวนการ เกณฑ์ เครื่องมือ และแนวทางปฏิบัติที่ส่วนงานสามารถนำไปใช้ในการดำเนินงานและการตัดสินใจได้จริง

2. กำหนดมาตรฐานร่วมของมหาวิทยาลัย: กำหนดคำศัพท์ วิธีระบุ วิเคราะห์ และประเมินความเสี่ยง ตารางประเมินระดับความเสี่ยง (Risk Matrix) แบบฟอร์ม นิยามข้อมูล และแนวทาง

รายงานให้สอดคล้องกัน เพื่อให้สามารถรวบรวม เปรียบเทียบ และติดตามความเสี่ยงระหว่างส่วนงานและในภาพรวมมหาวิทยาลัยได้

3. เชื่อมโยงกับยุทธศาสตร์และผลการดำเนินงาน: เชื่อมโยงความเสี่ยงและโอกาสกับวัตถุประสงค์ ตัวชี้วัดผลการดำเนินงาน (KPI) แผนงาน โครงการ การลงทุน งบประมาณ และผลลัพธ์ที่มหาวิทยาลัยต้องการบรรลุ ตั้งแต่การวางแผนจนถึงการติดตามและทบทวนผล

4. สนับสนุนการตัดสินใจโดยคำนึงถึงความเสี่ยงและใช้ข้อมูลเป็นฐาน: จัดให้มีข้อมูลความเสี่ยง โอกาส สมมติฐาน ทางเลือก และผลกระทบที่เชื่อถือได้ ทันเวลา และเหมาะสมกับระดับการตัดสินใจ พร้อมเปิดเผยข้อจำกัดและความไม่แน่นอนของข้อมูล เพื่อใช้ประกอบการอนุมัติ ปรับเปลี่ยน ชะลอ หรือยุติการดำเนินการ

5. กำหนดความรับผิดชอบและเส้นทางการรายงาน: กำหนดบทบาทของผู้กำกับดูแล ฝ่ายบริหาร ส่วนงาน เจ้าของความเสี่ยง และผู้เกี่ยวข้องตามหลัก Three Lines ให้ชัดเจน พร้อมเชื่อมโยงความรับผิดชอบ อำนาจตัดสินใจ และเส้นทางการรายงานตามกฎหมาย กฎบัตร คำสั่ง และการมอบอำนาจที่มีผลใช้บังคับ

6. เชื่อมโยงการบริหารความเสี่ยงกับกรอบ RA/RT: เชื่อมโยงผลการประเมินความเสี่ยงคงเหลือ ตัวชี้วัดความเสี่ยงที่สำคัญ (KRI) สัญญาณเตือนล่วงหน้า การตอบสนอง การยกระดับรายงาน และอำนาจยอมรับความเสี่ยง เพื่อให้ตรวจพบและจัดการความเสี่ยงที่เข้าใกล้หรือเกินเกณฑ์ได้อย่างทันเวลา

7. สนับสนุนการจัดลำดับความสำคัญและจัดสรรทรัพยากร: ใช้ระดับและแนวโน้มความเสี่ยง ความเร่งด่วน ความสำคัญเชิงยุทธศาสตร์ ความสัมพันธ์ และการกระจุกตัวของความเสี่ยงประกอบการจัดลำดับมาตรการและจัดสรรงบประมาณ บุคลากร เทคโนโลยี และทรัพยากรที่จำเป็นอย่างเหมาะสม

8. เชื่อมโยงการควบคุมและการให้ความเชื่อมั่น: สนับสนุนการออกแบบ นำไปใช้ และประเมินประสิทธิผลของการควบคุมภายใน เพื่อประเมินความเสี่ยงคงเหลือ (Residual Risk) จากหลักฐานการปฏิบัติจริง และประสานแหล่งการให้ความเชื่อมั่นให้ครอบคลุมความเสี่ยงสำคัญ โดยรักษาความเป็นอิสระของการตรวจสอบภายใน

9. เพิ่มความพร้อมและความยืดหยุ่นขององค์กร: สนับสนุนการติดตามความเสี่ยงเกิดใหม่ การเตรียมพร้อมและตอบสนองต่อเหตุฉุกเฉิน การบริหารความต่อเนื่อง และการฟื้นตัวจากเหตุหยุดชะงัก เพื่อคุ้มครองชีวิต ความปลอดภัย และพันธกิจสำคัญของมหาวิทยาลัย

10. จัดให้มีข้อมูลความเสี่ยงสำหรับการบริหารและการกำกับดูแล: จัดทำทะเบียนความเสี่ยง (Risk Register) ข้อมูลสรุปสถานะความเสี่ยง (Risk Profile) มุมมองความเสี่ยงในภาพรวม (Portfolio View) แผงสรุปข้อมูล (Dashboard) และรายงานตามความจำเป็น ให้เจ้าของความเสี่ยง ผู้บริหาร คณะกรรมการ และสภามหาวิทยาลัยได้รับข้อมูลที่เหมาะสมกับบทบาท สามารถตรวจสอบย้อนกลับได้ และใช้ประกอบการตัดสินใจได้

11. สนับสนุนการสร้างคุณค่าและความยั่งยืน: ส่งเสริมการใช้ประโยชน์จากโอกาส การพัฒนานวัตกรรม ความเป็นเลิศ และการดำเนินงานที่คำนึงถึงสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG) ภายใต้ความสามารถในการรองรับความเสี่ยง กรอบ RA/RT และข้อจำกัดตามกฎหมาย

12. สนับสนุนการเรียนรู้และปรับปรุงระบบ: ใช้ผลการติดตาม ผลการดำเนินงาน เหตุการณ์จริง เหตุการณ์เกือบเกิดความเสียหาย ข้อสังเกตจากการตรวจสอบ และบทเรียนที่ได้รับ เพื่อพัฒนากรอบ กระบวนการ คุณภาพข้อมูล สมรรถนะบุคลากร และประสิทธิผลของระบบบริหารความเสี่ยงอย่างต่อเนื่อง

กรอบการบริหารความเสี่ยงจึงทำหน้าที่เชื่อมโยงวัตถุประสงค์ ความเสี่ยงและโอกาส การควบคุม ข้อมูล การตอบสนอง การให้ความเชื่อมั่น และการตัดสินใจให้เป็นระบบเดียวกัน โดยประเมินผลสำเร็จจากการนำข้อมูลไปใช้ คุณภาพของการตัดสินใจ ประสิทธิผลของการจัดการความเสี่ยง และการสนับสนุนการบรรลุวัตถุประสงค์ของมหาวิทยาลัย

4.3 องค์ประกอบของกรอบการบริหารความเสี่ยง

มหาวิทยาลัยแม่โจ้กำหนดองค์ประกอบของกรอบการบริหารความเสี่ยงองค์กร โดยสังเคราะห์และประยุกต์ใช้ COSO ERM 2017, ISO 31000:2018 หลักเกณฑ์กระทรวงการคลัง และแนวทางที่เกี่ยวข้องให้เหมาะสมกับบริบทและพันธกิจของมหาวิทยาลัย ประกอบด้วย 8 องค์ประกอบที่เชื่อมโยงและสนับสนุนกัน ดังตารางที่ 4-1

องค์ประกอบดังกล่าวเป็นโครงสร้างของกรอบที่มหาวิทยาลัยนำมาประยุกต์ใช้ มิใช่การกำหนดองค์ประกอบใหม่ของมาตรฐานอ้างอิง และต้องใช้ร่วมกับหลักการ บทบาท และข้อกำหนดที่ระบุไว้ในคู่มือฉบับนี้

ตารางที่ 4-1 ***ตารางแสดงองค์ประกอบของกรอบการบริหารความเสี่ยงองค์กร มหาวิทยาลัยแม่โจ้***

องค์ประกอบ	สาระสำคัญ	ผลผลิตและผลลัพธ์หลัก
1. การกำกับดูแลและวัฒนธรรม (Governance and Culture)	กำหนดโครงสร้าง บทบาท และความสัมพันธ์ตามหลัก Three Lines ความเป็นเจ้าของความเสี่ยง อำนาจตัดสินใจ และสายการรายงาน พร้อมส่งเสริมภาวะผู้นำ ความโปร่งใส ความรับผิดชอบ และการรายงานโดยสุจริต	โครงสร้างและบทบาทที่ชัดเจน อำนาจและสายการรายงานที่สอดคล้องกับเอกสารให้อำนาจ และพฤติกรรมที่สนับสนุนการใช้ข้อมูลความเสี่ยงและการรายงานอย่างทันเวลา
2. ยุทธศาสตร์และวัตถุประสงค์ (Strategy and Objectives)	เชื่อมโยงความเสี่ยงและโอกาสกับวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ วัตถุประสงค์ ตัวชี้วัดผลการดำเนินงาน (KPI) แผนงาน โครงการ การลงทุน และการจัดสรรทรัพยากร โดยพิจารณาบริบทและสมมติฐานสำคัญ	วัตถุประสงค์ เจ้าของวัตถุประสงค์ ตัวชี้วัด เป้าหมาย และสมมติฐานที่ชัดเจน พร้อมหลักฐานความเชื่อมโยงระหว่างความเสี่ยงกับผลลัพธ์ที่ต้องการบรรลุ
3. ความสามารถในการรองรับและกรอบการยอมรับความเสี่ยง (Risk Capacity, Appetite and Tolerance)	กำหนดความสามารถในการรองรับความเสี่ยง ระดับความเสี่ยงที่ยอมรับได้ (RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (RT) พร้อมเชื่อมโยงกับเกณฑ์การตัดสินใจ ตัวชี้วัด อำนาจยอมรับ และเงื่อนไขการยกระดับ	กรอบ RA/RT ที่ได้รับอนุมัติตามอำนาจ เกณฑ์และเงื่อนไขที่นำไปใช้ได้จริง และตารางอำนาจยอมรับและยกระดับความเสี่ยงที่สอดคล้องกับการมอบอำนาจ
4. การระบุ วิเคราะห์ และประเมินความเสี่ยง (Risk Identification, Analysis and Evaluation)	วิเคราะห์บริบทและผู้มีส่วนได้ส่วนเสีย ระบุความเสี่ยงตามโครงสร้างสาเหตุ–เหตุการณ์–ผลกระทบ ประเมินโอกาสเกิดและผลกระทบ พิจารณาการควบคุม และแยกความเสี่ยงโดยธรรมชาติออกจากความเสี่ยงคงเหลือ พร้อมพิจารณาความสัมพันธ์และการกระจุกตัวของความเสี่ยง	ทะเบียนความเสี่ยง (Risk Register) ข้อมูลสรุปสถานะความเสี่ยง (Risk Profile) มุมมองความเสี่ยงในภาพรวม (Portfolio View) และลำดับความสำคัญที่มีเหตุผลและหลักฐานรองรับ
5. การตอบสนองและการควบคุม (Risk Response and Control)	เลือกแนวทางหลีกเลี่ยง ลดหรือควบคุม แบ่งปันหรือถ่ายโอน หรือยอมรับความเสี่ยงตามอำนาจ รวมทั้งพิจารณา	แผนบริหารความเสี่ยง (Risk Treatment Plan) รายละเอียดการควบคุม เจ้าของการควบคุม

องค์ประกอบ	สาระสำคัญ	ผลผลิตและผลลัพธ์หลัก
	แนวทางใช้ประโยชน์จากโอกาส กำหนดและดำเนินมาตรการที่เหมาะสมกับสาเหตุ ผลกระทบ และกรอบ RA/RT	เจ้าของมาตรการ ทรัพยากร กำหนดเวลา หลักฐานผลการดำเนินงาน และระดับความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk)
6. ข้อมูล ตัวชี้วัด การสื่อสาร และการรายงาน (Risk Information, Indicators, Communication and Reporting)	กำหนด KPI, KRI ตัวชี้วัดการควบคุมที่สำคัญ (KCI) ตามความจำเป็น และสัญญาณเตือนล่วงหน้า (EWS) โดยระบุนิยาม วิธีคำนวณ แหล่งข้อมูล เจ้าของข้อมูล ความถี่ และเงื่อนไขการตอบสนอง พร้อมจัดให้มีการสื่อสาร รายงาน และยกระดับที่เหมาะสมกับผู้รับและความเร่งด่วน	ข้อมูลที่เชื่อถือได้ ทันเวลา และตรวจสอบย้อนกลับได้ แผงสรุปข้อมูล (Dashboard) หรือรายงานตามความจำเป็น ตลอดจนบันทึกการแจ้งเตือน การยกระดับ และการตัดสินใจ
7. การติดตาม ทบทวน และการให้ความเชื่อมั่น (Monitoring, Review and Assurance)	ติดตามระดับความเสี่ยง ตัวชี้วัด และความก้าวหน้าของมาตรการ ประเมินการออกแบบ การนำไปใช้ และประสิทธิผลของการควบคุม ทบทวนความเหมาะสมของ RA/RT และเสนอปรับปรุงตามอำนาจ พร้อมประสานแหล่งการให้ความเชื่อมั่นโดยรักษาความเป็นอิสระของการตรวจสอบภายใน	รายงานสถานะและแนวโน้มความเสี่ยง ผลประเมินการควบคุม แผนผังการให้ความเชื่อมั่น (Assurance Map) ตามขอบเขตที่กำหนด ข้อค้นพบ ช่องว่าง และมาตรการปรับปรุงที่มีผู้รับผิดชอบ
8. ความต่อเนื่อง ความยืดหยุ่น และการปรับปรุง (Continuity, Resilience and Improvement)	เชื่อมโยงการบริหารความต่อเนื่องขององค์กร (BCM) แผนความต่อเนื่องในการดำเนินงาน (BCP) แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (DRP) และการจัดการภาวะวิกฤต พร้อมใช้ผลการทดสอบแผนและบทเรียนจากเหตุการณ์ปรับปรุงระบบอย่างต่อเนื่อง	แผนและความพร้อมที่ผ่านการทดสอบ ความสามารถในการรักษาและฟื้นฟูพันธกิจสำคัญตามเป้าหมายที่กำหนด และหลักฐานการปรับปรุงจากบทเรียนและผลการประเมิน

องค์ประกอบทั้ง 8 ประการต้องทำงานเชื่อมโยงกันตลอดวงจรการบริหารความเสี่ยง โดยการกำกับดูแลและวัฒนธรรมเป็นฐานสนับสนุน ยุทธศาสตร์และวัตถุประสงค์เป็นจุดอ้างอิง และกรอบ RA/RT เป็นเกณฑ์ประกอบการประเมินและการตัดสินใจ ส่วนข้อมูล การสื่อสาร การติดตาม และการให้ความเชื่อมั่นช่วยให้มหาวิทยาลัยรับรู้การเปลี่ยนแปลงและปรับการตอบสนองได้อย่างเหมาะสม

องค์ประกอบของกรอบทั้ง 8 ประการแตกต่างจากกระบวนการบริหารความเสี่ยง 8 ขั้นตอน กล่าวคือ *องค์ประกอบของกรอบแสดงโครงสร้างและกลไกที่ระบบต้องมี ขณะที่กระบวนการแสดงกิจกรรมการปฏิบัติที่ใช้บริหารความเสี่ยงแต่ละเรื่อง องค์ประกอบจึงไม่จำเป็นต้องดำเนินการตามลำดับ แต่ต้องสนับสนุนการปฏิบัติตลอดกระบวนการ*

4.3.1 การกำหนดทิศทางจากบนลงล่าง (Top-down Approach)

สภามหาวิทยาลัย คณะกรรมการที่เกี่ยวข้อง อธิการบดี และผู้บริหารระดับมหาวิทยาลัย กำหนด พิจารณาอนุมัติ หรือถ่ายทอดทิศทางการบริหารความเสี่ยงตามอำนาจหน้าที่ของแต่ละบทบาท โดยครอบคลุมเรื่องสำคัญดังต่อไปนี้

1. ทิศทางและวัตถุประสงค์เชิงยุทธศาสตร์: กำหนดเป้าหมาย ผลลัพธ์ และพันธกิจสำคัญที่ต้องบรรลุหรือคุ้มครอง พร้อมระบุสมมติฐานและความไม่แน่นอนที่มีผลต่อการเลือกและดำเนินยุทธศาสตร์

2. นโยบายและกรอบการบริหารความเสี่ยง: กำหนดหลักการ มาตรฐานขั้นต่ำ กระบวนการ เกณฑ์ และความคาดหวังที่ส่วนงานต้องนำไปปฏิบัติ

3. ความสามารถในการรองรับและกรอบการยอมรับความเสี่ยง: พิจารณาความสามารถในการรองรับความเสี่ยง (Risk Capacity) และกำหนดกรอบระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) กับระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) ให้สอดคล้องกับยุทธศาสตร์ ทรัพยากร และข้อจำกัดตามกฎหมาย

4. ตัวชี้วัดและเงื่อนไขการตอบสนอง: กำหนดตัวชี้วัดความเสี่ยงที่สำคัญระดับมหาวิทยาลัย (University-level KRI) เกณฑ์เฝ้าระวัง และเงื่อนไขการตอบสนองหรือยกระดับ เพื่อใช้ติดตามความเสี่ยงที่อาจกระทบเป้าหมายสำคัญ

5. ประเด็นความเสี่ยงและผลลัพธ์ที่ต้องติดตาม: กำหนดความเสี่ยงสำคัญ ขอบเขตการติดตาม เจ้าของความเสี่ยง และผลลัพธ์ที่คาดหวังจากการจัดการ

6. อำนาจยอมรับและเกณฑ์การยกระดับความเสี่ยง: กำหนดหรือถ่ายทอดขอบเขตอำนาจตัดสินใจ เงื่อนไขการยอมรับ และเส้นทางการรายงาน โดยอ้างอิงกฎหมาย กฎบัตร คำสั่ง และการมอบอำนาจที่มีผลใช้บังคับ

7. ลำดับความสำคัญและการจัดสรรทรัพยากร: กำหนดความสำคัญของมาตรการและกรอบการสนับสนุนงบประมาณ บุคลากร เทคโนโลยี และทรัพยากรที่จำเป็น โดยพิจารณาผลกระทบต่อยุทธศาสตร์และภาพรวมความเสี่ยง

ฝ่ายบริหารต้องถ่ายทอดทิศทางดังกล่าวไปสู่ส่วนงาน เจ้าของวัตถุประสงค์ และเจ้าของความเสี่ยง พร้อมกำหนดผู้รับผิดชอบและผลส่งมอบให้ชัดเจน กำกับติดตามผลการดำเนินงานและระดับความเสี่ยง และใช้ข้อมูลจากส่วนงานประกอบการทบทวนทิศทาง เกณฑ์ และการจัดสรรทรัพยากร

4.3.2 การบริหารจากล่างขึ้นบน (Bottom-up Approach)

ส่วนงานและหน่วยงานต้องระบุ ประเมิน และบริหารความเสี่ยงและโอกาสที่เกี่ยวข้องกับวัตถุประสงค์ กระบวนงาน โครงการ ระบบ และบริการในความรับผิดชอบ โดยเชื่อมโยงกับทิศทางและกรอบกลางของมหาวิทยาลัย อย่างน้อยต้องดำเนินการดังต่อไปนี้

1. วิเคราะห์บริบทและกำหนดวัตถุประสงค์: ระบุขอบเขต ภารกิจ ผู้มีส่วนได้ส่วนเสีย วัตถุประสงค์ ผลลัพธ์ ตัวชี้วัด และสมมติฐานที่เกี่ยวข้อง

2. ระบุความเสี่ยงอย่างชัดเจน: เขียนข้อความความเสี่ยงตามโครงสร้างสาเหตุ–เหตุการณ์–ผลกระทบ (Cause–Event–Impact) และแสดงความเชื่อมโยงกับวัตถุประสงค์ที่อาจได้รับผลกระทบ

3. จัดทำและทบทวนทะเบียนความเสี่ยง: บันทึกความเสี่ยงในทะเบียนความเสี่ยง (Risk Register) โดยใช้ประเภทความเสี่ยง เกณฑ์ และข้อมูลตามมาตรฐานกลาง พร้อมปรับปรุงเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4. ประเมินความเสี่ยงและการควบคุม: ประเมินความเสี่ยงโดยธรรมชาติ (Inherent Risk) ประเมินการออกแบบ การนำไปใช้ และประสิทธิผลของการควบคุม และประเมินความเสี่ยงคงเหลือ (Residual Risk) จากหลักฐาน ณ วันที่ประเมิน โดยแยกจากระดับความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk)

5. กำหนดผู้รับผิดชอบ: ระบุเจ้าของความเสี่ยง (Risk Owner) เจ้าของการควบคุม (Control Owner) เจ้าของมาตรการ (Action Owner) และเจ้าของข้อมูล (Data Owner) พร้อมขอบเขตหน้าที่และอำนาจที่เกี่ยวข้อง

6. กำหนดตัวชี้วัดและเกณฑ์ตอบสนอง: กำหนด KRI และเกณฑ์ที่เชื่อมโยงกับกรอบ RA/RT ที่ได้รับอนุมัติ พร้อมนิยาม วิธีคำนวณ แหล่งข้อมูล ความถี่ และ Trigger/Action หากจำเป็นต้องกำหนดหรือปรับเกณฑ์เฉพาะส่วนงาน ให้เสนอพิจารณาตามอำนาจ โดยไม่ผ่อนคลายกรอบของมหาวิทยาลัยเอง

7. ดำเนินและติดตามมาตรการ: จัดทำแผนตอบสนอง ดำเนินมาตรการ เก็บหลักฐาน และติดตามทั้งความก้าวหน้าของงานกับผลที่เกิดขึ้นต่อระดับความเสี่ยง

8. รายงานและยกระดับ: รายงานตามรอบและยกระดับเมื่อเข้าเงื่อนไขที่กำหนด เช่น เกิน RT เกินอำนาจหรือขีดความสามารถของส่วนงาน การควบคุมสำคัญไม่ทำงาน หรือมีผลกระทบข้ามส่วนงาน โดยไม่รอรอบรายงานปกติหากเป็นเหตุเร่งด่วน

เจ้าของข้อมูลต้องตรวจสอบคุณภาพและความทันเวลาของข้อมูล เจ้าของความเสี่ยงต้องยืนยันผลการประเมินและสถานะการจัดการ และผู้บริหารส่วนงานต้องรับรองรายงานตามบทบาทและสายการรายงาน ก่อนนำข้อมูลไปใช้จัดทำรายงานภาพรวม ทั้งนี้ การตรวจสอบหรือรับรองข้อมูลต้องไม่ทำให้การแจ้งเหตุฉุกเฉินหรือการยกระดับเร่งด่วนล่าช้า ข้อมูลที่ยังไม่ยืนยันให้ระบุสถานะและปรับปรุงเพิ่มเติมภายหลัง

4.3.3 การบูรณาการแนวราบและภาพรวมมหาวิทยาลัย (Horizontal Integration and Portfolio View)

หน่วยบริหารความเสี่ยงทำหน้าที่รวบรวม วิเคราะห์ สอบทานคุณภาพข้อมูล และให้ข้อเสนอแนะอย่างสร้างสรรค์ต่อข้อมูลจากแนวทาง Top-down และ Bottom-up โดยประสานกับหน่วยงานด้านยุทธศาสตร์ การเงิน กฎหมาย เทคโนโลยีดิจิทัล ความปลอดภัย BCM/BCP คุณภาพ และหน้าที่กำกับเฉพาะด้าน เพื่อให้เห็นความเสี่ยงที่เชื่อมโยงกันระหว่างส่วนงานและผลกระทบต่อมหาวิทยาลัยโดยรวม

การวิเคราะห์ภาพรวมความเสี่ยงต้องพิจารณาอย่างน้อยดังต่อไปนี้

1. ความเชื่อมโยงกับยุทธศาสตร์: วัตถุประสงค์ ผลลัพธ์ และพันธกิจสำคัญที่ความเสี่ยงแต่ละรายการอาจส่งผลกระทบ

2. ระดับและแนวโน้มความเสี่ยง: ความเสี่ยงคงเหลือ การเปลี่ยนแปลงจากรอบก่อน ความเร่งด่วน และระยะเวลาที่อาจเกิดผลกระทบ

3. สถานะเทียบกับกรอบ RA/RT: ค่าและแนวโน้ม KRI สัญญาณเตือน การเกินเกณฑ์ และสถานะการตอบสนองหรือยกระดับ

4. ความสัมพันธ์และการพึ่งพาระหว่างความเสี่ยง: ความเสี่ยงที่เป็นสาเหตุ ส่งเสริม หรือส่งผลต่อกัน รวมถึงการพึ่งพากระบวนการ ระบบ และบุคคลภายนอกร่วมกัน

5. ผลกระทบร่วมและการกระจุกตัว: ความเสี่ยงที่พึ่งพาผู้ให้บริการ แหล่งรายได้ ข้อมูล เทคโนโลยี บุคลากร หรือทรัพยากรเดียวกัน และอาจก่อให้เกิดความเสียหายพร้อมกันหรือเป็นลูกโซ่

6. ความเสี่ยงเกิดใหม่และการเปลี่ยนแปลงบริบท: ประเด็นที่ยังไม่ปรากฏชัดในทะเบียนความเสี่ยง หรือการเปลี่ยนแปลงที่ทำให้สมมติฐานและผลการประเมินเดิมไม่เหมาะสม

7. ความเพียงพอของการควบคุมและมาตรการ: ช่องว่างของการควบคุม มาตรการที่ซ้ำซ้อนหรือขัดกัน และมาตรการที่ต้องอาศัยความร่วมมือจากหลายส่วนงาน

8. ทรัพยากรและประเด็นที่ต้องตัดสินใจ: ทางเลือก ลำดับความสำคัญ และการสนับสนุนที่ต้องได้รับการพิจารณาในระดับมหาวิทยาลัย

กรณีความเสี่ยงเกี่ยวข้องกับหลายส่วนงาน ต้องเสนอให้กำหนดเจ้าของความเสี่ยงหลัก (Lead Risk Owner) และกลไกประสานงานที่ชัดเจน เพื่อลดความซ้ำซ้อนและป้องกันช่องว่างความรับผิดชอบ โดยเจ้าของความเสี่ยงเดิมยังคงรับผิดชอบจนกว่าจะมีการมอบหมายอย่างเป็นทางการ

ข้อมูลสรุปสถานะความเสี่ยงระดับมหาวิทยาลัย (University Risk Profile) และมุมมองความเสี่ยงในภาพรวม (Portfolio View) ต้องอาศัยข้อมูลที่เจ้าของความเสี่ยงยืนยัน ผ่านการกลั่นกรองของฝ่ายบริหาร และนำเสนอคณะกรรมการหรือผู้กำกับดูแลตามอำนาจหน้าที่ หน่วยบริหารความเสี่ยงรับผิดชอบการสังเคราะห์และสอบทานคุณภาพข้อมูล แต่ไม่รับรองข้อมูลหรือบริหารความเสี่ยงแทนเจ้าของความเสี่ยง

การจัดทำภาพรวมต้องวิเคราะห์ความสัมพันธ์และผลกระทบรวม มิใช่เพียงรวบรวมรายการหรือบวกคะแนนความเสี่ยงของแต่ละส่วนงาน เนื่องจากคะแนนจาก Risk Matrix ไม่ใช่มูลค่าความเสียหายที่สามารถนำมารวมกันโดยตรง ส่วนการบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัยต้องผ่านการพิจารณาและอนุมัติตามเกณฑ์และอำนาจที่กำหนด

ผลการวิเคราะห์ภาพรวมให้ใช้เป็นข้อมูลป้อนกลับเพื่อทบทวนยุทธศาสตร์ กรอบ RA/RT มาตรการ และการจัดสรรทรัพยากร พร้อมถ่ายทอดข้อสั่งการกลับไปยังส่วนงาน เพื่อให้การกำหนดทิศทาง การปฏิบัติ และการเรียนรู้เชื่อมโยงกันอย่างต่อเนื่อง

4.4 กระบวนการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้

มหาวิทยาลัยแม่โจ้กำหนดกระบวนการบริหารความเสี่ยง 8 ขั้นตอน เพื่อใช้เป็นแนวทางปฏิบัติร่วมกันในระดับมหาวิทยาลัย ส่วนงาน กระบวนงาน และโครงการ ดังตารางที่ 4-2 โดยประยุกต์ใช้กรอบอ้างอิงให้เหมาะสมกับบริบทของมหาวิทยาลัย มิใช่ขั้นตอนที่ ISO 31000:2018 หรือ COSO ERM 2017 กำหนดไว้โดยตรง

กระบวนการนี้เป็นวงจรต่อเนื่อง ครอบคลุมการกำกับดูแลและกำหนดบริบท การกำหนดวัตถุประสงค์และเกณฑ์ การระบุ วิเคราะห์ และประเมินความเสี่ยง การเลือกและดำเนินมาตรการ ตลอดจนการสื่อสาร รายงาน ติดตาม ทบทวน และปรับปรุง โดยเชื่อมโยงกับบทบาทและอำนาจตัดสินใจที่กำหนดไว้ในส่วนที่ 3

การสื่อสารและปรึกษาหารือ (Communication and Consultation) การติดตามและทบทวน (Monitoring and Review) และการบันทึกและรายงาน (Recording and Reporting) ต้องดำเนินการตลอดทั้งกระบวนการ แม้จะกำหนดขั้นตอนเฉพาะเพื่อเน้นความรับผิดชอบและผลผลิตของกิจกรรมดังกล่าวก็ตาม

ตารางที่ 4-2 ***ตารางแสดงกระบวนการบริหารความเสี่ยงของมหาวิทยาลัยแม่โจ้ 8 ขั้นตอน***

ขั้นตอน	กระบวนการ	คำถามสำคัญ	ผลผลิตและผลลัพธ์ขั้นต่ำ
1	**กำกับดูแลและกำหนดบริบท**	ประเมินเรื่องใด ภายในขอบเขตและช่วงเวลาใด ใครรับผิดชอบ และปัจจัยภายในหรือภายนอกใดเกี่ยวข้องกับการบรรลุวัตถุประสงค์	ขอบเขตและกรอบเวลา บริบท ผู้มีส่วนได้ส่วนเสีย สมมติฐานสำคัญ บทบาทผู้รับผิดชอบ อำนาจตัดสินใจ และสายการรายงาน
2	**กำหนดวัตถุประสงค์และเกณฑ์ความเสี่ยง**	ต้องบรรลุผลลัพธ์ใด วัดผลอย่างไร และใช้เกณฑ์ใดประเมิน ยอมรับหรือตอบสนองต่อความเสี่ยง	วัตถุประสงค์ เจ้าของวัตถุประสงค์ KPI และเป้าหมาย กรอบ Risk Capacity และ RA/RT ที่เกี่ยวข้อง เกณฑ์โอกาสเกิดและผลกระทบ เกณฑ์ระดับความเสี่ยง และเงื่อนไขตอบสนองหรือยกระดับ โดยระบุแหล่งอ้างอิงและสถานะการอนุมัติ

ขั้นตอน	กระบวนการ	คำถามสำคัญ	ผลผลิตและผลลัพธ์ขั้นต่ำ
3	**ระบุความเสี่ยงและโอกาส**	เหตุการณ์หรือความไม่แน่นอนใดอาจเกิดขึ้น มีสาเหตุหรือปัจจัยขับเคลื่อนอะไร และอาจส่งผลต่อวัตถุประสงค์อย่างไร	ข้อความความเสี่ยงตามโครงสร้างสาเหตุ–เหตุการณ์–ผลกระทบ ประเภทความเสี่ยงและมิติผลกระทบ เจ้าของความเสี่ยง ข้อมูลหรือหลักฐานที่ใช้ระบุและทะเบียนความเสี่ยงเบื้องต้น
4	**วิเคราะห์และประเมินความเสี่ยง**	ความเสี่ยงโดยธรรมชาติและความเสี่ยงคงเหลืออยู่ในระดับใด การควบคุมทำงานได้จริงหรือไม่ และความเสี่ยงคงเหลือสอดคล้องกับ RA/RT หรือเข้าเกณฑ์ยกระดับหรือไม่	ผลประเมิน Inherent Risk รายละเอียดการควบคุมและเจ้าของการควบคุม ผลประเมินการออกแบบ การนำไปใช้ และประสิทธิผลพร้อมหลักฐาน ผลประเมิน Residual Risk ณ วันที่ประเมิน สถานะเทียบ RA/RT ลำดับความสำคัญ และเหตุผลการใช้ Override หากมี
5	**ตอบสนองและจัดทำแผนบริหารความเสี่ยง**	จะเลือกแนวทางจัดการใด ใครรับผิดชอบ ต้องใช้ทรัพยากรเท่าใด และต้องการบรรลุระดับความเสี่ยงหรือผลลัพธ์ใดภายในเวลาใด	แนวทางตอบสนองและเหตุผล แผนบริหารความเสี่ยง เจ้าของมาตรการ ผลส่งมอบ ทรัพยากร กำหนดเวลา Target Residual Risk ตัวชี้วัดและเงื่อนไขติดตาม รวมถึงหลักฐานการอนุมัติหรือยอมรับความเสี่ยงตามอำนาจ
6	**ดำเนินการควบคุมและมาตรการ**	การควบคุมและมาตรการได้รับการดำเนินการจริงตามแผนหรือไม่ มีข้อบกพร่องใด และมีหลักฐานว่าช่วยจัดการความเสี่ยงได้เพียงใด	หลักฐานการปฏิบัติ สถานะและผลส่งมอบของมาตรการ ผลการทดสอบหรือประเมินการควบคุม ข้อบกพร่อง มาตรการแก้ไข ผู้รับผิดชอบ และกำหนดแล้วเสร็จ
7	**สื่อสาร รายงาน และยกระดับ**	ใครต้องได้รับข้อมูล เมื่อใด ผ่านช่องทางใด มีเรื่องใดต้องตัดสินใจ และเข้าเงื่อนไขรายงานเร่งด่วนหรือไม่	ค่าและแนวโน้ม KRI/EWS รายงานหรือ Dashboard ตามความจำเป็น ข้อเสนอเพื่อการตัดสินใจ บันทึกเหตุการณ์และการยกระดับ และบันทึกการตัดสินใจ

ขั้นตอน	กระบวนการ	คำถามสำคัญ	ผลผลิตและผลลัพธ์ขั้นต่ำ
			(Decision Log) พร้อมผู้รับผิดชอบดำเนินการตามข้อสั่งการ
8	**ติดตาม ทบทวน และปรับปรุงอย่างต่อเนื่อง**	บริบท สมมติฐาน และระดับความเสี่ยงเปลี่ยนแปลงหรือไม่ มาตรการได้ผลตามเป้าหมายหรือไม่ และต้องปรับปรุงเรื่องใด	ทะเบียนความเสี่ยงและผลประเมินความเสี่ยงคงเหลือที่ปรับปรุงแล้ว Risk Profile และ Portfolio View ตามขอบเขต ผลการทบทวนของฝ่ายบริหาร บทเรียน และแผนปรับปรุง พร้อมผู้รับผิดชอบและกำหนดเวลา

ภาพที่ 4-2 ภาพแสดงกระบวนการบริหารความเสี่ยง 8 ขั้นตอน

ที่มา: งานบริหารความเสี่ยงและการควบคุมภายใน กองพัฒนาคุณภาพ สำนักงานมหาวิทยาลัย มหาวิทยาลัยแม่โจ้ (2570) จัดทำโดยประยุกต์ใช้ ISO 31000:2018, COSO ERM 2017 และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562

รายละเอียดวิธีดำเนินการและผลผลิตของแต่ละขั้นตอนอธิบายในข้อ 4.5–4.12 ส่วนงานให้ใช้ตารางที่ 4-2 เป็นรายการตรวจสอบภาพรวม และใช้แบบ RISK-MJU-01 ในภาคผนวก ก บันทึกข้อมูลตั้งแต่วัตถุประสงค์จนถึงการติดตามผล โดยเชื่อมโยงกับหลักฐานจากระบบงานปกติและแบบบันทึกที่เกี่ยวข้อง เพื่อให้ตรวจสอบย้อนกลับได้และลดการจัดทำข้อมูลซ้ำซ้อน ทั้งนี้ การดำเนินงานสามารถย้อนกลับไปทบทวนขั้นตอนก่อนหน้าได้เมื่อบริบท วัตถุประสงค์ สมมติฐาน ข้อมูล หรือระดับความเสี่ยงเปลี่ยนแปลง ทั้งนี้ ให้ยึดหลักปฏิบัติสำคัญดังต่อไปนี้

1. กำหนดตัวชี้วัดก่อนนำไปติดตาม: จัดทำหรือปรับปรุง KRI นิยามข้อมูล เกณฑ์เตือน และ Trigger/Action ในขั้นกำหนดเกณฑ์ ประเมินความเสี่ยง และจัดทำแผน ไม่รอจนถึงขั้นรายงาน

2. ประเมินความเสี่ยงคงเหลือจากสภาพจริง: การอนุมัติแผนหรือความก้าวหน้าของกิจกรรมเพียงอย่างเดียวไม่ถือเป็นหลักฐานว่าความเสี่ยงลดลง ต้องประเมินจากการควบคุมที่นำไปใช้และผลที่เกิดขึ้นจริง โดยแยก Residual Risk ออกจาก Target Residual Risk ให้ชัดเจน

3. ตอบสนองและยกระดับทันทีเมื่อจำเป็น: หากพบเหตุฉุกเฉิน เหตุ Zero Tolerance หรือเข้าเกณฑ์ยกระดับ ให้ดำเนินการคุ้มครอง ระงับเหตุ และรายงานตามข้อ 3.6 และข้อ 3.9 โดยไม่รอให้ครบทั้ง 8 ขั้นตอนหรือรอรอบรายงานปกติ

4. ติดตามทั้งกิจกรรมและผลลัพธ์: พิจารณาความก้าวหน้าของมาตรการควบคู่กับแนวโน้ม KRI ประสิทธิผลของการควบคุม และระดับความเสี่ยงคงเหลือ เพื่อให้ทราบว่าการดำเนินการช่วยสนับสนุนวัตถุประสงค์ได้จริงหรือจำเป็นต้องปรับมาตรการ

ทุกขั้นตอนต้องมีผู้รับผิดชอบ ข้อมูล และหลักฐานที่เหมาะสมกับระดับความเสี่ยง โดยการบันทึกและรายงานต้องช่วยให้สามารถตรวจสอบได้ว่า ความเสี่ยงมีที่มาอย่างไร ใช้เกณฑ์และข้อมูลใดในการประเมิน เลือกมาตรการด้วยเหตุผลใด และผลการติดตามนำไปสู่การตัดสินใจหรือการปรับปรุงอย่างไร

4.5 ขั้นตอนที่ 1 การกำกับดูแลและกำหนดบริบท (Governance and Context Setting)

การกำกับดูแลและกำหนดบริบทเป็นการวางรากฐานของการประเมินความเสี่ยง เพื่อให้ผู้เกี่ยวข้องเข้าใจตรงกันเกี่ยวกับวัตถุประสงค์ ขอบเขต กรอบเวลา สมมติฐาน ผู้รับผิดชอบ ผู้มีส่วนได้ส่วนเสีย และปัจจัยที่อาจส่งผลต่อการบรรลุวัตถุประสงค์ รวมทั้งกำหนดบทบาทและอำนาจตัดสินใจให้สอดคล้องกับโครงสร้างการกำกับดูแลของมหาวิทยาลัย

ข้อมูลที่ใช้ต้องเหมาะสมกับระดับและวัตถุประสงค์ของการประเมิน สามารถบันทึกรวมไว้ในแบบบันทึกบริบทและขอบเขตความเสี่ยง (Risk Context and Scope Record) ทะเบียนความเสี่ยง (Risk Register) หรือเอกสารที่เกี่ยวข้องได้ โดยไม่จำเป็นต้องจัดทำเอกสารแยกหลายชุด หากมีสาระครบถ้วนและตรวจสอบย้อนกลับได้

4.5.1 การกำหนดขอบเขต (Scope Definition)

ก่อนประเมินความเสี่ยง ต้องกำหนดขอบเขตให้ชัดเจนอย่างน้อยดังต่อไปนี้

1. ระดับการประเมิน (Assessment Level): ระบุระดับมหาวิทยาลัย ส่วนงาน กระบวนงาน โครงการ ระบบสารสนเทศ หรือกิจกรรมที่ต้องการประเมิน

2. วัตถุประสงค์ของการประเมิน (Assessment Purpose): ระบุว่าการประเมินจัดทำขึ้นเพื่อสนับสนุนการตัดสินใจ การจัดทำแผน การอนุมัติโครงการ การปรับปรุงการควบคุม หรือวัตถุประสงค์อื่นใด โดยแยกจากวัตถุประสงค์ของภารกิจที่นำมาประเมิน

3. ขอบเขตภารกิจและกระบวนงาน (Functional and Process Scope): ระบุกิจกรรม หน่วยงาน ระบบ พื้นที่ และกลุ่มผู้มีส่วนได้ส่วนเสียที่อยู่ในขอบเขต รวมถึงจุดเชื่อมโยงกับกิจกรรมหรือหน่วยงานนอกขอบเขต

4. กรอบเวลาที่ใช้ในการประเมิน (Time Horizon): ระบุช่วงเวลาที่พิจารณาการเกิดและผลกระทบของความเสี่ยง เช่น ปีงบประมาณ ระยะเวลาแผนยุทธศาสตร์ อายุโครงการ หรือช่วงเปลี่ยนผ่านที่สำคัญ

5. มิติและขอบเขตผลกระทบ (Impact Dimensions and Scope): พิจารณาผลกระทบต่อยุทธศาสตร์ การดำเนินงาน การเงิน การปฏิบัติตามกฎหมาย เทคโนโลยีดิจิทัล ชื่อเสียง ความปลอดภัย สิ่งแวดล้อม ความต่อเนื่อง และผู้มีส่วนได้ส่วนเสียตามความเกี่ยวข้อง

6. ความสัมพันธ์และการพึ่งพา (Relationships and Dependencies): ระบุส่วนงาน ระบบ ผู้รับจ้าง ผู้ให้บริการ คู่สัญญา และทรัพยากรที่การดำเนินงานต้องพึ่งพา รวมทั้งจุดที่อาจทำให้เกิดผลกระทบต่อเนื่องหรือเป็นลูกโซ่

7. ผู้รับผิดชอบและผู้มีอำนาจตัดสินใจ (Accountability and Decision Authority): ระบุเจ้าของวัตถุประสงค์ ผู้กำกับดูแล ผู้อนุมัติ และผู้มีอำนาจยอมรับความเสี่ยง พร้อมเส้นทางการยกระดับตามเอกสารให้อำนาจที่เกี่ยวข้อง

8. ทรัพยากรและข้อจำกัด (Resources and Constraints): ระบุข้อจำกัดด้านงบประมาณ บุคลากร เวลา ข้อมูล เทคโนโลยี กฎหมาย และข้อผูกพันที่มีผลต่อการประเมินหรือการจัดการความเสี่ยง

9. สมมติฐานและรายการนอกขอบเขต (Assumptions and Exclusions): ระบุสมมติฐานที่ใช้ รายการที่ไม่นำมาประเมิน และเหตุผลประกอบ โดยการกำหนดรายการนอกขอบเขตต้องไม่เป็นการยกเว้นหน้าที่ตามกฎหมายหรือทำให้ละเลยความเสี่ยงสำคัญ

การเปลี่ยนแปลงขอบเขตภายหลังเริ่มประเมินต้องได้รับความเห็นชอบจากเจ้าของวัตถุประสงค์หรือผู้มีอำนาจตามโครงสร้างที่กำหนด พร้อมบันทึกเหตุผล วันที่ ผู้ให้ความเห็นชอบ และผลต่อการประเมิน เพื่อให้ตรวจสอบย้อนกลับได้

4.5.2 การวิเคราะห์บริบทภายนอก (External Context Analysis)

ให้พิจารณาปัจจัยภายนอกที่อาจส่งผลต่อวัตถุประสงค์ทั้งในด้านภัยคุกคามและโอกาส โดยเลือกประเด็นที่เกี่ยวข้องกับขอบเขตการประเมิน ดังต่อไปนี้

1. นโยบายภาครัฐและการอุดมศึกษา (Public and Higher Education Policy): ทิศทางนโยบาย การสนับสนุน และเงื่อนไขที่มีผลต่อพันธกิจของมหาวิทยาลัย

2. กฎหมายและข้อกำหนดกำกับดูแล (Legal and Regulatory Requirements): กฎหมาย ระเบียบ มาตรฐาน และข้อกำหนดของหน่วยงานกำกับดูแล

3. เศรษฐกิจและแหล่งเงินทุน (Economic and Funding Conditions): ภาวะเศรษฐกิจ การเงิน เงินเฟ้อ และความเปลี่ยนแปลงของแหล่งงบประมาณหรือแหล่งรายได้

4. ประชากรและผู้เรียน (Demographics and Learners): โครงสร้างประชากร จำนวนผู้เรียนที่มีศักยภาพ ความต้องการ และพฤติกรรมการเลือกศึกษาหรือใช้บริการ

5. ตลาดแรงงานและผู้ใช้บัณฑิต (Labour Market and Graduate Employers): ความต้องการทักษะ สมรรถนะ และกำลังคนของภาคอุตสาหกรรมและผู้ใช้บัณฑิต

6. การแข่งขันและความร่วมมือ (Competition and Collaboration): การเปลี่ยนแปลงด้านการศึกษา การวิจัย นวัตกรรม และเครือข่ายความร่วมมือ

7. เทคโนโลยีและภัยคุกคามไซเบอร์ (Technology and Cyber Threats): ปัญญาประดิษฐ์ เทคโนโลยีดิจิทัล และภัยคุกคามที่อาจกระทบระบบ ข้อมูล หรือรูปแบบการดำเนินงาน

8. ภูมิอากาศและสิ่งแวดล้อม (Climate and Environment): การเปลี่ยนแปลงสภาพภูมิอากาศ ภัยพิบัติ ทรัพยากรธรรมชาติ และความหลากหลายทางชีวภาพ

9. สังคม การเมือง และภูมิรัฐศาสตร์ (Social, Political and Geopolitical Conditions): สถานการณ์ที่อาจกระทบการดำเนินงาน ความร่วมมือ หรือผู้มีส่วนได้ส่วนเสีย

10. ความคาดหวังของผู้มีส่วนได้ส่วนเสีย (Stakeholder Expectations): ความต้องการและความคาดหวังของผู้เรียน ผู้ปกครอง ชุมชน คู่ความร่วมมือ และกลุ่มที่เกี่ยวข้อง

11. ความเสี่ยงและโอกาสเกิดใหม่ (Emerging Risks and Opportunities): ประเด็นที่ยังมีข้อมูลจำกัดหรือเปลี่ยนแปลงอย่างรวดเร็ว แต่อาจส่งผลต่อวัตถุประสงค์ในอนาคต

เครื่องมือที่อาจนำมาใช้ ได้แก่

- การวิเคราะห์ปัจจัยการเมือง เศรษฐกิจ สังคม เทคโนโลยี กฎหมาย และสิ่งแวดล้อม (PESTLE Analysis)
- การวิเคราะห์สถานการณ์สมมติ (Scenario Analysis)
- การสำรวจแนวโน้มและสัญญาณการเปลี่ยนแปลงในอนาคต (Horizon Scanning)
- การสำรวจสภาพแวดล้อมที่เกี่ยวข้อง (Environmental Scanning)
- การเทียบเคียงผลการดำเนินงานและแนวปฏิบัติ (Benchmarking)
- การปรึกษาหารือกับผู้มีส่วนได้ส่วนเสีย (Stakeholder Consultation)
- การวิเคราะห์แนวโน้มและข้อมูล (Trend and Data Analysis)

ให้เลือกใช้เครื่องมือตามวัตถุประสงค์ ความซับซ้อน และข้อมูลที่มี โดยไม่จำเป็นต้องใช้ทุกเครื่องมือในทุกกรณี ผลการวิเคราะห์ควรระบุแหล่งข้อมูล วันที่ของข้อมูล แนวโน้ม และข้อจำกัดที่สำคัญ

4.5.3 การวิเคราะห์บริบทภายใน (Internal Context Analysis)

ให้พิจารณาปัจจัยภายในที่อาจสนับสนุนหรือเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ โดยครอบคลุมประเด็นที่เกี่ยวข้องดังต่อไปนี้

1. ทิศทางและเป้าหมายองค์กร (Organizational Direction and Goals): วิสัยทัศน์ พันธกิจ ยุทธศาสตร์ วัตถุประสงค์ และเป้าหมาย

2. โครงสร้างการกำกับดูแล (Governance Structure): บทบาท ความรับผิดชอบ การมอบอำนาจ และกลไกการตัดสินใจ

3. นโยบาย กระบวนงาน และการควบคุม (Policies, Processes and Controls): นโยบาย ระเบียบ ขั้นตอนการปฏิบัติงาน และระบบควบคุมภายใน

4. บุคลากรและสมรรถนะ (People and Competencies): จำนวน โครงสร้างกำลังคน ความรู้ ทักษะ และความพร้อมของบุคลากร

5. ฐานะและทรัพยากรทางการเงิน (Financial Position and Resources): งบประมาณ รายได้ ต้นทุน สภาพคล่อง และภาระผูกพัน

6. ข้อมูลและเทคโนโลยี (Information and Technology): ระบบข้อมูล คุณภาพข้อมูล เทคโนโลยี และความมั่นคงปลอดภัย

7. ทรัพย์สินและโครงสร้างพื้นฐาน (Assets and Infrastructure): อาคาร สถานที่ เครื่องมือ อุปกรณ์ และสาธารณูปโภค

8. การบริหารความสัมพันธ์กับบุคคลภายนอก (Third-party Relationship Management): การคัดเลือก กำกับ และติดตามผู้รับจ้าง ผู้ให้บริการ และคู่สัญญา รวมถึงระดับการพึ่งพา

9. วัฒนธรรมและพฤติกรรมองค์กร (Organizational Culture and Behaviour): ค่านิยม พฤติกรรม แรงจูงใจ การสื่อสาร และสภาพแวดล้อมในการรายงานข้อกังวล

10. ผลการดำเนินงานและตัวชี้วัด (Performance and Indicators): ผลและแนวโน้มของตัวชี้วัดผลการดำเนินงาน (KPI) และตัวชี้วัดความเสี่ยงที่สำคัญ (KRI)

11. เหตุการณ์และข้อร้องเรียน (Incidents and Complaints): เหตุการณ์ความเสียหาย เหตุการณ์เกือบเกิดความเสียหาย (Near Miss) ข้อร้องเรียน ข้อพิพาท และคดี

12. ผลการประเมินและตรวจสอบ (Assessment and Audit Results): ผลประเมินการควบคุม การตรวจสอบภายในและภายนอก และการประกันคุณภาพ

13. ความพร้อมด้านความต่อเนื่องและการกู้คืน (Continuity and Recovery Readiness): การบริหารความต่อเนื่องขององค์กร (BCM) แผนความต่อเนื่องในการดำเนินงาน (BCP) แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (DRP) และผลการทดสอบแผน

14. บทเรียนและปัญหาที่เกิดซ้ำ (Lessons Learned and Recurring Issues): สาเหตุและผลการแก้ไขประเด็นจากรอบก่อน รวมถึงข้อบกพร่องที่ยังคงค้างอยู่

เครื่องมือที่อาจนำมาใช้ ได้แก่

- **การวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรค (SWOT Analysis)**

- การจัดทำแผนผังกระบวนงาน (Process Mapping)
- การวิเคราะห์ห่วงโซ่คุณค่า (Value Chain Analysis)
- การวิเคราะห์ข้อมูล (Data Analysis)
- การประเมินการควบคุมด้วยตนเอง (Control Self-assessment)
- การสัมภาษณ์ (Interviews)
- การประชุมเชิงปฏิบัติการ (Workshops)
- การทบทวนบทเรียน (Lessons Learned Review)

ผลการวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรคให้ใช้เป็นข้อมูลสนับสนุนการกำหนดบริบท โดยต้องวิเคราะห์ความเชื่อมโยงกับวัตถุประสงค์และโครงสร้างสาเหตุ–เหตุการณ์–ผลกระทบ (Cause–Event–Impact) ก่อนนำไปจัดทำข้อความความเสี่ยง ไม่ใช้รายการจุดอ่อนหรืออุปสรรคเป็นข้อความความเสี่ยงโดยตรง

4.5.4 การวิเคราะห์ผู้มีส่วนได้ส่วนเสีย (Stakeholder Analysis)

ให้ระบุผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับวัตถุประสงค์และขอบเขตการประเมิน พร้อมพิจารณาอย่างน้อยดังต่อไปนี้

1. บทบาทและความสัมพันธ์ (Roles and Relationships): ความเกี่ยวข้องกับภารกิจ กระบวนงาน หรือการตัดสินใจของมหาวิทยาลัย

2. ความต้องการและความคาดหวัง (Needs and Expectations): ผลลัพธ์ บริการ หรือการคุ้มครองที่แต่ละกลุ่มคาดหวัง

3. สิทธิและข้อผูกพัน (Rights and Obligations): สิทธิ หน้าที่ และข้อกำหนดตามกฎหมาย สัญญา หรือข้อตกลง

4. อิทธิพลและผลกระทบ (Influence and Impact): ความสามารถในการส่งผลต่อการดำเนินงาน และระดับผลกระทบที่อาจได้รับ

5. ความเปราะบางและความต้องการการคุ้มครอง (Vulnerability and Protection Needs): ลักษณะของกลุ่มที่อาจได้รับผลกระทบรุนแรงหรือมีข้อจำกัดในการปกป้องสิทธิและเข้าถึงความช่วยเหลือ

6. ผลกระทบที่ไม่อาจยอมรับได้ (Unacceptable Impacts): ผลกระทบที่ขัดต่อกฎหมาย สิทธิ หรือข้อกำหนดการคุ้มครองที่เกี่ยวข้อง รวมถึงประเด็นที่ต้องเสนอพิจารณากำหนดเกณฑ์ตอบสนองเป็นพิเศษ

7. การสื่อสารและปรึกษาหารือ (Communication and Consultation): ช่องทาง ความถี่ ผู้รับผิดชอบ และวิธีเข้าถึงแต่ละกลุ่มอย่างเหมาะสม

8. ข้อมูลและมุมมองประกอบการประเมิน (Assessment Inputs and Perspectives): ข้อมูล ประสบการณ์ และข้อกังวลที่ควรนำมาใช้ในการระบุและประเมินความเสี่ยง

ความคาดหวังของผู้มีส่วนได้ส่วนเสียไม่ถือเป็นข้อผูกพันของมหาวิทยาลัยทั้งหมดโดยอัตโนมัติ ต้องพิจารณาร่วมกับกฎหมาย นโยบาย ยุทธศาสตร์ ทรัพยากร และอำนาจหน้าที่ โดยไม่ลดทอนสิทธิหรือหน้าที่การคุ้มครองที่กฎหมายกำหนด

4.5.5 การกำหนดบทบาทและโครงสร้างการตัดสินใจ (Governance Roles and Decision Structure)

ก่อนเริ่มประเมิน ต้องระบุบทบาท ผู้รับผิดชอบ และขอบเขตอำนาจอย่างน้อยดังต่อไปนี้

1. เจ้าของวัตถุประสงค์ (Objective Owner): ผู้รับผิดชอบต่อผลลัพธ์ของภารกิจที่นำมาประเมิน

2. ผู้รับผิดชอบนำการประเมิน (Assessment Lead): ผู้วางแผนและประสานการประเมินให้ครบถ้วนตามขอบเขต

3. ผู้เข้าร่วมและผู้เชี่ยวชาญ (Participants and Subject Matter Experts): ผู้ให้ข้อมูลและความเห็นที่จำเป็นต่อการประเมิน

4. ผู้สอบทานคุณภาพการประเมิน (Assessment Quality Reviewer): ผู้สอบทานความครบถ้วน ความสอดคล้องของเกณฑ์ สมมติฐาน และหลักฐาน โดยการสอบทานไม่ทดแทนความรับผิดชอบของเจ้าของความเสี่ยง

5. ผู้มีอำนาจพิจารณาหรืออนุมัติผลการประเมิน (Assessment Review or Approval Authority): ผู้พิจารณาผลตามโครงสร้างและอำนาจที่กำหนด ทั้งนี้ การอนุมัติผลการประเมินไม่ถือเป็นการอนุมัติยอมรับความเสี่ยงโดยอัตโนมัติ

6. ผู้มีอำนาจยอมรับความเสี่ยงและผู้รับการยกระดับ (Risk Acceptance Authority and Escalation Recipient): ผู้มีอำนาจตัดสินใจตามระดับความเสี่ยง ขอบเขตผลกระทบ และการมอบอำนาจ

7. เส้นทางและระยะเวลาการรายงาน (Reporting Routes and Timelines): ผู้รับรายงาน ช่องทาง และกำหนดเวลาสำหรับการรายงานตามรอบและการรายงานเร่งด่วน

8. ผู้ประสานงานและผู้ดูแลบันทึก (Coordinator and Record Custodian): ผู้ประสานข้อมูล จัดเก็บหลักฐาน และควบคุมฉบับของเอกสาร

9. วิธีจัดการผลประโยชน์ทับซ้อน (Conflict of Interest Management): การเปิดเผยความเกี่ยวข้อง การจัดผู้สอบทานทดแทน หรือการงดร่วมพิจารณาตามความเหมาะสมและข้อกำหนดที่เกี่ยวข้อง

อาจกำหนดเจ้าของความเสี่ยง (Risk Owner) เบื้องต้นตามเจ้าของวัตถุประสงค์หรือกระบวนงาน และยืนยันเมื่อระบุความเสี่ยงในขั้นตอนที่ 3 ส่วนเจ้าของการควบคุม (Control Owner) ให้ระบุเมื่อทบทวนการควบคุมที่มีอยู่ และเจ้าของมาตรการ (Action Owner) ให้กำหนดเมื่อเลือกมาตรการในขั้นตอนที่ 5

การกำหนดบทบาทต้องสอดคล้องกับหลัก Three Lines และเอกสารให้อำนาจที่มีผลใช้บังคับ โดยไม่มอบหมายให้กองตรวจสอบภายในเป็นเจ้าของความเสี่ยงหรือผู้อนุมัติการยอมรับความเสี่ยงแทนฝ่ายบริหาร

4.5.6 ข้อมูลพื้นฐานสำหรับกำหนดเกณฑ์ความเสี่ยง (Baseline Information for Risk Criteria)

ให้รวบรวมข้อมูลที่จำเป็นต่อการเลือกใช้หรือกำหนดเกณฑ์ในขั้นตอนที่ 2 อย่างน้อยดังต่อไปนี้

1. **ผลกระทบที่ไม่อาจยอมรับได้ (Unacceptable Impacts):** ข้อมูลเกี่ยวกับผลกระทบต่อมหาวิทยาลัยและผู้มีส่วนได้ส่วนเสียที่ต้องป้องกันหรือกำหนดเงื่อนไขตอบสนองเป็นพิเศษ
2. **ข้อจำกัดทางกฎหมายและเหตุที่ไม่ยอมรับ (Legal Constraints and Zero Tolerance):** ข้อห้าม หน้าที่ตามกฎหมาย และเหตุ Zero Tolerance ตามนโยบายที่เกี่ยวข้อง
3. **เป้าหมายและความเบี่ยงเบนของผลการดำเนินงาน (Performance Targets and Deviations):** เป้าหมายของ KPI และข้อมูลความเบี่ยงเบนที่อาจกระทบการบรรลุวัตถุประสงค์ ทั้งนี้ความเบี่ยงเบนของ KPI ไม่ถือเป็น RT โดยอัตโนมัติ
4. **ข้อมูลเหตุการณ์และความเสียหายในอดีต (Historical Incident and Loss Data):** ความถี่ ความรุนแรง สาเหตุ และผลกระทบของเหตุการณ์ รวมถึงเหตุการณ์เกือบเกิดความเสียหาย
5. **ขีดความสามารถและทรัพยากร (Capabilities and Resources):** ความพร้อมด้านการเงิน บุคลากร เทคโนโลยี การควบคุม การตอบสนอง และการฟื้นตัว

6. เกณฑ์และข้อกำหนดเฉพาะด้าน (Specific Criteria and Requirements): เกณฑ์กลางของมหาวิทยาลัย ข้อกำหนดทางวิชาชีพ สัญญา หรือข้อกำหนดกำกับเฉพาะด้านที่เกี่ยวข้อง

การเลือกใช้เกณฑ์โอกาสเกิด (Likelihood) ผลกระทบ (Impact) ตารางประเมินระดับความเสี่ยง (Risk Matrix) กรอบ RA/RT เกณฑ์ยกระดับเป็นกรณีพิเศษ (Override Criteria) และเกณฑ์การยกระดับความเสี่ยง (Risk Escalation Criteria) ให้ดำเนินการในขั้นตอนที่ 2 ตามข้อ 4.6 โดยยึดเกณฑ์ที่ได้รับอนุมัติแล้วเป็นฐาน

หากจำเป็นต้องกำหนดหรือปรับเกณฑ์เฉพาะ ให้เสนอพิจารณาตามอำนาจ พร้อมเหตุผลและหลักฐานก่อนนำไปใช้ ไม่ปรับเกณฑ์ย้อนหลังเพื่อให้ได้คะแนนหรือระดับความเสี่ยงตามที่ต้องการ

4.5.7 ผลผลิตขั้นต่ำของขั้นตอนที่ 1 (Minimum Outputs of Step 1)

เมื่อสิ้นสุดขั้นตอนนี้ ต้องมีข้อมูลและหลักฐานอย่างน้อยดังต่อไปนี้

1. ขอบเขตและวัตถุประสงค์ของการประเมินความเสี่ยง (Risk Assessment Scope and Purpose)
2. ผลการวิเคราะห์บริบทภายในและภายนอก (Internal and External Context Analysis)
3. แผนที่หรือข้อมูลสรุปผู้มีส่วนได้ส่วนเสีย (Stakeholder Map or Summary)
4. กรอบเวลาที่ใช้ในการประเมิน (Time Horizon)
5. สมมติฐานและข้อจำกัด (Assumptions and Constraints)
6. การพึ่งพาและจุดเชื่อมโยงกับระบบหรือหน่วยงานอื่น (Dependencies and Interfaces)
7. โครงสร้างบทบาทและอำนาจตัดสินใจ (Roles and Decision Authority Structure)
8. แหล่งข้อมูลและเจ้าของข้อมูลเบื้องต้น (Preliminary Data Sources and Data Owners)
9. ข้อมูลพื้นฐานสำหรับกำหนดเกณฑ์ความเสี่ยง (Baseline Information for Risk Criteria)
10. กำหนดการประเมินและการรายงาน (Assessment and Reporting Schedule)

ข้อมูลดังกล่าวอาจบันทึกรวมในแบบบันทึกบริบทและขอบเขตความเสี่ยง (Risk Context and Scope Record) ฉบับเดียว หรือเชื่อมโยงกับทะเบียนความเสี่ยงและเอกสารที่มีอยู่ โดยระบุวันที่จัดทำ ผู้รับผิดชอบ และฉบับของข้อมูลให้ชัดเจน เพื่อใช้เป็นข้อมูลตั้งต้นสำหรับขั้นตอนที่ 2 และทบทวนได้เมื่อบริบทเปลี่ยนแปลง

4.6 ขั้นตอนที่ 2 การกำหนดวัตถุประสงค์และเกณฑ์ความเสี่ยง (Objectives and Risk Criteria)

การบริหารความเสี่ยงต้องอ้างอิงวัตถุประสงค์ที่ชัดเจน เนื่องจากความเสี่ยงหมายถึงผลกระทบของความไม่แน่นอนต่อวัตถุประสงค์ การระบุความเสี่ยงโดยไม่มีวัตถุประสงค์อ้างอิงอาจทำให้ได้เพียงรายการปัญหาทั่วไป ซึ่งไม่สามารถประเมิน จัดลำดับความสำคัญ กำหนดเจ้าของความเสี่ยง หรือนำไปใช้ประกอบการตัดสินใจได้อย่างเหมาะสม

ในขั้นตอนนี้ ให้นำข้อมูลบริบทและขอบเขตจากขั้นตอนที่ 1 มากำหนดหรือยืนยันวัตถุประสงค์ เป้าหมาย และเกณฑ์ที่จะใช้ประเมินและจัดการความเสี่ยง โดยยึดเกณฑ์กลางและกรอบการยอมรับความเสี่ยงที่ได้รับอนุมัติแล้วเป็นฐาน หากจำเป็นต้องกำหนดเกณฑ์เฉพาะ ให้เสนอพิจารณาตามอำนาจก่อนนำไปใช้

4.6.1 การกำหนดวัตถุประสงค์และเป้าหมาย (Objective and Target Setting)

วัตถุประสงค์ควรมีคุณลักษณะตามหลัก SMART และมีเจ้าของวัตถุประสงค์ที่ชัดเจน ดังต่อไปนี้

1. **เฉพาะเจาะจง (Specific):** ระบุผลลัพธ์ที่ต้องการบรรลุและขอบเขตให้เข้าใจตรงกัน
2. **วัดผลหรือตรวจสอบได้ (Measurable):** มีตัวชี้วัดหรือหลักฐานที่ใช้ยืนยันความสำเร็จ
3. **มีความเป็นไปได้ (Achievable):** สอดคล้องกับทรัพยากร ขีดความสามารถ และข้อจำกัด
4. **เกี่ยวข้องกับทิศทางองค์กร (Relevant):** เชื่อมโยงกับยุทธศาสตร์ พันธกิจ หรือภารกิจที่รับผิดชอบ
5. **มีกรอบเวลาชัดเจน (Time-bound):** ระบุช่วงเวลาหรือกำหนดแล้วเสร็จ
6. **มีเจ้าของวัตถุประสงค์ (Objective Owner):** ระบุผู้รับผิดชอบต่อผลลัพธ์และการติดตามความสำเร็จ

ตัวอย่าง: “รักษาสภาพคล่องให้เพียงพอต่อการดำเนินพันธกิจสำคัญและชำระภาระผูกพันตลอดปีงบประมาณ พ.ศ. 2570 โดยติดตามประมาณการกระแสเงินสดและจำนวนวันที่สามารถดำเนินงานได้ด้วยเงินสดที่มีอยู่ทุกเดือน และมีผู้บริหารที่กำกับด้านการเงินเป็นเจ้าของวัตถุประสงค์”

วัตถุประสงค์ของภารกิจต้องแยกจากวัตถุประสงค์ของการประเมิน เช่น “รักษาสภาพคล่อง” เป็นวัตถุประสงค์ของภารกิจ ส่วน “ประเมินเพื่อประกอบการอนุมัติแผนสภาพคล่อง” เป็นวัตถุประสงค์ของการประเมิน

4.6.2 องค์ประกอบของวัตถุประสงค์และเกณฑ์ความเสี่ยง (Objectives and Risk Criteria Components)

ตารางที่ 4-3 ***ตารางแสดงองค์ประกอบที่ต้องกำหนดสำหรับการประเมินและจัดการความเสี่ยง***

องค์ประกอบ	ความหมายและสิ่งที่ต้องระบุ	คำถามสำคัญ
1) **วัตถุประสงค์และเจ้าของวัตถุประสงค์ (Objective and Objective Owner)**	ผลลัพธ์ที่ต้องการบรรลุ กรอบเวลา และผู้รับผิดชอบต่อผลลัพธ์	ต้องบรรลุอะไร ภายในเมื่อใด และใครรับผิดชอบ
2) **ตัวชี้วัดผลการดำเนินงานและเป้าหมาย (KPI and Target)**	ตัววัดความสำเร็จ นิยาม วิธีคำนวณ หน่วยวัด และค่าเป้าหมาย	จะตรวจสอบความสำเร็จได้อย่างไร
3) **ความสามารถในการรองรับความเสี่ยง (Risk Capacity)**	ขีดความสามารถสูงสุดในการรองรับความเสี่ยงหรือผลกระทบ โดยพิจารณาทรัพยากร ภาระผูกพัน ข้อจำกัด และความต่อเนื่องของพันธกิจ	ผลกระทบระดับใดจะเกินขีดความสามารถของมหาวิทยาลัย
4) **ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA)**	ประเภทและระดับความเสี่ยงที่มหาวิทยาลัยยินดีรับในการดำเนินยุทธศาสตร์และบรรลุวัตถุประสงค์	มหาวิทยาลัยยินดีรับความเสี่ยงประเภทใดและเพียงใด
5) **ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT)**	ขอบเขตความเบี่ยงเบนที่อนุญาตตามกรอบ RA และวัตถุประสงค์ ภายใต้เงื่อนไขที่ได้รับอนุมัติ	จุดใดที่ต้องดำเนินมาตรการและยกระดับ
6) **เกณฑ์การประเมินความเสี่ยง (Risk Assessment Criteria)**	เกณฑ์โอกาสเกิด ผลกระทบ กรอบเวลา ตารางระดับความเสี่ยง และวิธีพิจารณาหลายมิติผลกระทบ	จะประเมินและเปรียบเทียบความเสี่ยงอย่างสม่ำเสมอได้อย่างไร
7) **ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators: KRI)**	ตัววัดการเปลี่ยนแปลงของปัจจัยเสี่ยง การเปิดรับความเสี่ยง หรือผลกระทบ พร้อมเกณฑ์ที่เชื่อมโยงกับ RA/RT	ข้อมูลใดแสดงว่าความเสี่ยงเพิ่มขึ้นหรือลดลง

องค์ประกอบ	ความหมายและสิ่งที่ต้องระบุ	คำถามสำคัญ
8) **จุดแจ้งเตือนและเงื่อนไขดำเนินการ (Trigger and Action)**	ค่า เหตุการณ์ หรือแนวโน้มที่กำหนดให้ต้องเฝ้าระวัง ดำเนินมาตรการ หรือยกระดับ พร้อมผู้รับผิดชอบและเวลา	เมื่อใดต้องเริ่มดำเนินการ และต้องทำอะไร
9) **อำนาจตัดสินใจ (Decision Authority)**	ผู้มีอำนาจอนุมัติมาตรการ จัดสรรทรัพยากร หรือยอมรับความเสี่ยง และผู้รับการยกระดับตามเอกสารให้อำนาจ	ใครตัดสินใจเรื่องใดได้
10)**เจ้าของข้อมูลและแหล่งข้อมูล (Data Owner and Data Source)**	ผู้รับผิดชอบคุณภาพข้อมูล แหล่งข้อมูล ความถี่ และวิธีตรวจสอบ	ข้อมูลมาจากที่ใด ใครรับผิดชอบ และเชื่อถือได้เพียงใด

ตัวชี้วัดผลการดำเนินงาน (KPI) และตัวชี้วัดความเสี่ยง (KRI) มีหน้าที่ต่างกัน แม้อาจใช้ข้อมูลชุดเดียวกันได้ KPI ใช้ประเมินความสำเร็จ ส่วน KRI ใช้ติดตามสถานะหรือแนวโน้มความเสี่ยง การใช้ตัวชี้วัดเดียวกันทั้งสองหน้าที่ต้องอธิบายเกณฑ์และวิธีตีความให้ชัดเจน

4.6.3 หลักการกำหนดระดับความเสี่ยงที่ยอมรับได้และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Appetite and Risk Tolerance Setting)

1. เชื่อมโยงกับวัตถุประสงค์: RA/RT ต้องสัมพันธ์กับวัตถุประสงค์ ความเสี่ยง และขีดความสามารถในการรองรับผลกระทบ ไม่กำหนดจากคะแนนความเสี่ยงเพียงอย่างเดียว

2. แยกนโยบายออกจากเกณฑ์ตัวชี้วัด: RA อาจเป็นข้อความเชิงคุณภาพ เช่น ยอมรับความเสี่ยงด้านสภาพคล่องในระดับต่ำ ส่วนเกณฑ์ KRI เป็นการแปลงกรอบดังกล่าวให้ติดตามได้ในทางปฏิบัติ ค่า KRI จึงไม่ใช่ RA ทั้งหมดของมหาวิทยาลัย

3. ระบุข้อมูลให้ครบถ้วน: เกณฑ์เชิงปริมาณต้องมีนิยาม สูตร หน่วยวัด แหล่งข้อมูล เจ้าของข้อมูล ความถี่ และกรอบเวลาที่ใช้ เพื่อให้เปรียบเทียบและตรวจสอบได้

4. กำหนดช่วงสถานะให้ชัดเจน: ช่วงปกติ ช่วงเฝ้าระวัง และช่วงเกิน RT ต้องไม่ซ้อนทับหรือมีช่องว่าง โดยระบุการรวมค่าที่ขอบเขต เช่น “ตั้งแต่ 120 วันขึ้นไป” หรือ “ต่ำกว่า 120 วัน” ให้ชัดเจน

5. กำหนดการเตือนก่อนเกิน RT: อาจกำหนด Trigger จากค่าจริง ค่าคาดการณ์ หรือแนวโน้ม เพื่อให้มีเวลาป้องกันหรือแก้ไข โดยระบุเงื่อนไขและการดำเนินการที่แตกต่างกัน

6. ตอบสนองเมื่อเกิน RT: ต้องดำเนินมาตรการและยกระดับตามเกณฑ์ โดยไม่รอให้ผลกระทบเข้าใกล้หรือเกิน Risk Capacity การอนุมัติให้คงความเสี่ยงไว้ชั่วคราวไม่เปลี่ยนสถานะว่าเกิน RT

7. ประยุกต์ใช้ภายในอำนาจ: ส่วนงานอาจเสนอเกณฑ์ที่เข้มงวดกว่ากรอบมหาวิทยาลัย แต่ต้องได้รับความเห็นชอบตามอำนาจ และไม่ผ่อนคลาย RA/RT ข้อห้าม หรือ Zero Tolerance ด้วยตนเอง

8. ควบคุมการเปลี่ยนแปลงเกณฑ์: การทบทวน RA/RT ต้องมีเหตุผล หลักฐาน ผู้อนุมัติ วันที่มีผล และบันทึกฉบับเดิม ไม่ปรับย้อนหลังเพื่อทำให้ผลที่เกินเกณฑ์กลับเป็นผลที่ยอมรับได้

9. ไม่ขัดต่อข้อกำหนด: RA/RT ต้องไม่ใช้เป็นเหตุยกเว้นกฎหมาย ข้อบังคับ จริยธรรม ข้อผูกพัน หรือข้อห้ามตามนโยบาย Zero Tolerance

4.6.4 ตัวอย่างการกำหนดวัตถุประสงค์ ตัวชี้วัด และเกณฑ์ตอบสนอง (Objective, Indicator and Response Criteria Examples)

ตัวอย่างต่อไปนี้ใช้เพื่ออธิบายวิธีจัดทำคู่มือเท่านั้น ไม่ถือเป็นเกณฑ์ที่มหาวิทยาลัยอนุมัติแล้ว ส่วนงานต้องตรวจสอบข้อมูลและเสนอเกณฑ์ตามอำนาจก่อนนำไปใช้

ตัวอย่างที่ 1 ความมั่นคงและความยั่งยืนทางการเงิน (Financial Sustainability)

ตัวอย่างการเชื่อมโยงวัตถุประสงค์ ความเสี่ยง และเกณฑ์ด้านสภาพคล่อง

องค์ประกอบ	ตัวอย่าง
วัตถุประสงค์ (Objective)	รักษาสภาพคล่องให้เพียงพอต่อการดำเนินพันธกิจสำคัญและชำระภาระผูกพันตลอดปีงบประมาณ พ.ศ. 2570
เจ้าของวัตถุประสงค์ (Objective Owner)	ผู้บริหารที่กำกับด้านการเงินตามการมอบหมาย
ตัวชี้วัดและเป้าหมาย (KPI and Target)	จำนวนวันที่สามารถดำเนินงานได้ด้วยเงินสดที่มีอยู่ (Days Cash on Hand: DCOH) ไม่น้อยกว่า 180 วัน
ข้อความความเสี่ยง (Risk Statement)	เนื่องจากรายได้ค่าเล่าเรียนและรายได้จากแหล่งอื่นอาจต่ำกว่าแผน ขณะที่ค่าใช้จ่ายคงที่อยู่ในระดับสูง อาจทำให้เงินสดที่ใช้ดำเนินงานไม่เพียงพอ ส่งผลต่อความต่อเนื่องของพันธกิจและการชำระภาระผูกพัน
ประเภทความเสี่ยงหลัก (Primary Risk Category)	ความเสี่ยงด้านการเงิน (F)

องค์ประกอบ	ตัวอย่าง
กรอบความสามารถในการรองรับความเสี่ยง (Risk Capacity)	ประเมินจากประมาณการเงินสด ภาระชำระหนี้ ค่าใช้จ่ายจำเป็น และแหล่งเงินที่เข้าถึงได้ โดยต้องวิเคราะห์ว่ามหาวิทยาลัยสามารถรักษาพันธกิจสำคัญได้นานเพียงใดภายใต้สถานการณ์กดดัน
ระดับความเสี่ยงที่ยอมรับได้ (RA)	ยอมรับความเสี่ยงต่อการขาดสภาพคล่องในระดับต่ำ โดยใช้ DCOH ตั้งแต่ 180 วันขึ้นไปเป็นเกณฑ์ปฏิบัติประกอบการติดตาม
ระดับความเบี่ยงเบนที่ยอมรับได้ (RT)	กำหนดขอบเขตขั้นต่ำของ DCOH ที่ 120 วัน การต่ำกว่าเป้าหมาย 180 วัน แต่ยังไม่ต่ำกว่า 120 วันต้องมีการตอบสนองตามช่วงสถานะ และไม่ถือเป็นการอนุมัติยอมรับความเสี่ยงโดยอัตโนมัติ
ตัวชี้วัดความเสี่ยง (KRI)	ค่า DCOH ปัจจุบันและค่าคาดการณ์ตามประมาณการกระแสเงินสด
สูตรและหน่วยวัด (Formula and Unit)	เงินสดและรายการเทียบเท่าเงินสดที่พร้อมใช้และไม่มีข้อจำกัด ÷ ค่าใช้จ่ายดำเนินงานที่จ่ายเป็นเงินสดเฉลี่ยต่อวัน หน่วยเป็นวัน โดยต้องกำหนดรายการและช่วงเวลาคำนวณให้ชัดเจน
จุดแจ้งเตือนล่วงหน้า (Early Warning Trigger)	ค่าคาดการณ์ DCOH ต่ำกว่า 150 วันภายในช่วงประมาณการที่กำหนด หรือค่าจริงลดลงต่อเนื่อง 3 เดือน ให้ทบทวนสมมติฐานและแผนสภาพคล่อง
เงื่อนไขเกิน RT (RT Breach)	DCOH ต่ำกว่า 120 วัน ให้ยกระดับและดำเนินแผนแก้ไขสภาพคล่อง (Liquidity Action Plan)
เงื่อนไขเร่งด่วน (Urgent Trigger)	DCOH ต่ำกว่า 90 วัน หรือคาดว่าจะไม่สามารถชำระภาระผูกพันจำเป็นได้ ให้ยกระดับเร่งด่วน ทั้งนี้ 90 วันเป็นจุดสั่งการในตัวอย่าง ไม่ใช่หลักฐานว่าเกิน Risk Capacity โดยอัตโนมัติ
เจ้าของข้อมูลและความถี่ (Data Owner and Frequency)	กองคลังหรือผู้รับผิดชอบข้อมูลที่ได้รับมอบหมาย ติดตามรายเดือนและถี่ขึ้นเมื่อเข้าเกณฑ์เตือน
อำนาจตัดสินใจ (Decision Authority)	ตามการมอบอำนาจและตารางอำนาจยอมรับและยกระดับความเสี่ยง

ตัวอย่างช่วงสถานะของตัวชี้วัดสภาพคล่อง

สถานะ	(Days Cash on Hand)	แนวทางดำเนินการ
เป็นไปตามเกณฑ์ปฏิบัติที่เชื่อมโยงกับ RA	ตั้งแต่ 180 วันขึ้นไป	ติดตามตามรอบและทบทวนประมาณการ

สถานะ	(Days Cash on Hand)	แนวทางดำเนินการ
เฝ้าระวัง: ต่ำกว่าเป้าหมาย แต่ยังไม่เกิน RT	ตั้งแต่ 150 วัน แต่ต่ำกว่า 180 วัน	วิเคราะห์สาเหตุและแนวโน้ม พร้อมเตรียมมาตรการ
แก้ไขใกล้ชิด: เข้าใกล้ขอบเขต RT	ตั้งแต่ 120 วัน แต่ต่ำกว่า 150 วัน	ดำเนินแผนแก้ไข เพิ่มความถี่ติดตาม และรายงานผู้บริหารที่กำกับ
เกิน RT	ตั้งแต่ 90 วัน แต่ต่ำกว่า 120 วัน	ยกระดับตามเกณฑ์และเร่งดำเนินแผนสภาพคล่อง
เกิน RT และเข้าเงื่อนไขเร่งด่วน	ต่ำกว่า 90 วัน	ยกระดับเร่งด่วน ประเมินความสามารถชำระภาระผูกพัน และคุ้มครองพันธกิจสำคัญ

Trigger จากค่าคาดการณ์หรือแนวโน้มอาจทำให้ต้องดำเนินการก่อนค่าจริงเข้าสู่ช่วงที่กำหนด ส่วนการประเมิน Risk Capacity ต้องใช้ข้อมูลและสถานการณ์ประกอบ ไม่สรุปจากค่า DCOH ตัวเดียว

ตัวอย่างที่ 2 ความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาลที่ไม่ยอมรับ (Zero Tolerance)

องค์ประกอบ	ตัวอย่าง
วัตถุประสงค์ (Objective)	ดำเนินงานอย่างโปร่งใส ถูกต้องตามกฎหมาย และป้องกันการทุจริตตลอดปีงบประมาณ
ตัวชี้วัดผลการดำเนินงานและเป้าหมาย (KPI and Target)	จำนวนกรณีทุจริตที่ได้รับการยืนยันข้อเท็จจริงเท่ากับ 0 กรณี โดยพิจารณาควบคู่กับคุณภาพการตรวจพบและการรายงาน
ประเภทความเสี่ยงหลัก (Primary Risk Category)	ความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (C)
ระดับความเสี่ยงที่ยอมรับได้ (RA)	ไม่ยอมรับการทุจริต การรับสินบน หรือการใช้ทรัพย์สินของมหาวิทยาลัยโดยมิชอบ
ระดับความเบี่ยงเบนที่ยอมรับได้ (RT)	ไม่มีช่วงความเบี่ยงเบนที่อนุญาตให้กระทำหรือคงการกระทำดังกล่าวไว้
จุดแจ้งเตือน (Trigger)	พบเหตุ ข้อร้องเรียน หรือข้อมูลที่มีมูลเกี่ยวกับการทุจริต แม้ยังไม่มีข้อยุติ
การดำเนินการ (Action)	ระงับหรือจำกัดความเสียหาย รักษาพยานหลักฐาน รายงานตามเส้นทางที่กำหนด และเริ่มตรวจสอบข้อเท็จจริงโดยไม่ชักช้า

องค์ประกอบ	ตัวอย่าง
อำนาจตัดสินใจ (Decision Authority)	ผู้มีอำนาจตามกฎหมาย ระเบียบ และเส้นทางรายงานเหตุ Zero Tolerance

Zero Tolerance ไม่ได้หมายความว่าโอกาสเกิดเหตุเป็นศูนย์ แต่หมายถึงไม่ยอมรับการกระทำ การเพิกเฉย หรือการคงเหตุไว้โดยไม่ดำเนินการ จำนวนกรณีที่ยืนยันเป็นศูนย์เพียงอย่างเดียวจึงไม่เพียงพอที่จะสรุปว่าการควบคุมมีประสิทธิผล

การรายงานข้อสงสัยหรือเริ่มตรวจสอบไม่ถือเป็นข้อยุติว่าบุคคลใดกระทำผิด การวินิจฉัยต้องเป็นไปตามกระบวนการตรวจสอบข้อเท็จจริงและหลักความเป็นธรรม

4.6.5 ตัวอย่างการเชื่อมโยงกับความเสี่ยงหลัก 5 ประเภท (Examples Across Five Risk Categories)

การจำแนกประเภทให้พิจารณาลักษณะเหตุการณ์ความเสี่ยงและวัตถุประสงค์ที่ได้รับผลกระทบ โดยกำหนดประเภทหลักหนึ่งประเภท พร้อมระบุประเภทที่เกี่ยวข้องและมิติผลกระทบร่วมตามความจำเป็น

ตัวอย่างวัตถุประสงค์ ความเสี่ยง และตัวชี้วัดตามประเภทความเสี่ยง

ประเภทความเสี่ยง	ตัวอย่างวัตถุประสงค์	ตัวอย่างข้อความความเสี่ยง	ตัวอย่างตัวชี้วัดและเงื่อนไขตอบสนอง
ความเสี่ยงด้านยุทธศาสตร์ (Strategic Risk: S)	บรรลุเป้าหมายการรับผู้เรียนและพัฒนาหลักสูตรให้สอดคล้องกับแผนยุทธศาสตร์	เนื่องจากจำนวนผู้เรียนเป้าหมายลดลงและความต้องการทักษะเปลี่ยนแปลง อาจทำให้หลักสูตรดึงดูดผู้เรียนได้ไม่เพียงพอ ส่งผลให้ไม่บรรลุเป้าหมายการรับผู้เรียนและผลลัพธ์เชิงยุทธศาสตร์	**KPI:** จำนวนผู้เข้าศึกษาจริงเทียบแผน **KRI:** อัตรายืนยันสิทธิ์และแนวโน้มผู้เข้าศึกษาจริงที่คาดการณ์ **เงื่อนไข:** หากคาดว่าจะต่ำกว่าขอบเขตที่อนุมัติ ให้ทบทวนแผนรับผู้เรียนและเสนอทางเลือก
ความเสี่ยงด้านการดำเนินงาน	ให้บริการสำคัญได้ต่อเนื่องและ	เนื่องจากงานสำคัญพึ่งพาบุคลากรเฉพาะรายและยังไม่มีผู้ทดแทนที่พร้อม อาจทำ	**KPI:** ร้อยละบริการที่แล้วเสร็จตามเวลา **KRI:** สัดส่วนงานสำคัญที่ไม่มีผู้ทดแทนผ่าน

ประเภทความเสี่ยง	ตัวอย่างวัตถุประสงค์	ตัวอย่างข้อความความเสี่ยง	ตัวอย่างตัวชี้วัดและเงื่อนไขตอบสนอง
(Operational Risk: O)	ทันเวลาตามมาตรฐาน	ให้การปฏิบัติงานหยุดชะงักเมื่อบุคลากรไม่สามารถปฏิบัติงาน ส่งผลให้บริการล่าช้าและไม่เป็นไปตามมาตรฐาน	การทดสอบ **เงื่อนไข:** หากเกินเกณฑ์ ให้จัดผู้ทดแทนถ่ายทอดงาน และทดสอบความพร้อม
ความเสี่ยงด้านการเงิน (Financial Risk: F)	รักษาสภาพคล่องและความสามารถชำระภาระผูกพัน	เนื่องจากรายรับต่ำกว่าแผนและรายจ่ายจำเป็นไม่ลดลง อาจทำให้เงินสดไม่เพียงพอ ส่งผลต่อการชำระภาระผูกพันและความต่อเนื่องของพันธกิจ	**KPI/KRI:** DCOH โดยแยกเป้าหมายความสำเร็จจากเกณฑ์ตอบสนอง **เงื่อนไข:** เมื่อค่าจริงหรือค่าคาดการณ์เข้าเกณฑ์เตือน ให้ดำเนินแผนสภาพคล่องและยกระดับตามความรุนแรง
ความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (Compliance and Governance Risk: C)	ดำเนินการจัดซื้อจัดจ้างอย่างถูกต้องและโปร่งใส	เนื่องจากการสอบทานข้อกำหนดและผลประโยชน์ทับซ้อนไม่เพียงพอ อาจเกิดการจัดซื้อจัดจ้างที่ฝ่าฝืนข้อกำหนด ส่งผลให้เกิดข้อพิพาท ความรับผิด และความเสียหายต่อความเชื่อมั่น	**KPI:** ความครบถ้วนของการปฏิบัติตามข้อกำหนด **KRI:** จำนวนข้อบกพร่องสำคัญที่ยังไม่แก้ไข **เงื่อนไข:** เมื่อพบข้อบกพร่องให้แก้ไขตามเกณฑ์ หากมีข้อมูลที่มีมูลเกี่ยวกับการทุจริตให้ใช้แนวทาง Zero Tolerance
ความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Technology Risk: D)	รักษาความพร้อมใช้ ความมั่นคง ปลอดภัย และความถูกต้องของระบบและข้อมูลสำคัญ	เนื่องจากช่องโหว่สำคัญยังไม่ได้รับการแก้ไขและการป้องกันไม่ครอบคลุม อาจเกิดการโจมตีหรือเข้าถึงระบบโดยไม่ได้รับอนุญาต ส่งผลให้บริการหยุดชะงักหรือข้อมูลรั่วไหล	**KPI:** ความพร้อมใช้ของบริการสำคัญ **KRI:** จำนวนช่องโหว่รุนแรงที่ค้างเกินกำหนด **เงื่อนไข:** เมื่อเกินเกณฑ์ให้เร่งแก้ไข หากเกิดเหตุให้ใช้แผนเผชิญเหตุและเส้นทางรายงานเฉพาะด้าน

ชื่อเสียง ความเชื่อมั่น ความปลอดภัย ความต่อเนื่อง และ ESG ให้พิจารณาเป็นมิติผลกระทบร่วม ตัวอย่างเช่น เหตุโจมตีระบบอาจมีประเภทหลักเป็น D และเชื่อมโยงกับ C เมื่อเกี่ยวข้องกับหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยไม่จำเป็นต้องสร้างรายการความเสี่ยงซ้ำ หากสามารถระบุเจ้าของและมาตรการร่วมได้ชัดเจน

4.6.6 การจัดหมวดข้อมูลในทะเบียนความเสี่ยง (Risk Register Information Structure)

เพื่อให้ส่วนงานบันทึกและใช้ข้อมูลได้สะดวก ให้จัดข้อมูลในทะเบียนความเสี่ยงหรือแบบ RISK-MJU-01 เป็นหมวดที่เชื่อมโยงกัน ดังต่อไปนี้

หมวดข้อมูล	รายการสำคัญ	ช่วงที่จัดทำหรือปรับปรุง
1. ข้อมูลอ้างอิงและวัตถุประสงค์ (Reference and Objectives)	รหัสความเสี่ยง ส่วนงาน รอบการประเมิน ขอบเขต วัตถุประสงค์ เจ้าของวัตถุประสงค์ รหัสยุทธศาสตร์หรือแผน KPI และเป้าหมาย	ขั้นตอนที่ 1–2
2. เกณฑ์และกรอบการตัดสินใจ (Criteria and Decision Framework)	เกณฑ์โอกาสเกิดและผลกระทบ กรอบเวลา RA/RT ที่เกี่ยวข้อง เกณฑ์ Override ผู้มีอำนาจ และแหล่งอ้างอิงฉบับที่ใช้	ขั้นตอนที่ 2
3. รายละเอียดความเสี่ยง (Risk Description)	ชื่อและข้อความความเสี่ยง สาเหตุ เหตุการณ์ ผลกระทบ ประเภทหลัก ประเภทที่เกี่ยวข้อง มิติผลกระทบ และเจ้าของความเสี่ยง	ขั้นตอนที่ 3
4. ผลการประเมินและการควบคุม (Assessment and Controls)	ความเสี่ยงโดยธรรมชาติ การควบคุม เจ้าของการควบคุม หลักฐานและผลประเมินประสิทธิผล ความเสี่ยงคงเหลือ วันที่ประเมิน และสถานะเทียบ RA/RT	ขั้นตอนที่ 4
5. การตอบสนองและแผนมาตรการ (Response and Treatment Plan)	แนวทางตอบสนอง มาตรการ เจ้าของมาตรการ ทรัพยากร ผลส่งมอบ กำหนดเวลา ความเสี่ยงคงเหลือเป้าหมาย และหลักฐานอนุมัติ	ขั้นตอนที่ 5–6
6. ตัวชี้วัดและการรายงาน (Indicators and Reporting)	นิยามและสูตร KRI หน่วยวัด แหล่งข้อมูล เจ้าของข้อมูล ความถี่ เกณฑ์สถานะ Trigger/Action ค่าจริง แนวโน้ม และบันทึกการยกระดับ	เริ่มกำหนดในขั้นตอนที่ 2 และเพิ่มเติมในขั้นตอนที่ 3–7

หมวดข้อมูล	รายการสำคัญ	ช่วงที่จัดทำหรือปรับปรุง
7. การทบทวนและประวัติการตัดสินใจ (Review and Decision History)	ผลติดตาม ระดับความเสี่ยงที่ปรับปรุง ข้อสั่งการผู้อนุมัติ เงื่อนไขและวันสิ้นสุดการยอมรับความเสี่ยง บทเรียน และกำหนดทบทวน	ขั้นตอนที่ 7–8 และเมื่อมีการเปลี่ยนแปลง

การจัดหมวดนี้เป็นโครงสร้างข้อมูลสำหรับทั้งวงจร ไม่ได้กำหนดให้กรอกข้อมูลทุกหมวดให้เสร็จในขั้นตอนที่ 2 ส่วนงานสามารถใช้ข้อมูลอ้างอิงร่วมกันและเชื่อมโยงหลักฐานจากระบบงานเดิมโดยไม่ต้องคัดลอกเอกสารทั้งหมดลงในทะเบียนความเสี่ยง

4.6.7 ผลผลิตขั้นต่ำของขั้นตอนที่ 2 (Minimum Outputs of Step 2)

เมื่อสิ้นสุดขั้นตอนนี้ ต้องมีข้อมูลและหลักฐานอย่างน้อยดังต่อไปนี้

1. วัตถุประสงค์ เจ้าของวัตถุประสงค์ และเป้าหมายที่ได้รับการยืนยัน (Confirmed Objectives, Owners and Targets)

2. ความเชื่อมโยงกับยุทธศาสตร์ พันธกิจ และตัวชี้วัด (Strategy, Mission and KPI Linkage)

3. กรอบความสามารถในการรองรับและการยอมรับความเสี่ยงที่เกี่ยวข้อง (Applicable Risk Capacity, Appetite and Tolerance Framework)

4. เกณฑ์โอกาสเกิดและผลกระทบ พร้อมกรอบเวลาประเมิน (Likelihood, Impact and Time Horizon Criteria)

5. ตารางประเมินระดับความเสี่ยงและเกณฑ์จัดลำดับความสำคัญ (Risk Matrix and Prioritization Criteria)

6. เกณฑ์ยกระดับเป็นกรณีพิเศษและเหตุที่ไม่ยอมรับ (Override and Zero Tolerance Criteria)

7. ตัวชี้วัดเบื้องต้น จุดแจ้งเตือน และเงื่อนไขดำเนินการ (Preliminary Indicators, Triggers and Actions)

8. เจ้าของข้อมูล แหล่งข้อมูล และความถี่ (Data Owners, Sources and Frequency)

9. อำนาจตัดสินใจและเส้นทางการยกระดับ (Decision Authority and Escalation Routes)

10. หลักฐานการอนุมัติหรือแหล่งอ้างอิงเกณฑ์ พร้อมวันที่มีผลและฉบับที่ใช้ (Criteria Approval or Reference, Effective Date and Version)

ให้บันทึกข้อมูลดังกล่าวในแบบ RISK-MJU-01 ทะเบียนความเสี่ยง หรือเอกสารอ้างอิงที่เชื่อมโยงกัน เพื่อใช้เป็นฐานในการระบุและประเมินความเสี่ยงในขั้นตอนต่อไป ส่วนความเชื่อมโยงระหว่างวัตถุประสงค์ KPI และความเสี่ยงแต่ละรายการให้เพิ่มเติมและยืนยันเมื่อดำเนินการระบุความเสี่ยงในขั้นตอนที่ 3

4.7 ขั้นตอนที่ 3 การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยงเป็นกระบวนการค้นหาและอธิบายเหตุการณ์หรือความไม่แน่นอนที่อาจส่งผลต่อการบรรลุวัตถุประสงค์ ทั้งในด้านภัยคุกคามและโอกาสในการสร้างคุณค่า โดยใช้วัตถุประสงค์ บริบท และเกณฑ์จากขั้นตอนที่ 1–2 เป็นฐานในการพิจารณาสาเหตุ เหตุการณ์ ผลกระทบ และความสัมพันธ์กับความเสี่ยงอื่น

การระบุต้องครอบคลุมความเสี่ยงที่อยู่ภายในและภายนอกการควบคุมของมหาวิทยาลัย รวมถึงความเสี่ยงจากบุคคลภายนอกและความเสี่ยงเกิดใหม่ ไม่จำกัดเฉพาะเหตุการณ์ที่เคยเกิดขึ้นหรือประเด็นที่มีข้อมูลครบถ้วนแล้ว หากข้อมูลยังมีจำกัด ให้ระบุข้อจำกัดและสมมติฐานไว้เพื่อประเมินเพิ่มเติมในขั้นตอนต่อไป

4.7.1 รูปแบบการเขียนข้อความความเสี่ยง (Risk Statement)

ให้เขียนข้อความความเสี่ยงตามโครงสร้าง **สาเหตุ–เหตุการณ์–ผลกระทบ (Cause–Event–Impact)** ดังนี้ “เนื่องจาก [สาเหตุหรือปัจจัยขับเคลื่อนความเสี่ยง] อาจทำให้เกิด [เหตุการณ์หรือความไม่แน่นอน] ส่งผลให้ [วัตถุประสงค์ ผลลัพธ์ หรือผู้มีส่วนได้ส่วนเสียได้รับผลกระทบอย่างไร]” องค์ประกอบของข้อความประกอบด้วย

- **สาเหตุหรือปัจจัยขับเคลื่อนความเสี่ยง (Cause/Risk Driver):** ปัจจัย เงื่อนไข หรือการเปลี่ยนแปลงที่ทำให้เหตุการณ์อาจเกิดขึ้นหรือรุนแรงขึ้น
- **เหตุการณ์ความเสี่ยง (Risk Event):** เหตุการณ์หรือสถานการณ์ที่ยังมีความไม่แน่นอนและอาจส่งผลต่อวัตถุประสงค์
- **ผลกระทบ (Impact/Consequence):** ผลที่อาจทำให้การดำเนินงานเบี่ยงเบนจากเป้าหมาย หรือกระทบผู้มีส่วนได้ส่วนเสีย

ตัวอย่างข้อความความเสี่ยงด้านยุทธศาสตร์

"เนื่องจากข้อมูลความต้องการของผู้เรียนและตลาดแรงงานยังไม่เชื่อมโยงกับการทบทวนหลักสูตรอย่างเพียงพอ อาจทำให้มหาวิทยาลัยปรับหลักสูตรและแผนรับผู้เรียนไม่ทันต่อการเปลี่ยนแปลง ส่งผลให้จำนวนผู้เข้าศึกษาจริงและผลลัพธ์ด้านความสามารถในการแข่งขันต่ำกว่าเป้าหมายตามแผนยุทธศาสตร์"

หลักการเขียนข้อความความเสี่ยง

1. **เชื่อมโยงกับวัตถุประสงค์:** ระบุวัตถุประสงค์ ผลลัพธ์ หรือ KPI ที่อาจได้รับผลกระทบให้ชัดเจน

2. **ระบุเหตุการณ์ให้เฉพาะเจาะจง:** ไม่ใช้เพียงหัวข้อกว้าง เช่น "บุคลากร" "งบประมาณ" หรือ "เทคโนโลยี"

3. **แยกสาเหตุออกจากเหตุการณ์:** ข้อความ เช่น "บุคลากรไม่เพียงพอ" หรือ "งบประมาณไม่เพียงพอ" ต้องวิเคราะห์ต่อว่าอาจทำให้เกิดเหตุการณ์ใดและกระทบเป้าหมายอย่างไร

4. **ไม่ระบุเพียงผลกระทบ:** ข้อความ เช่น "มหาวิทยาลัยเสียชื่อเสียง" ต้องระบุสาเหตุและเหตุการณ์ที่อาจนำไปสู่ผลกระทบนั้น

5. **ไม่ใช้การขาดกิจกรรมเป็นข้อความความเสี่ยงทั้งหมด:** "ไม่ได้จัดอบรม" หรือ "ไม่มีการประชุมติดตาม" อาจเป็นข้อบกพร่องของมาตรการหรือปัจจัยเสี่ยง แต่ต้องระบุเหตุการณ์และผลกระทบเพิ่มเติม

6. **แยกความเสี่ยงออกจากปัญหาและเหตุการณ์ที่เกิดแล้ว:** บันทึกปัญหา (Issue) หรือเหตุการณ์ที่เกิดขึ้น (Incident) ตามกระบวนการที่เกี่ยวข้อง และใช้ข้อมูลดังกล่าวระบุความเสี่ยงต่อการเกิดซ้ำ การขยายตัว หรือผลกระทบในอนาคต

7. **ใช้ข้อความกระชับและนำไปจัดการได้:** สามารถกำหนดเจ้าของความเสี่ยง ตัวชี้วัด และมาตรการตอบสนองได้ หากมีหลายเหตุการณ์ที่มีเจ้าของหรือแนวทางจัดการต่างกันอย่างมีนัยสำคัญ ให้พิจารณาแยกรายการ

8. **ระบุความไม่แน่นอนอย่างตรงไปตรงมา:** ไม่เขียนเหตุการณ์ในอนาคตเป็นข้อเท็จจริงที่ยืนยันแล้ว และไม่ระบุว่ามีการฝ่าฝืนกฎหมายหรือกระทำผิดโดยไม่มีหลักฐานเพียงพอ

ตัวอย่างการปรับข้อความความเสี่ยงให้ชัดเจน

ข้อความที่ยังไม่เพียงพอ	ตัวอย่างข้อความที่ปรับปรุงแล้ว	ประเภทหลักในตัวอย่าง
หลักสูตรไม่ทันสมัย	เนื่องจากการทบทวนหลักสูตรใช้ข้อมูลความต้องการของผู้เรียนและตลาดแรงงานไม่เพียงพอ อาจทำให้หลักสูตรไม่ตอบสนองทักษะที่จำเป็น ส่งผลให้ไม่บรรลุเป้าหมายการรับผู้เรียนและผลลัพธ์ด้านคุณภาพบัณฑิตตามแผนยุทธศาสตร์	S
บุคลากรขาดทักษะ	เนื่องจากการพัฒนาบุคลากรยังไม่ครอบคลุมสมรรถนะที่กระบวนงานต้องใช้ อาจทำให้บุคลากรปฏิบัติงานด้วยระบบดิจิทัลได้ไม่ถูกต้องหรือไม่ทันเวลา ส่งผลให้คุณภาพและระยะเวลาการให้บริการไม่เป็นไปตามมาตรฐาน	O
งบประมาณไม่เพียงพอ	เนื่องจากรายได้ค่าเล่าเรียนอาจต่ำกว่าแผนและต้นทุนคงที่อยู่ในระดับสูง อาจทำให้เงินสดที่พร้อมใช้ลดลง ส่งผลต่อความสามารถในการดำเนินพันธกิจและชำระภาระผูกพัน	F
การจัดซื้อจัดจ้างไม่ถูกต้อง	เนื่องจากการสอบทานข้อกำหนดและผลประโยชน์ทับซ้อนยังไม่ครอบคลุม อาจเกิดการดำเนินการจัดซื้อจัดจ้างที่ฝ่าฝืนข้อกำหนด ส่งผลให้เกิดข้อพิพาท ความรับผิด และความเสียหายต่อความเชื่อมั่น	C
ความเสี่ยงด้านไซเบอร์	เนื่องจากระบบสำคัญยังมีช่องโหว่และการควบคุมสิทธิไม่เพียงพอ อาจเกิดการเข้าถึงระบบหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต ส่งผลให้บริการหยุดชะงัก ข้อมูลรั่วไหล และอาจเกิดความรับผิดตามกฎหมาย	D
ชื่อเสียงเสียหาย	เนื่องจากการตรวจสอบและตอบสนองต่อข้อมูลข่าวสารไม่ทันเวลา อาจทำให้ข้อมูลที่ไม่ถูกต้องแพร่กระจายในวงกว้าง ส่งผลต่อความเชื่อมั่นของผู้เรียน ผู้ปกครอง และสาธารณชน	O โดยกำหนดชื่อเสียงและความเชื่อมั่นเป็นมิติผลกระทบร่วม

การจำแนกในตารางเป็นตัวอย่างตามลักษณะเหตุการณ์ที่ระบุ ไม่ใช่ข้อกำหนดตายตัวสำหรับทุกส่วนงาน เช่น ช่องว่างสมรรถนะอาจจัดเป็นความเสี่ยงด้านยุทธศาสตร์ หากเหตุการณ์หลักคือมหาวิทยาลัยไม่สามารถปรับขีดความสามารถเพื่อดำเนินยุทธศาสตร์ใหม่ได้

การระบุโอกาส (Opportunity Identification)

การระบุโอกาสให้แสดงปัจจัยที่เอื้อ เหตุการณ์หรือทางเลือกที่อาจเกิดขึ้น และคุณค่าที่คาดว่าจะได้รับ พร้อมพิจารณาความเสี่ยงของการใช้ประโยชน์จากโอกาสนั้น

ตัวอย่าง: “เนื่องจากความต้องการพัฒนาทักษะระยะสั้นเพิ่มขึ้นและมหาวิทยาลัยมีความเชี่ยวชาญด้านเกษตรและอาหาร อาจเปิดโอกาสให้พัฒนาหลักสูตรร่วมกับภาคอุตสาหกรรม ส่งผลให้เพิ่มการเข้าถึงผู้เรียนกลุ่มใหม่และรายได้จากการเรียนรู้ตลอดชีวิต”

ต้องประเมินความต้องการจริง ความพร้อม ต้นทุน คุณภาพ และข้อกำหนดที่เกี่ยวข้องก่อนตัดสินใจ โดยไม่หักล้างคะแนนภัยคุกคามด้วยคะแนนโอกาสโดยตรง

4.7.2 แหล่งข้อมูลและเทคนิคการระบุความเสี่ยง (Risk Identification Sources and Techniques)

การระบุความเสี่ยงควรใช้ข้อมูลหลายแหล่งและรับฟังมุมมองจากผู้เกี่ยวข้อง เพื่อลดอคติและเพิ่มความครอบคลุม

แหล่งข้อมูลสำคัญ (Key Information Sources)

1. **วัตถุประสงค์และแผนงาน (Objectives and Plans):** แผนยุทธศาสตร์ แผนปฏิบัติการ โครงการ KPI และ KRI ที่เกี่ยวข้อง

2. **ผลการดำเนินงานและประมาณการ (Performance and Forecasts):** แนวโน้มผลลัพธ์ ความเบี่ยงเบนจากเป้าหมาย และข้อมูลคาดการณ์

3. **เหตุการณ์และเหตุการณ์เกือบเกิดความเสียหาย (Incidents and Near Misses):** สาเหตุ ความเสียหาย และผลการแก้ไข

4. **ข้อมูลผู้มีส่วนได้ส่วนเสีย (Stakeholder Information):** ข้อร้องเรียน ความคิดเห็น ข้อพิพาท และคดี

5. **ผลการตรวจสอบและประเมินการควบคุม (Audit and Control Assessment Results):** ข้อค้นพบ ช่องว่าง และประเด็นที่เกิดซ้ำ

6. **การเปลี่ยนแปลงข้อกำหนด (Changes in Requirements):** กฎหมาย นโยบาย มาตรฐาน สัญญา และข้อกำหนดกำกับดูแล

7. **ข้อมูลคู่เทียบและภาคอุดมศึกษา (Benchmarking and Higher Education Information):** แนวโน้มการแข่งขัน รูปแบบบริการ และบทเรียนจากองค์กรอื่น

8. ข้อมูลบุคคลภายนอกและการพึ่งพา (Third-party and Dependency Information): ผู้รับจ้าง ผู้ให้บริการ คู่สัญญา และคู่ความร่วมมือ

9. ข้อมูลความพร้อมและการทดสอบแผน (Readiness and Exercise Results): ผลทดสอบความต่อเนื่อง การกู้คืนระบบ และการตอบสนองเหตุ

10. ความเสี่ยงเกิดใหม่ (Emerging Risks): สัญญาณการเปลี่ยนแปลงของบริบทและสมมติฐานสำคัญ

เทคนิคที่อาจนำมาใช้ (Applicable Techniques)

- การประชุมเชิงปฏิบัติการระบุความเสี่ยง (Risk Workshop)
- การสัมภาษณ์ (Interview)
- การจัดทำแผนผังกระบวนงาน (Process Mapping)
- การวิเคราะห์สาเหตุและผลด้วยแผนผังก้างปลา (Cause-and-effect/Fishbone Analysis)
- การวิเคราะห์แบบโบว์ไทเพื่อเชื่อมโยงสาเหตุ เหตุการณ์ ผลกระทบ และการควบคุม (Bow-tie Analysis)
- การวิเคราะห์สาเหตุราก (Root Cause Analysis)
- การวิเคราะห์สถานการณ์สมมติ (Scenario Analysis)
- การสำรวจแนวโน้มและสัญญาณการเปลี่ยนแปลงในอนาคต (Horizon Scanning)
- การวิเคราะห์ปัจจัยการเมือง เศรษฐกิจ สังคม เทคโนโลยี กฎหมาย และสิ่งแวดล้อม (PESTLE Analysis)
- การวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรค (SWOT Analysis)
- การวิเคราะห์ข้อมูลและแนวโน้ม (Data and Trend Analysis)

ให้เลือกเทคนิคตามวัตถุประสงค์ ความซับซ้อน และข้อมูลที่มี ไม่จำเป็นต้องใช้ทุกเทคนิค ทั้งนี้ ผลจากการวิเคราะห์บริบทหรือการระดมความคิดเห็นต้องนำมาวิเคราะห์ความเชื่อมโยงกับวัตถุประสงค์ก่อนบันทึกเป็นรายการความเสี่ยง

4.7.3 ประเภทความเสี่ยง (Risk Categories)

คู่มือฉบับปรับปรุง พ.ศ. 2570 กำหนดประเภทความเสี่ยงหลัก 5 ประเภท ได้แก่ **S O F C D** เพื่อใช้เป็นกรอบร่วมในการระบุ วิเคราะห์ ประเมิน และรายงาน โดยกำหนดประเภทหลักตามลักษณะเหตุการณ์และวัตถุประสงค์ที่ได้รับผลกระทบ พร้อมระบุประเภทที่เกี่ยวข้องเพิ่มเติมได้

ตารางที่ 4-4 ***ตารางแสดงประเภทความเสี่ยง ขอบเขต และตัวอย่าง***

ประเภทความเสี่ยง	ขอบเขต	ตัวอย่าง
ความเสี่ยงด้านยุทธศาสตร์ (Strategic Risk: S)	ความไม่แน่นอนเกี่ยวกับการเลือกและดำเนินยุทธศาสตร์ การปรับตัว และความสามารถในการบรรลุวิสัยทัศน์ พันธกิจ เป้าประสงค์ และผลลัพธ์สำคัญ ครอบคลุมความสามารถในการแข่งขัน ผู้เรียน หลักสูตร การวิจัย นวัตกรรม และความร่วมมือ	การปรับหลักสูตรไม่ทันต่อความต้องการ การรับผู้เรียนไม่บรรลุเป้าหมายเชิงยุทธศาสตร์ หรือการปรับขีดความสามารถองค์กรไม่ทันต่อการเปลี่ยนแปลง
ความเสี่ยงด้านการดำเนินงาน (Operational Risk: O)	ความไม่แน่นอนจากบุคลากร กระบวนงาน การให้บริการ ทรัพย์สิน อาคารสถานที่ และการบริหารคู่สัญญา ซึ่งอาจกระทบคุณภาพ ประสิทธิภาพ ความปลอดภัย และความต่อเนื่อง	ความผิดพลาดในการให้บริการ การขาดผู้ปฏิบัติงานทดแทน อุบัติเหตุ หรือการหยุดชะงักจากภัยพิบัติและสาธารณูปโภค
ความเสี่ยงด้านการเงิน (Financial Risk: F)	ความไม่แน่นอนที่กระทบรายได้ รายจ่าย สภาพคล่อง กระแสเงินสด การลงทุน ภาระผูกพัน และความยั่งยืนทางการเงิน	รายได้ต่ำกว่าแผน การพึ่งพารายได้แหล่งเดียว เงินสดไม่เพียงพอ หรือโครงการลงทุนไม่ให้ผลตอบแทนตามสมมติฐาน
ความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (Compliance and Governance Risk: C)	ความไม่แน่นอนเกี่ยวกับการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ สัญญา มาตรฐาน จริยธรรม และข้อกำหนดกำกับดูแล รวมถึงข้อบกพร่องด้านอำนาจหน้าที่ ความโปร่งใส และความรับผิดชอบ	การจัดซื้อจัดจ้างฝ่าฝืนข้อกำหนด การทุจริต ผลประโยชน์ทับซ้อน การประพฤติมิชอบทางการวิจัย หรือการไม่ปฏิบัติตามหน้าที่คุ้มครองข้อมูลส่วนบุคคล
ความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Technology Risk: D)	ความไม่แน่นอนเกี่ยวกับระบบสารสนเทศ โครงสร้างพื้นฐานดิจิทัล ข้อมูล ปัญญาประดิษฐ์ และการพึ่งพาเทคโนโลยี ซึ่งกระทบความพร้อมใช้ ความมั่นคงปลอดภัย ความถูกต้องครบถ้วน และความลับ	การโจมตีไซเบอร์ ระบบสำคัญล้มเหลว ข้อมูลสูญหาย การกู้คืนไม่สำเร็จ ผู้ให้บริการคลาวด์หยุดให้บริการ หรือผลลัพธ์จาก AI ผิดพลาดจนกระทบงานสำคัญ

หลักการจำแนกและกำหนดรหัส (Classification and Coding Principles)

1. กำหนดประเภทหลักหนึ่งประเภท: ใช้ลักษณะเหตุการณ์และวัตถุประสงค์เป็นฐาน ไม่จำแนกจากชื่อหน่วยงานหรือผลกระทบปลายทางเพียงอย่างเดียว

2. ระบุความเชื่อมโยงข้ามประเภท: เช่น เหตุโจมตีระบบมีประเภทหลักเป็น D และอาจเชื่อมโยงกับ C และ F ตามผลกระทบและหน้าที่ที่เกี่ยวข้อง

3. ใช้มิติผลกระทบร่วม: ชื่อเสียงและความเชื่อมั่น ความปลอดภัย ความต่อเนื่อง สิ่งแวดล้อมและ ESG ตลอดจนผลกระทบต่อการศึกษา การวิจัย และวิชาการ ให้ระบุเป็นมิติผลกระทบร่วมหรือป้ายกำกับตามความเกี่ยวข้อง ไม่เพิ่มเป็นประเภทหลักซ้ำกับ S O F C D

4. แยกความหมายของรหัส: รหัส S ของประเภทความเสี่ยงหมายถึงด้านยุทธศาสตร์ ส่วนมิติสังคมของ ESG ให้ใช้ป้ายกำกับ ESG-S เพื่อป้องกันความสับสน

5. หลีกเลี่ยงรายการซ้ำ: หากเป็นเหตุการณ์เดียวกันที่มีหลายผลกระทบ ให้ใช้รายการหลักและเชื่อมโยงผู้รับผิดชอบหรือมาตรการร่วม เว้นแต่มีเหตุผลชัดเจนในการแยก เช่น เหตุการณ์เจ้าของ หรือแนวทางตอบสนองแตกต่างกัน

6. รักษาประวัติรหัส: รหัสประเด็นความเสี่ยงระดับมหาวิทยาลัยให้ยึดแผนที่ได้รับความเห็นชอบ หากรหัสเดิมแตกต่างจากกรอบประเภทปัจจุบัน ให้จัดทำตารางเทียบรหัสและเก็บประวัติการเปลี่ยนแปลง ไม่เปลี่ยนรหัสในแผนที่อนุมัติแล้วโดยพลการ

4.7.4 การบันทึกและยืนยันรายการความเสี่ยง (Risk Recording and Confirmation) ให้บันทึกข้อมูลในหมวดรายละเอียดความเสี่ยงของทะเบียนความเสี่ยงหรือแบบ RISK-MJU-01 โดยมีอย่างน้อยดังต่อไปนี้

1. รหัสและชื่อความเสี่ยง (Risk ID and Title)
2. วัตถุประสงค์และตัวชี้วัดที่เกี่ยวข้อง (Related Objective and KPI)
3. ข้อความความเสี่ยง (Risk Statement)
4. สาเหตุหรือปัจจัยขับเคลื่อน (Causes/Risk Drivers)
5. เหตุการณ์ความเสี่ยง (Risk Event)
6. ผลกระทบและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง (Impacts and Affected Stakeholders)
7. ประเภทหลัก ประเภทที่เกี่ยวข้อง และมิติผลกระทบ (Primary Category, Related Categories and Impact Dimensions)

8. เจ้าของความเสี่ยงและส่วนงานที่เกี่ยวข้อง (Risk Owner and Related Units)

9. กรอบเวลาที่ความเสี่ยงอาจเกิดหรือส่งผล (Time Horizon)

10. การควบคุมที่มีอยู่เบื้องต้น (Preliminary Existing Controls)

11. แหล่งข้อมูล หลักฐาน สมมติฐาน และข้อจำกัด (Sources, Evidence, Assumptions and Limitations)

12. ความสัมพันธ์กับความเสี่ยงหรือเหตุการณ์อื่น (Links to Other Risks or Incidents)

เจ้าของความเสี่ยงต้องยืนยันว่าข้อความและขอบเขตสอดคล้องกับวัตถุประสงค์ กรณีเกี่ยวข้องกับหลายส่วนงาน ให้เสนอเจ้าของความเสี่ยงหลัก (Lead Risk Owner) และผู้ร่วมรับผิดชอบตามอำนาจ หน่วยบริหารความเสี่ยงสนับสนุนการสอบทานความครบถ้วนและความสอดคล้อง แต่ไม่เป็นเจ้าของความเสี่ยงแทนส่วนงาน

การระบุการควบคุมในขั้นตอนนี้เป็นข้อมูลตั้งต้น ส่วนการประเมินประสิทธิผลของการควบคุมและระดับความเสี่ยงให้ดำเนินการในขั้นตอนที่ 4 หากพบเหตุเร่งด่วนหรือเข้าเกณฑ์ยกระดับต้องรายงานและตอบสนองทันทีโดยไม่รอให้การบันทึกครบถ้วน

4.7.5 ผลผลิตขั้นต่ำของขั้นตอนที่ 3 (Minimum Outputs of Step 3)

เมื่อสิ้นสุดขั้นตอนนี้ ต้องมีข้อมูลและหลักฐานอย่างน้อยดังต่อไปนี้

1. รายการความเสี่ยงและโอกาสที่เชื่อมโยงกับวัตถุประสงค์ (Objective-linked Risks and Opportunities)

2. ข้อความความเสี่ยงตามโครงสร้างสาเหตุ–เหตุการณ์–ผลกระทบ (Cause–Event–Impact Risk Statements)

3. ประเภทความเสี่ยงและมิติผลกระทบที่เกี่ยวข้อง (Risk Categories and Impact Dimensions)

4. เจ้าของความเสี่ยงและกลไกประสานงานกรณีข้ามส่วนงาน (Risk Owners and Cross-unit Coordination)

5. แหล่งข้อมูล หลักฐาน และข้อจำกัดในการระบุ (Identification Sources, Evidence and Limitations)

6. ข้อมูลการควบคุมและการพึ่งพาที่เกี่ยวข้องเบื้องต้น (Preliminary Controls and Dependencies)

7. ทะเบียนความเสี่ยงที่ได้รับการทบทวนและยืนยันตามบทบาท (Reviewed and Confirmed Risk Register)

ผลผลิตดังกล่าวใช้เป็นข้อมูลตั้งต้นสำหรับการวิเคราะห์และประเมินความเสี่ยงในขั้นตอนที่ 4 และต้องทบทวนเมื่อวัตถุประสงค์ บริบท สมมติฐาน หรือข้อมูลสำคัญเปลี่ยนแปลง

หลักการจำแนกประเภทความเสี่ยง (Risk Classification Principles)

การจำแนกประเภทความเสี่ยงมีวัตถุประสงค์เพื่อให้การระบุ ประเมิน และบริหารความเสี่ยงมีความครบถ้วนและเป็นระบบ พร้อมกำหนดความรับผิดชอบและสายการรายงานให้ชัดเจน โดยต้องพิจารณาความเชื่อมโยงระหว่างประเภทควบคู่กัน เนื่องจากความเสี่ยงหนึ่งรายการอาจมีหลายสาเหตุและส่งผลกระทบต่อหลายวัตถุประสงค์ ให้ใช้หลักการจำแนกดังต่อไปนี้

1. พิจารณาวัตถุประสงค์ สาเหตุ และเหตุการณ์หลัก: จำแนกจากวัตถุประสงค์ที่ได้รับผลกระทบ สาเหตุหรือปัจจัยขับเคลื่อน และลักษณะเหตุการณ์ความเสี่ยงร่วมกัน ไม่จำแนกจากผลกระทบปลายทางหรือชื่อหน่วยงานเพียงอย่างเดียว

2. กำหนดประเภทหลักหนึ่งประเภท (Primary Risk Category): ความเสี่ยงแต่ละรายการต้องมีประเภทหลักหนึ่งประเภท พร้อมกำหนดเจ้าของความเสี่ยง (Risk Owner) ตามอำนาจและความรับผิดชอบที่เกี่ยวข้อง สามารถระบุประเภทที่เกี่ยวข้องเพิ่มเติมได้ โดยการจำแนกประเภทไม่ทดแทนการมอบหมายเจ้าของความเสี่ยงอย่างชัดเจน

3. จำแนกความเสี่ยงด้านปัญญาประดิษฐ์และเทคโนโลยีดิจิทัลตามลักษณะประเด็น: ไม่จัดเป็นความเสี่ยงด้านเทคโนโลยีดิจิทัลทุกกรณี เพียงเพราะมีการใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) หรือระบบดิจิทัล แต่ให้พิจารณาดังนี้

ประเภทหลัก	ลักษณะประเด็นที่ใช้พิจารณา
ความเสี่ยงด้านยุทธศาสตร์ (Strategic Risk: S)	ความสามารถในการปรับตัว การเลือกทิศทางหรือรูปแบบการลงทุน และการใช้เทคโนโลยีสร้างคุณค่าเพื่อบรรลุเป้าหมายเชิงยุทธศาสตร์
ความเสี่ยงด้านการดำเนินงาน (Operational Risk: O)	สมรรถนะบุคลากร กระบวนงาน การตรวจสอบผลลัพธ์ และวิธีนำเทคโนโลยีไปใช้ในการปฏิบัติงาน
ความเสี่ยงด้านการเงิน (Financial Risk: F)	ความคุ้มค่าทางการเงิน ต้นทุน ภาระผูกพัน หรือสภาพคล่องจากการลงทุนและใช้เทคโนโลยี
ความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล	การปฏิบัติตามกฎหมาย จริยธรรม ความโปร่งใส สิทธิของผู้มีส่วนได้ส่วนเสีย และธรรมาภิบาลด้านปัญญาประดิษฐ์

ประเภทหลัก	ลักษณะประเด็นที่ใช้พิจารณา
(Compliance and Governance Risk: C)	
ความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Technology Risk: D)	ความผิดพลาดหรือความล้มเหลวของระบบ โครงสร้างพื้นฐาน ข้อมูล แบบจำลอง ระบบอัตโนมัติ หรือกลไกความมั่นคงปลอดภัยทางเทคนิค

4. จำแนกความเสี่ยงด้านไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลตามเหตุการณ์หลัก: ให้พิจารณาประเภทหลักและความเชื่อมโยงดังนี้

- **ความเสี่ยงด้านเทคโนโลยีดิจิทัล (D):** เมื่อประเด็นหลักเป็นช่องโหว่ การโจมตีทางไซเบอร์ ความล้มเหลวของระบบ การควบคุมสิทธิทางเทคนิค หรือการสำรองและกู้คืนข้อมูล
- **ความเสี่ยงด้านการดำเนินงาน (O):** เมื่อประเด็นหลักเป็นความผิดพลาดของกระบวนงานหรือการปฏิบัติงาน เช่น ส่งข้อมูลให้ผู้รับผิดคน หรือจัดเก็บเอกสารไม่ปลอดภัย
- **ความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (C):** เมื่อประเด็นหลักเป็นการไม่ปฏิบัติตามหน้าที่หรือข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล

เหตุการณ์เดียวกันอาจเกี่ยวข้องกับหลายประเภท ให้ระบุความเชื่อมโยงและมาตรการร่วมโดยไม่สร้างรายการซ้ำโดยไม่จำเป็น ทั้งนี้ การคุ้มครองข้อมูลส่วนบุคคลครอบคลุมทั้งข้อมูลดิจิทัลและข้อมูลในรูปแบบอื่น

5. ระบุมิติผลกระทบร่วม (Cross-cutting Impact Dimensions): ชื่อเสียงและความเชื่อมั่น ชีวิตและความปลอดภัย ความต่อเนื่อง สิ่งแวดล้อมและ ESG ตลอดจนคุณภาพการศึกษา การวิจัย และวิชาการ ให้พิจารณาเป็นมิติผลกระทบร่วมที่อาจเกิดจากความเสี่ยงทุกประเภท ส่วนประเด็น ESG สามารถใช้ป้ายกำกับข้ามประเภท (Cross-cutting Tags) เพื่อแสดงความเกี่ยวข้องได้

6. กำหนดการจัดการสำหรับผลกระทบสำคัญ: หากมิติผลกระทบร่วมมีนัยสำคัญ ต้องกำหนดเจ้าของความเสี่ยง ตัวชี้วัดความเสี่ยงที่สำคัญ (KRI) เกณฑ์ที่เชื่อมโยงกับระดับความเสี่ยงที่ยอมรับได้ (RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (RT) มาตรการ และเงื่อนไขการรายงานหรือยกระดับ (Escalation) ให้เหมาะสม แม้ไม่ได้แยกเป็นประเภทความเสี่ยงหลัก

7. พิจารณาความเสี่ยงในภาพรวม: วิเคราะห์ความสัมพันธ์และการพึ่งพาระหว่างความเสี่ยง (Risk Interdependencies) ผลกระทบสะสม (Cumulative Impacts) และการกระจุกตัวของ

ความเสี่ยง (Risk Concentration) ทั้งระดับส่วนงานและระดับมหาวิทยาลัย โดยเฉพาะการพึ่งพาระบบ ผู้ให้บริการ แหล่งรายได้ หรือทรัพยากรร่วมกัน

8. บันทึกเหตุผลและรักษาประวัติ: บันทึกเหตุผลในการเลือกประเภทหลัก หากเปลี่ยนประเภทหรือรหัส ให้เก็บประวัติและตารางเทียบรหัส โดยรหัสประเด็นระดับมหาวิทยาลัยต้องสอดคล้องกับแผนที่ได้รับความเห็นชอบและกระบวนการอนุมัติที่เกี่ยวข้อง

ตัวอย่างการจำแนกประเภทความเสี่ยงหลัก ประเภทที่เกี่ยวข้อง และมิติผลกระทบร่วม

ตัวอย่างเหตุการณ์ความเสี่ยง	ประเภทหลัก	ประเภทที่อาจเกี่ยวข้อง	มิติผลกระทบร่วม
มหาวิทยาลัยอาจปรับตัวและใช้ประโยชน์จาก AI และเทคโนโลยีดิจิทัลเพื่อขับเคลื่อนยุทธศาสตร์ไม่ทันต่อการเปลี่ยนแปลง	**ด้านยุทธศาสตร์ (S)**	ด้านการดำเนินงาน (O) ด้านเทคโนโลยีดิจิทัล (D) และด้านกฎหมายและธรรมาภิบาล (C)	คุณภาพการศึกษาและการวิจัย ชื่อเสียงและความเชื่อมั่น
ระบบสารสนเทศสำคัญอาจหยุดชะงักจากช่องโหว่หรือการโจมตีทางไซเบอร์	**ด้านเทคโนโลยีดิจิทัล (D)**	ด้านการดำเนินงาน (O) และด้านกฎหมายและธรรมาภิบาล (C)	ความต่อเนื่อง ความลับของข้อมูล ชื่อเสียงและความเชื่อมั่น
การประมวลผลข้อมูลส่วนบุคคลอาจไม่เป็นไปตามหน้าที่หรือข้อกำหนดทางกฎหมาย	**ด้านกฎหมายและธรรมาภิบาล (C)**	ด้านการดำเนินงาน (O) และด้านเทคโนโลยีดิจิทัล (D) ตามลักษณะการประมวลผล	สิทธิและความเป็นส่วนตัว ชื่อเสียงและความเชื่อมั่น
บุคลากรอาจส่งข้อมูลส่วนบุคคลให้ผู้รับผิดคนจากขั้นตอนตรวจสอบที่ไม่เพียงพอ	**ด้านการดำเนินงาน (O)**	ด้านกฎหมายและธรรมาภิบาล (C) และด้านเทคโนโลยีดิจิทัล (D) หากเกี่ยวข้อง	สิทธิและความเป็นส่วนตัว ชื่อเสียงและความเชื่อมั่น
ฐานข้อมูลสำคัญอาจสูญหายหรือกู้คืนไม่สำเร็จจากความบกพร่องของระบบสำรองและกู้คืน	**ด้านเทคโนโลยีดิจิทัล (D)**	ด้านการดำเนินงาน (O)	ความต่อเนื่อง คุณภาพบริการ ชื่อเสียงและความเชื่อมั่น

ตัวอย่างเหตุการณ์ความเสี่ยง	ประเภทหลัก	ประเภทที่อาจเกี่ยวข้อง	มิติผลกระทบร่วม
รายรับอาจต่ำกว่าแผนจนเงินสดที่พร้อมใช้ลดลงต่ำกว่าเกณฑ์	**ด้านการเงิน (F)**	ด้านยุทธศาสตร์ (S)	ความต่อเนื่องของพันธกิจและบริการ
หลักสูตรอาจไม่ตอบสนองความต้องการของผู้เรียนและตลาดแรงงานจนไม่บรรลุเป้าหมายเชิงยุทธศาสตร์	**ด้านยุทธศาสตร์ (S)**	ด้านการดำเนินงาน (O) และด้านการเงิน (F)	คุณภาพการศึกษา ชื่อเสียงและความเชื่อมั่น
บุคลากรอาจปฏิบัติงานสำคัญได้ไม่ถูกต้องหรือไม่ทันเวลาเนื่องจากขาดสมรรถนะที่จำเป็น	**ด้านการดำเนินงาน (O)**	ด้านยุทธศาสตร์ (S) และด้านเทคโนโลยีดิจิทัล (D) ตามลักษณะงาน	คุณภาพบริการและความต่อเนื่อง
อาจเกิดอุบัติเหตุจากกระบวนงานหรือการควบคุมความปลอดภัยที่ไม่เพียงพอ	**ด้านการดำเนินงาน (O)**	ด้านกฎหมายและธรรมาภิบาล (C)	ชีวิต สุขภาพและความปลอดภัย ชื่อเสียงและความเชื่อมั่น
อาจเกิดการทุจริต การรับสินบนหรือการจัดซื้อจัดจ้างโดยมิชอบ	**ด้านกฎหมายและธรรมาภิบาล (C)**	ด้านการเงิน (F) และด้านการดำเนินงาน (O)	ชื่อเสียง ความเชื่อมั่นและธรรมาภิบาล
AI อาจให้ผลลัพธ์คลาดเคลื่อนจากข้อมูลหรือแบบจำลองที่ไม่มีคุณภาพ	**ด้านเทคโนโลยีดิจิทัล (D)**	ด้านการดำเนินงาน (O) และด้านกฎหมายและธรรมาภิบาล (C) ตามการนำไปใช้	คุณภาพการตัดสินใจ คุณภาพการศึกษาและการวิจัย ชื่อเสียงและความเชื่อมั่น

หมายเหตุ: ตารางนี้ใช้แสดงตัวอย่างการจำแนก ไม่ใช่ข้อความความเสี่ยงฉบับสมบูรณ์ ทุกส่วนงานต้องเพิ่มเติมสาเหตุ เหตุการณ์ และผลกระทบให้สอดคล้องกับวัตถุประสงค์จริง ประเภทที่เกี่ยวข้องและมิติผลกระทบให้ระบุเฉพาะที่มีเหตุผลรองรับ ไม่จำเป็นต้องใช้ครบทุกประเภทตามตัวอย่าง

4.7.6 องค์ประกอบขั้นต่ำของทะเบียนความเสี่ยง (Minimum Risk Register Components)

ทะเบียนความเสี่ยง (Risk Register) เป็นข้อมูลกลางที่เชื่อมโยงวัตถุประสงค์ รายละเอียดความเสี่ยง ผลการประเมิน การควบคุม มาตรการ และการติดตาม เพื่อสนับสนุนการบริหารและการตัดสินใจอย่างต่อเนื่อง

ให้จัดข้อมูลเป็น 6 หมวดดังต่อไปนี้ โดยทยอยบันทึกและปรับปรุงตามขั้นตอนที่เกี่ยวข้อง ไม่จำเป็นต้องกรอกผลการประเมินหรือแผนมาตรการให้ครบในขั้นตอนการระบุความเสี่ยง หากข้อมูลยังไม่พร้อม ให้ระบุสถานะ ผู้รับผิดชอบ และกำหนดเวลาจัดทำเพิ่มเติม

ก. ข้อมูลอ้างอิงและวัตถุประสงค์ (Reference Information and Objectives)

1. รหัสและชื่อความเสี่ยง (Risk ID and Title)
2. ระดับการบริหารและส่วนงานที่รับผิดชอบ (Management Level and Responsible Unit)
3. วัตถุประสงค์ เจ้าของวัตถุประสงค์ และความเชื่อมโยงกับยุทธศาสตร์ (Objective, Objective Owner and Strategic Linkage)
4. ตัวชี้วัดผลการดำเนินงานและเป้าหมายที่เกี่ยวข้อง (KPI and Target)
5. ประเภทความเสี่ยงหลัก (Primary Risk Category)
6. ประเภทที่เกี่ยวข้องและมิติผลกระทบร่วม (Related Categories and Cross-cutting Impact Dimensions)
7. กรอบเวลาและรอบการประเมิน (Time Horizon and Assessment Period)
8. วันที่ระบุ วันที่ทบทวนล่าสุด และฉบับข้อมูล (Identification Date, Latest Review Date and Version)

ข. รายละเอียดความเสี่ยง (Risk Description)

1. ข้อความความเสี่ยง (Risk Statement)
2. สาเหตุหรือปัจจัยขับเคลื่อน (Causes/Risk Drivers)
3. เหตุการณ์ความเสี่ยง (Risk Event)
4. ผลกระทบและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง (Impacts and Affected Stakeholders)
5. ความสัมพันธ์ การพึ่งพา และการกระจุกตัวของความเสี่ยง (Interdependencies and Risk Concentration)

6. เจ้าของความเสี่ยงและผู้ร่วมรับผิดชอบ (Risk Owner and Supporting Roles)

7. แหล่งข้อมูล หลักฐาน สมมติฐาน และข้อจำกัด (Sources, Evidence, Assumptions and Limitations)

<u>ค. การประเมินและการควบคุม (Assessment and Controls)</u>

1. เกณฑ์และวันที่ประเมิน (Assessment Criteria and Date)

2. ความเสี่ยงโดยธรรมชาติ (Inherent Risk): โอกาสเกิด ผลกระทบ คะแนน และระดับความเสี่ยง พร้อมเหตุผล

3. การควบคุมที่มีอยู่ (Existing Controls): วิธีปฏิบัติ ขอบเขต และความถี่

4. เจ้าของการควบคุม (Control Owner)

5. หลักฐานการออกแบบและการปฏิบัติ (Control Design and Operating Evidence)

6. ผลประเมินการควบคุม (Control Assessment): ความเหมาะสมของการออกแบบ การนำไปใช้ และประสิทธิผลในการปฏิบัติงาน

7. ความเสี่ยงคงเหลือ (Residual Risk): โอกาสเกิด ผลกระทบ คะแนน และระดับ ณ วันที่ประเมิน พร้อมหลักฐานและเหตุผล

8. สถานะเทียบกับกรอบการยอมรับความเสี่ยง (RA/RT Status)

9. เกณฑ์ยกระดับเป็นกรณีพิเศษหรือเหตุที่ไม่ยอมรับ (Override or Zero Tolerance Criteria): ระบุเหตุผลและระดับการตอบสนองแยกจากคะแนนความเสี่ยง

<u>ง. ตัวชี้วัดและข้อมูล (Indicators and Data)</u>

1. ตัวชี้วัดที่เกี่ยวข้อง (Relevant Indicators): KPI, KRI และตัวชี้วัดการควบคุมที่สำคัญ (KCI) ตามความจำเป็น โดยระบุหน้าที่ของแต่ละตัว

2. นิยาม สูตรคำนวณ และหน่วยวัด (Definition, Formula and Unit)

3. ค่าเริ่มต้น ค่าเป้าหมาย และช่วงเวลาที่ใช้วัด (Baseline, Target and Measurement Period)

4. เกณฑ์ที่เชื่อมโยงกับ RA/RT และช่วงสถานะ (RA/RT-linked Thresholds and Status Bands)

5. จุดแจ้งเตือนและเงื่อนไขดำเนินการ (Trigger and Action)

6. แหล่งข้อมูลและวิธีตรวจสอบ (Data Source and Validation Method)

7. เจ้าของข้อมูล (Data Owner)

8. ความถี่และกำหนดเวลารายงานข้อมูล (Monitoring Frequency and Data Reporting Deadline)

9. ค่าจริง ค่าคาดการณ์ และแนวโน้มตามความเกี่ยวข้อง (Actual Value, Forecast and Trend)

<u>จ. การตอบสนองและมาตรการ (Response and Treatment)</u>

1. แนวทางตอบสนองและเหตุผล (Risk Response and Rationale)

2. แผนบริหารความเสี่ยงและมาตรการ (Risk Treatment Plan and Actions)

3. เจ้าของมาตรการและผู้ร่วมดำเนินการ (Action Owner and Supporting Units): กำหนดผู้รับผิดชอบหลักให้ชัดเจนสำหรับแต่ละมาตรการ

4. ทรัพยากรและงบประมาณ (Resources and Budget)

5. จุดตรวจสอบความก้าวหน้าและกำหนดแล้วเสร็จ (Milestones and Completion Date)

6. ผลส่งมอบ หลักฐาน และเกณฑ์ยืนยันผล (Deliverables, Evidence and Verification Criteria)

7. ระดับความเสี่ยงคงเหลือเป้าหมายและสมมติฐาน (Target Residual Risk and Assumptions)

8. ผู้มีอำนาจอนุมัติมาตรการหรือยอมรับความเสี่ยง (Treatment Approval or Risk Acceptance Authority)

9. เงื่อนไขและวันสิ้นสุดการยอมรับความเสี่ยง หากมี (Acceptance Conditions and Expiry Date)

<u>ฉ. การติดตามและรายงาน (Monitoring and Reporting)</u>

1. สถานะและความก้าวหน้าของมาตรการ (Action Status and Progress): หากใช้ร้อยละความก้าวหน้า ต้องกำหนดวิธีคำนวณหรือเกณฑ์ให้ชัดเจน

2. ผลของมาตรการต่อความเสี่ยงและแนวโน้ม (Risk Treatment Results and Trend)

3. เหตุการณ์และเหตุการณ์เกือบเกิดความเสียหาย (Incidents and Near Misses)

4. ปัญหา อุปสรรค และข้อบกพร่องของการควบคุม (Issues, Obstacles and Control Deficiencies)

5. มาตรการแก้ไข ผู้รับผิดชอบ และกำหนดเวลา (Corrective Actions, Owners and Due Dates)

6. ประเด็นและสถานะการยกระดับ (Escalation Issues and Status)

7. ผลการตัดสินใจและบันทึกข้อสั่งการ (Decisions and Decision Log)

8. วันที่ติดตามและรอบติดตามครั้งถัดไป (Monitoring Date and Next Review Date)

9. บทเรียนและประเด็นปรับปรุง (Lessons Learned and Improvement Issues)

ข้อมูลทั้ง 6 หมวดสามารถจัดทำในแบบ RISK-MJU-01 หรือระบบสารสนเทศเดียวกัน และเชื่อมโยงหลักฐานจากระบบงานที่มีอยู่ได้ โดยต้องตรวจสอบย้อนกลับถึงแหล่งข้อมูล ผู้รับผิดชอบ และผลการตัดสินใจ

4.7.7 ตัวอย่างทะเบียนความเสี่ยงแบบย่อ (Illustrative Risk Register)

ตารางที่ 4-5 ตัวอย่างทะเบียนความเสี่ยงด้านการใช้ปัญญาประดิษฐ์และเทคโนโลยีดิจิทัล ตัวอย่างนี้เป็นข้อมูลสมมติเพื่ออธิบายการบันทึกตลอดวงจร ไม่ใช่ผลประเมินจริงหรือเกณฑ์ที่มหาวิทยาลัยอนุมัติ และไม่กำหนดให้จัดทำข้อมูลทุกช่องให้แล้วเสร็จในขั้นตอนที่ 3

หมวด/รายการ	ตัวอย่างการบันทึก
ก. รหัสและชื่อความเสี่ยง (Risk ID and Title)	**EX-S-01:** การปรับขีดความสามารถด้าน AI และดิจิทัลไม่ทันต่อยุทธศาสตร์ ใช้รหัสตัวอย่างเพื่อไม่สับสนกับรหัสในแผนที่ได้รับความเห็นชอบ
วัตถุประสงค์ (Objective)	ยกระดับความสามารถในการใช้ AI และเทคโนโลยีดิจิทัลเพื่อสนับสนุนผลลัพธ์เชิงยุทธศาสตร์ภายในปีงบประมาณ พ.ศ. 2570
ประเภทหลัก (Primary Category)	ความเสี่ยงด้านยุทธศาสตร์ (Strategic Risk: S)
ประเภทที่เกี่ยวข้อง (Related Categories)	ด้านการดำเนินงาน (O) ด้านเทคโนโลยีดิจิทัล (D) และด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (C)
มิติผลกระทบร่วม (Cross-cutting Impacts)	คุณภาพการศึกษาและการวิจัย ชื่อเสียงและความเชื่อมั่น และธรรมาภิบาล
ข. ข้อความความเสี่ยง (Risk Statement)	เนื่องจากการกำกับดูแล AI การพัฒนาสมรรถนะ และการเชื่อมโยงข้อมูลยังไม่ครอบคลุม อาจทำให้มหาวิทยาลัยปรับขีดความสามารถและนำ AI มาใช้สนับสนุนงานสำคัญไม่ทันต่อแผน ส่งผลให้ไม่บรรลุเป้าหมายด้านคุณภาพ ประสิทธิภาพ และความสามารถในการแข่งขัน

หมวด/รายการ	ตัวอย่างการบันทึก
เจ้าของความเสี่ยง (Risk Owner)	ผู้บริหารที่ได้รับมอบหมายให้กำกับการขับเคลื่อนยุทธศาสตร์ด้าน AI และดิจิทัล
ค. ความเสี่ยงโดยธรรมชาติ (Inherent Risk)	โอกาสเกิด 4 × ผลกระทบ 4 = **16 ระดับสูงมาก (E)** โดยมีเหตุผลตามเกณฑ์และกรอบเวลาที่ใช้ประเมิน
การควบคุมที่มีอยู่ (Existing Controls)	แนวทางใช้เทคโนโลยี การพัฒนาทักษะ และการสอบทานโครงการนำร่อง โดยต้องระบุเจ้าของ ความถี่ และหลักฐานของแต่ละการควบคุม
ผลประเมินการควบคุม (Control Assessment)	สมมติว่ามีหลักฐานยืนยันการนำไปใช้และผลทดสอบในงานนำร่อง ซึ่งช่วยลดโอกาสเกิดบางส่วน แต่ความครอบคลุมและผลต่อความรุนแรงยังมีข้อจำกัด
ความเสี่ยงคงเหลือ (Residual Risk)	โอกาสเกิด 3 × ผลกระทบ 4 = **12 ระดับสูง (H)** การลดโอกาสเกิดจาก 4 เป็น 3 ต้องมีหลักฐานรองรับ ไม่ลดคะแนนจากการมีแผนหรือจัดกิจกรรมเพียงอย่างเดียว
ง. ตัวชี้วัดความเสี่ยง (KRI)	ร้อยละบุคลากรกลุ่มเป้าหมายในงานสำคัญที่ผ่านเกณฑ์สมรรถนะ AI และดิจิทัล โดยใช้ผลทดสอบหรือประเมินการปฏิบัติ ไม่ใช้จำนวนผู้เข้าอบรมแทนสมรรถนะ
นิยามและสูตร (Definition and Formula)	จำนวนบุคลากรกลุ่มเป้าหมายที่ผ่านเกณฑ์สมรรถนะ ÷ จำนวนบุคลากรกลุ่มเป้าหมายทั้งหมด × 100 โดยกำหนดกลุ่มเป้าหมายและเกณฑ์ผ่านไว้ล่วงหน้า
กรอบ RA และเกณฑ์ปฏิบัติ (RA and Operational Threshold)	กำหนดเชิงสมมติให้ยอมรับความเสี่ยงต่อความไม่พร้อมของบุคลากรในระดับต่ำ และใช้สัดส่วนผู้ผ่านเกณฑ์ **ตั้งแต่ร้อยละ 80 ขึ้นไป** เป็นเกณฑ์ปฏิบัติประกอบการติดตาม
ขอบเขต RT (RT Boundary)	กำหนดเชิงสมมติให้สัดส่วนผู้ผ่านเกณฑ์ไม่ต่ำกว่าร้อยละ 70 ณ จุดตรวจสอบที่กำหนด โดยต้องดำเนินมาตรการเมื่อยังต่ำกว่าเกณฑ์ปฏิบัติร้อยละ 80
ช่วงเฝ้าระวัง (Warning Band)	ตั้งแต่ร้อยละ 70 แต่ต่ำกว่าร้อยละ 80 ให้เร่งพัฒนาสมรรถนะ วิเคราะห์ช่องว่าง และติดตามใกล้ชิด
จุดแจ้งเตือนและการดำเนินการ (Trigger and Action)	ต่ำกว่าร้อยละ 70 ณ จุดตรวจสอบ ให้ยกระดับและจัดทำแผนแก้ไข หรือหากคาดว่าจะไม่บรรลุเกณฑ์ในรอบถัดไป ให้ดำเนินการล่วงหน้า
เจ้าของข้อมูลและความถี่ (Data Owner and Frequency)	ผู้รับผิดชอบข้อมูลการพัฒนาบุคลากรที่ได้รับมอบหมาย ติดตามตามจุดตรวจสอบรายไตรมาส และถี่ขึ้นเมื่อเข้าเกณฑ์เตือน

หมวด/รายการ	ตัวอย่างการบันทึก
จ. แนวทางตอบสนอง (Risk Response)	ลดความเสี่ยงควบคู่กับใช้ประโยชน์จากโอกาส (Risk Reduction and Opportunity Pursuit)
มาตรการสำคัญ (Key Actions)	จัดทำกรอบการกำกับดูแล AI พัฒนาสมรรถนะตามบทบาท และดำเนินโครงการนำร่องที่ผ่านการประเมินความเสี่ยงและผลลัพธ์
เจ้าของมาตรการ (Action Owners)	กำหนดผู้รับผิดชอบหลักหนึ่งรายต่อมาตรการ เช่น มาตรการด้านกำกับดูแล ด้านบุคลากร และด้านเทคโนโลยี พร้อมผู้ร่วมดำเนินการ
ความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk)	โอกาสเกิด 2 × ผลกระทบ 3 = **6 ระดับปานกลาง (M)** ภายในสิ้นปีงบประมาณ พ.ศ. 2570 โดยต้องมีมาตรการและหลักฐานรองรับทั้งการลดโอกาสเกิดและผลกระทบ หากลดได้เฉพาะโอกาสเกิด ต้องทบทวนค่าเป้าหมาย
ผลส่งมอบและหลักฐาน (Deliverables and Evidence)	กรอบกำกับดูแลที่ได้รับอนุมัติ ผลประเมินสมรรถนะ ผลทดสอบโครงการนำร่อง และหลักฐานผลต่อคุณภาพหรือประสิทธิภาพของงาน
ฉ. สถานะและแนวโน้ม (Status and Trend)	บันทึกจากผลจริงในแต่ละรอบ พร้อมเปรียบเทียบค่า KRI ความก้าวหน้ามาตรการ และระดับความเสี่ยงคงเหลือ
ประเด็นยกระดับ (Escalation Issues)	ความเสี่ยงคงเหลือระดับสูง KRI เกิน RT มาตรการสำคัญล่าช้า หรือการจัดการต้องใช้ทรัพยากรและอำนาจเกินขอบเขตเจ้าของความเสี่ยง

ข้อควรพิจารณา: สมรรถนะบุคลากรเป็นเพียงปัจจัยหนึ่งของความเสี่ยงในตัวอย่าง ค่า KRI ที่ผ่านเกณฑ์จึงไม่ยืนยันว่าความเสี่ยงทั้งรายการอยู่ภายใน RA/RT หรือบรรลุระดับเป้าหมาย ต้องพิจารณาความพร้อมด้านการกำกับดูแล ข้อมูล ระบบ และผลลัพธ์ของการนำ AI ไปใช้ร่วมด้วย หากไม่มีหลักฐานเพียงพอว่าการควบคุมช่วยลดโอกาสเกิดหรือผลกระทบได้ ต้องไม่ลดระดับความเสี่ยงโดยอัตโนมัติ และให้บันทึกข้อจำกัดกับแผนตรวจสอบเพิ่มเติม

4.7.8 ผลผลิตขั้นต่ำของขั้นตอนที่ 3 (Minimum Outputs of Step 3)

เมื่อสิ้นสุดขั้นตอนการระบุความเสี่ยง ต้องมีข้อมูลและหลักฐานอย่างน้อยดังต่อไปนี้

1. ทะเบียนความเสี่ยงในส่วนการระบุที่เจ้าของความเสี่ยงยืนยัน (Risk Register Confirmed by Risk Owners): ครอบคลุมข้อมูลอ้างอิง วัตถุประสงค์ และรายละเอียดความเสี่ยง ส่วนผลประเมินและมาตรการให้เพิ่มเติมในขั้นตอนต่อไป

2. รายการความเสี่ยงและโอกาสที่เชื่อมโยงกับวัตถุประสงค์ (Objective-linked Risks and Opportunities)

3. ข้อความความเสี่ยงตามโครงสร้างสาเหตุ–เหตุการณ์–ผลกระทบ (Cause–Event–Impact Risk Statements)

4. ประเภทความเสี่ยงหลัก ประเภทที่เกี่ยวข้อง และมิติผลกระทบร่วม (Primary Categories, Related Categories and Cross-cutting Impacts)

5. เจ้าของความเสี่ยงและผู้เกี่ยวข้อง (Risk Owners and Related Roles)

6. ความสัมพันธ์ การพึ่งพา และการกระจุกตัวที่ระบุได้เบื้องต้น (Preliminary Interdependencies and Concentrations)

7. ประเด็นที่ต้องยกระดับทันทีหรือเสนอพิจารณาระดับมหาวิทยาลัย พร้อมเหตุผล (Immediate Escalation or Enterprise-level Consideration Issues)

8. หลักฐาน แหล่งข้อมูล สมมติฐาน และข้อจำกัด (Evidence, Sources, Assumptions and Limitations)

การเสนอประเด็นเพื่อพิจารณาระดับมหาวิทยาลัยไม่ทำให้เป็นความเสี่ยงระดับมหาวิทยาลัยโดยอัตโนมัติ ต้องผ่านการกลั่นกรองและอนุมัติตามอำนาจ ส่วนเหตุเร่งด่วนให้ตอบสนองและรายงานทันที โดยไม่รอการยืนยันทะเบียนหรือการประเมินให้ครบทุกขั้นตอน

4.8 ขั้นตอนที่ 4 การวิเคราะห์และประเมินความเสี่ยง (Risk Analysis and Evaluation)

การวิเคราะห์และประเมินความเสี่ยงมีวัตถุประสงค์เพื่อทำความเข้าใจสาเหตุ ลักษณะเหตุการณ์ โอกาสเกิด ผลกระทบ และประสิทธิผลของการควบคุม รวมทั้งประเมินระดับความเสี่ยงเพื่อเปรียบเทียบกับกรอบระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) ใช้จัดลำดับความสำคัญ เลือกแนวทางตอบสนอง และพิจารณาการยกระดับ

การวิเคราะห์ความเสี่ยง (Risk Analysis) เป็นการทำความเข้าใจและประเมินลักษณะกับระดับความเสี่ยง ส่วน **การประเมินเพื่อตัดสินใจ (Risk Evaluation)** เป็นการเปรียบเทียบผลการวิเคราะห์กับเกณฑ์ที่กำหนด เพื่อพิจารณาว่าต้องจัดการเพิ่มเติม ยอมรับตามอำนาจ หรือยกระดับอย่างไร

คะแนนความเสี่ยงเป็นข้อมูลประกอบการตัดสินใจ ต้องพิจารณาร่วมกับแนวโน้ม ความเร็วในการเกิดผลกระทบ ความสัมพันธ์และการกระจุกตัวของความเสี่ยง คุณภาพข้อมูล เกณฑ์ยกระดับเป็น

กรณีพิเศษ (Override Criteria) และข้อจำกัดตามกฎหมาย โดยใช้เกณฑ์ที่กำหนดไว้ในขั้นตอนที่ 2 และบันทึกเหตุผลกับหลักฐานให้ตรวจสอบย้อนกลับได้

4.8.1 ระดับความเสี่ยงที่ต้องประเมิน (Risk Assessment States)

ให้แยกการประเมินความเสี่ยง 3 สถานะดังต่อไปนี้

สถานะ	ความหมาย	หลักในการประเมิน
ความเสี่ยงโดยธรรมชาติ (Inherent Risk)	ระดับความเสี่ยงก่อนพิจารณาผลของการควบคุมหรือมาตรการที่มีอยู่	ประเมินโอกาสเกิดและผลกระทบภายใต้สมมติฐานว่ายังไม่มีผลของการควบคุมที่นำมาพิจารณา พร้อมระบุสมมติฐานให้ชัดเจน
ความเสี่ยงคงเหลือ (Residual Risk)	ระดับความเสี่ยงภายหลังพิจารณาผลของการควบคุมที่นำไปใช้และมีหลักฐานการทำงาน ณ วันที่ประเมิน	ใช้ผลประเมินการออกแบบ การนำไปใช้ และประสิทธิผลของการควบคุม พร้อมหลักฐานรองรับการเปลี่ยนแปลงของโอกาสเกิดหรือผลกระทบ
ความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk)	ระดับความเสี่ยงที่คาดว่าจะเหลือหลังดำเนินมาตรการเพิ่มเติมและเกิดผลตามที่กำหนด	ระบุเป็นค่าคาดการณ์ พร้อมมาตรการ สมมติฐาน ผู้รับผิดชอบ กำหนดเวลา และวิธียืนยันผล โดยจัดทำหรือยืนยันร่วมกับแผนในขั้นตอนที่ 5

ห้ามใช้ความเสี่ยงคงเหลือเป้าหมายแทนความเสี่ยงคงเหลือปัจจุบัน และห้ามลดคะแนนความเสี่ยงคงเหลือเพียงเพราะมีแผน ได้รับอนุมัติงบประมาณ หรือกำลังดำเนินกิจกรรม หากยังไม่มีหลักฐานว่ามาตรการช่วยลดโอกาสเกิดหรือผลกระทบได้จริง

กรณีการควบคุมมีผลเพียงบางส่วน ให้พิจารณาเฉพาะผลที่มีหลักฐานรองรับ หากหลักฐานไม่เพียงพอ ต้องบันทึกข้อจำกัดและกำหนดการตรวจสอบเพิ่มเติม ไม่ถือว่าการควบคุมนั้นมีประสิทธิผลเต็มที่ และไม่ใช้วิธีหักคะแนนประสิทธิผลของการควบคุมออกจากคะแนนความเสี่ยงโดยตรง

ตัวอย่าง: ความเสี่ยงระบบสำคัญหยุดชะงักมีความเสี่ยงโดยธรรมชาติเท่ากับโอกาสเกิด 4 × ผลกระทบ 4 = 16 หากมีหลักฐานว่าการแก้ไขช่องโหว่ช่วยลดโอกาสเกิดเป็น 3 แต่ยังไม่มีหลักฐานว่ากู้คืนบริการได้เร็วขึ้น ความเสี่ยงคงเหลืออาจเป็น 3 × 4 = 12 ส่วนเป้าหมาย 2 × 3 = 6 ต้องอาศัยมาตรการเพิ่มเติมและผลทดสอบที่รองรับทั้งการลดโอกาสเกิดและผลกระทบ

4.8.2 เกณฑ์โอกาสเกิด (Likelihood Criteria)

ต้องกำหนดกรอบเวลาที่ใช้ประเมิน (Time Horizon) ให้ชัดเจนและใช้สอดคล้องกันในการประเมินแต่ละสถานะ โดยทั่วไปอาจใช้หนึ่งปีงบประมาณ หรือช่วงเวลาของยุทธศาสตร์ โครงการ สัญญา หรืออายุระบบตามความเหมาะสม

ให้ประเมินโอกาสเกิดจากข้อมูลเหตุการณ์ แนวโน้ม ปัจจัยขับเคลื่อน ระดับการเปิดรับความเสี่ยง และความเห็นผู้เชี่ยวชาญตามความเกี่ยวข้อง ไม่สรุปว่าโอกาสเกิดต่ำเพียงเพราะไม่เคยเกิดเหตุ หรือยังไม่มีข้อมูลในอดีต

ตารางที่ 4-6 ***ตารางแสดงแนวทางการประเมินโอกาสเกิด (Likelihood)***

คะแนน	ระดับ	คำอธิบายเชิงคุณภาพ	ตัวอย่างความถี่เฉลี่ยระยะยาว
1	**น้อยมาก (Rare)**	มีโอกาสเกิดน้อยมากภายในกรอบเวลาประเมิน และต้องอาศัยเงื่อนไขผิดปกติหลายประการ	น้อยกว่า 0.2 ครั้งต่อปี หรือห่างกันโดยเฉลี่ยมากกว่า 5 ปี
2	**น้อย (Unlikely)**	อาจเกิดขึ้นได้ แต่ข้อมูลและเงื่อนไขปัจจุบันยังไม่ชี้ว่ามีแนวโน้มเกิดในกรอบเวลาประเมิน	ตั้งแต่ 0.2 แต่ต่ำกว่า 1 ครั้งต่อปี
3	**ปานกลาง (Possible)**	มีความเป็นไปได้ที่จะเกิด โดยมีปัจจัยหรือหลักฐานสนับสนุนบางส่วน	ตั้งแต่ 1 แต่ต่ำกว่า 2 ครั้งต่อปี
4	**มาก (Likely)**	มีแนวโน้มเกิดสูง หรือมีปัจจัยขับเคลื่อนและการเปิดรับความเสี่ยงอย่างต่อเนื่อง	ตั้งแต่ 2 ถึง 6 ครั้งต่อปี
5	**มากที่สุด (Almost Certain)**	มีแนวโน้มเกิดเกือบแน่นอนภายในกรอบเวลาประเมิน หรือเกิดซ้ำอย่างต่อเนื่อง	มากกว่า 6 ครั้งต่อปี

ตัวอย่างความถี่ในตารางเป็นแนวทางสำหรับเหตุการณ์ที่เกิดซ้ำ ไม่ใช่เกณฑ์ตายตัวสำหรับความเสี่ยงทุกประเภท และไม่ใช่ค่าความน่าจะเป็นโดยตรง ต้องกำหนดให้ชัดเจนว่าอะไรนับเป็นหนึ่งเหตุการณ์ และข้อมูลครอบคลุมช่วงเวลาใดก่อนนำไปใช้ หากใช้เกณฑ์ความน่าจะเป็นแทนความถี่ ต้องกำหนดช่วงคะแนนที่ไม่ซ้อนทับและครอบคลุมค่าที่เป็นไปได้ พร้อมอนุมัติตามอำนาจก่อนใช้ ไม่แปลงความถี่เป็นความน่าจะเป็นโดยไม่มีแบบจำลองและสมมติฐานรองรับ

สำหรับ **ความเสี่ยงด้านยุทธศาสตร์ (Strategic Risk)** หรือ **ความเสี่ยงเกิดใหม่ (Emerging Risk)** ที่ไม่เหมาะกับการวัดเป็นความถี่ ให้พิจารณาจาก

1. ความน่าจะเป็นในกรอบเวลาประเมิน (Probability within the Time Horizon)
2. แนวโน้มและปัจจัยขับเคลื่อน (Trends and Risk Drivers)
3. ความเปราะบางและระดับการเปิดรับความเสี่ยง (Vulnerability and Risk Exposure)
4. สมมติฐานเชิงยุทธศาสตร์และการเปลี่ยนแปลงของสมมติฐาน (Strategic Assumptions and Changes)
5. ข้อมูลคู่เทียบและความเห็นผู้เชี่ยวชาญ (Benchmarking Data and Expert Judgement)
6. ผลการวิเคราะห์สถานการณ์สมมติ (Scenario Analysis)
7. ข้อมูลจากการสำรวจแนวโน้มและสัญญาณอนาคต (Horizon Scanning)
8. ระดับความเชื่อมั่นและข้อจำกัดของข้อมูล (Confidence and Data Limitations)

ตัวอย่าง: การประเมินโอกาสที่จำนวนผู้เข้าศึกษาจริงจะต่ำกว่าเกณฑ์ในปีงบประมาณ ไม่ควรใช้จำนวนครั้งที่เคยรับผู้เรียนต่ำกว่าแผนเพียงอย่างเดียว แต่ควรพิจารณาจำนวนผู้สมัคร ผู้ผ่านคัดเลือก ผู้ยืนยันสิทธิ์ อัตราเข้าศึกษาจริง แนวโน้มประชากร และการแข่งขันร่วมกัน

เมื่อข้อมูลเชิงสถิติกับดุลยพินิจเชิงคุณภาพให้ผลต่างกัน ต้องบันทึกเหตุผล แหล่งข้อมูล และสมมติฐานที่ใช้เลือกคะแนน หากยังมีความไม่แน่นอนสูง ให้แสดงข้อจำกัดและพิจารณาหลายสถานการณ์ แทนการลดคะแนนโดยไม่มีหลักฐาน

4.8.3 เกณฑ์ผลกระทบ (Impact Criteria)

ให้ประเมินผลกระทบทุกมิติที่เกี่ยวข้องและบันทึกคะแนนแยกตามมิติ โดยใช้ **คะแนนสูงสุดที่มีเหตุผลและหลักฐานรองรับ** เป็นคะแนนผลกระทบ (Impact Score) ไม่เฉลี่ยคะแนนข้ามมิติ เพราะอาจลดทอนความสำคัญของผลกระทบรุนแรงบางด้าน

การประเมินต้องอ้างอิงเหตุการณ์หรือสถานการณ์ที่ระบุไว้อย่างชัดเจน และใช้คะแนนโอกาสเกิดกับผลกระทบของสถานการณ์เดียวกัน ไม่เลือกโอกาสเกิดจากเหตุการณ์ทั่วไปมาคูณกับผลกระทบจากสถานการณ์รุนแรงอีกแบบหนึ่ง หากมีหลายสถานการณ์ที่แตกต่างกันอย่างมีนัยสำคัญ ให้ประเมินแยกและอธิบายผลที่ใช้ประกอบการตัดสินใจ

ตารางที่ 4-8 ***ตารางแสดงคำอธิบายกลางสำหรับการประเมินผลกระทบ (Impact)***

คะแนน	ระดับ	คำอธิบายกลาง
1	น้อยมาก (Insignificant)	ผลกระทบเล็กน้อย แก้ไขได้ในการปฏิบัติงานประจำ ไม่กระทบเป้าหมาย บริการ หรือผู้มีส่วนได้ส่วนเสียอย่างมีนัยสำคัญ
2	น้อย (Minor)	ผลกระทบจำกัดและฟื้นฟูได้ด้วยทรัพยากรที่มี ทำให้การดำเนินงานหรือผลลัพธ์เบี่ยงเบนเล็กน้อย
3	ปานกลาง (Moderate)	กระทบเป้าหมาย คุณภาพบริการ หรือผู้มีส่วนได้ส่วนเสียอย่างมีนัยสำคัญ ต้องมีมาตรการแก้ไขและการกำกับติดตามเพิ่มเติม
4	มาก (Major)	กระทบอย่างรุนแรงต่อวัตถุประสงค์สำคัญ หลายส่วนงาน หรือความต่อเนื่อง ต้องประสานการจัดการและทรัพยากรระดับมหาวิทยาลัย
5	มากที่สุดหรือวิกฤต (Severe/Catastrophic)	กระทบรุนแรงมากต่อชีวิต พันธกิจหลัก ความสามารถดำเนินงาน ฐานะทางการเงิน สิทธิที่ต้องคุ้มครอง หรือความเชื่อมั่นในวงกว้าง และอาจฟื้นฟูได้ยากหรือไม่สามารถฟื้นคืนได้ทั้งหมด

คำอธิบายกลางใช้ประกอบการประเมิน ไม่ให้ใช้อำนาจของผู้จัดการเหตุหรือจำนวนส่วนงานที่เกี่ยวข้องเป็นตัวกำหนดคะแนนเพียงอย่างเดียว ต้องพิจารณาความรุนแรง ขนาด ระยะเวลา และความสามารถในการฟื้นฟูผลกระทบด้วย

มิติผลกระทบที่ต้องพิจารณา (Impact Dimensions) ให้พิจารณามิติต่อไปนี้ตามความเกี่ยวข้อง และระบุเหตุผลเมื่อไม่นำมิติใดมาใช้

1. **ยุทธศาสตร์และผลการดำเนินงาน (Strategy and Performance):** ความเบี่ยงเบนของผลลัพธ์สำคัญและความสามารถในการบรรลุแผนยุทธศาสตร์
2. **การดำเนินงานและคุณภาพบริการ (Operations and Service Quality):** ความล่าช้า ความผิดพลาด ปริมาณงาน และผู้รับบริการที่ได้รับผลกระทบ
3. **การเงินและทรัพย์สิน (Finance and Assets):** ความเสียหาย รายได้ที่สูญเสีย ค่าใช้จ่ายเพิ่มเติม สภาพคล่อง และภาระผูกพัน
4. **กฎหมาย จริยธรรม และธรรมาภิบาล (Legal, Ethics and Governance):** ลักษณะการฝ่าฝืน ความรับผิด ข้อพิพาท และผลต่อสิทธิหรือการกำกับดูแล

5. **ชื่อเสียงและความเชื่อมั่น (Reputation and Trust):** ขอบเขต ระยะเวลา และผลต่อความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย

6. **บุคลากร นักศึกษา สุขภาพ และความปลอดภัย (People, Health and Safety):** การบาดเจ็บ การเจ็บป่วย การสูญเสียชีวิต และผลต่อสุขภาวะ

7. **ข้อมูลและเทคโนโลยีดิจิทัล (Information and Digital Technology):** ความลับ ความถูกต้องครบถ้วน ความพร้อมใช้ และความมั่นคงปลอดภัยของข้อมูลและระบบ

8. **ความต่อเนื่องและการฟื้นตัว (Continuity and Recovery):** ระยะเวลาหยุดชะงัก ระดับบริการที่รักษาได้ และความสามารถในการกู้คืน

9. **สิ่งแวดล้อม สังคม และธรรมาภิบาล (Environmental, Social and Governance: ESG):** ความเสียหายต่อสิ่งแวดล้อม ชุมชน สิทธิ ความเสมอภาค และผู้ได้รับผลกระทบที่เปราะบาง

10. **การศึกษา การวิจัย และวิชาการ (Education, Research and Academic Activities):** คุณภาพการเรียนรู้ ความก้าวหน้าของผู้เรียน ผลงานวิจัย นวัตกรรม และความซื่อสัตย์ทางวิชาการ

มิติผลกระทบไม่ใช่ประเภทความเสี่ยงหลักเพิ่มเติม ความเสี่ยงแต่ละรายการยังคงจำแนกตามประเภทหลัก S O F C D และสามารถมีหลายมิติผลกระทบได้

การกำหนดเกณฑ์เฉพาะมิติ (Dimension-specific Criteria) ให้กำหนดเกณฑ์เฉพาะมิติโดยใช้ข้อมูลของส่วนงานและกรอบมหาวิทยาลัย พร้อมบันทึกตามแบบในภาคผนวก ง โดยระบุอย่างน้อย

- นิยามผลกระทบและหน่วยวัด (Impact Definition and Unit)
- ฐานที่ใช้เปรียบเทียบ (Reference Base): เช่น งบประมาณ รายได้ จำนวนผู้รับบริการ หรือช่วงเวลาบริการ
- ช่วงคะแนน 1–5 ที่ไม่ซ้อนทับและไม่มีช่องว่าง (Complete and Non-overlapping Score Bands)
- กรอบเวลาและสมมติฐาน (Time Horizon and Assumptions)
- แหล่งข้อมูลและหลักฐาน (Data Sources and Evidence)
- ผู้อนุมัติ วันที่มีผล และฉบับเกณฑ์ (Approver, Effective Date and Version)

เกณฑ์การเงินที่ใช้ร้อยละต้องระบุฐานคำนวณ เกณฑ์ความต่อเนื่องต้องสัมพันธ์กับความสำคัญของบริการและเป้าหมายการฟื้นตัว ส่วนเกณฑ์ข้อมูลต้องพิจารณาความอ่อนไหวและสิทธิของเจ้าของข้อมูลร่วมกับจำนวนรายการ ไม่ใช้ปริมาณเพียงอย่างเดียว

กรณียังไม่มีเกณฑ์เชิงปริมาณ ให้ใช้คำอธิบายกลางหรือเกณฑ์เชิงคุณภาพที่ได้รับความเห็นชอบ พร้อมเหตุผลและหลักฐาน ห้ามสร้างหรือปรับเกณฑ์ย้อนหลังเพื่อให้ได้คะแนนที่ต้องการ

ตัวอย่างการเลือกคะแนนผลกระทบ: หากสถานการณ์หนึ่งได้รับคะแนนด้านการเงิน 2 ด้านการดำเนินงาน 3 และด้านข้อมูลส่วนบุคคล 4 ให้ใช้คะแนนผลกระทบรวมเป็น 4 พร้อมบันทึกคะแนนรายมิติและเหตุผล ไม่ใช้ค่าเฉลี่ยเท่ากับ 3

เมื่อผลกระทบเท่ากับ 5 ให้ใช้แนวทางตอบสนองอย่างน้อยเทียบเท่าความเสี่ยงระดับสูงตามเกณฑ์ Override ส่วนเหตุ Zero Tolerance ให้รายงานและตอบสนองทันทีตามข้อกำหนด โดยบันทึกระดับการตอบสนองแยกจากคะแนนความเสี่ยง

4.8.4 การประเมินประสิทธิผลของการควบคุม (Control Effectiveness Assessment)

ให้ประเมินการควบคุมที่มีอยู่แต่ละรายการ โดยระบุเจ้าของการควบคุม ขอบเขต ความถี่และหลักฐาน พร้อมพิจารณาอย่างน้อย 3 มิติ ดังต่อไปนี้

1. ความเหมาะสมของการออกแบบ (Design Adequacy): การควบคุมตอบสนองต่อสาเหตุ เหตุการณ์ หรือผลกระทบของความเสี่ยงได้หรือไม่ มีขั้นตอน ผู้รับผิดชอบ และเงื่อนไขดำเนินการชัดเจนเพียงใด

2. การนำไปใช้ (Implementation): การควบคุมได้รับการนำไปใช้จริงและครอบคลุมกระบวนงาน ระบบ หรือส่วนงานตามขอบเขตที่กำหนดหรือไม่

3. ประสิทธิผลในการปฏิบัติงาน (Operating Effectiveness): การควบคุมทำงานถูกต้องสม่ำเสมอ และทันเวลา รวมทั้งมีผลช่วยลดโอกาสเกิดหรือผลกระทบตามวัตถุประสงค์หรือไม่ หลักฐานอาจประกอบด้วยเอกสารอนุมัติ บันทึกการปฏิบัติงาน รายงานจากระบบ บันทึกการเข้าถึง ผลทดสอบ ตัวอย่างรายการ ข้อยกเว้น และข้อบกพร่อง โดยต้องระบุช่วงเวลาที่หลักฐานครอบคลุมและวิธีตรวจสอบให้ชัดเจน

ตารางที่ 4-9 ***ตารางแสดงเกณฑ์สรุปผลการประเมินการควบคุม***

ผลการประเมิน	ข้อพิจารณา	การนำไปใช้ประเมินความเสี่ยงคงเหลือ
มีประสิทธิผล (Effective)	ออกแบบตอบสนองต่อความเสี่ยง มีเจ้าของการควบคุม นำไปใช้ครบตามขอบเขต ปฏิบัติสม่ำเสมอ และมีหลักฐานหรือผลทดสอบสนับสนุน	พิจารณาผลต่อโอกาสเกิดหรือผลกระทบตามขอบเขตที่มีหลักฐานรองรับ ไม่ถือว่าต้องลดคะแนนเสมอไป
มีประสิทธิผลบางส่วน (Partially Effective)	มีการควบคุมและหลักฐานว่าทำงานได้บางส่วน แต่ยังมีช่องว่าง ขอบเขตไม่ครบ ปฏิบัติไม่สม่ำเสมอ หรือมีข้อยกเว้นที่กระทบผลของการควบคุม	พิจารณาเฉพาะส่วนที่ยืนยันผลได้ พร้อมบันทึกช่องว่างและมาตรการปรับปรุง
ไม่มีประสิทธิผล (Ineffective)	การออกแบบไม่ตอบสนองต่อความเสี่ยงสำคัญ หรือมีหลักฐานว่าไม่ได้นำไปใช้หรือไม่ทำงานตามวัตถุประสงค์	ไม่ถือว่าช่วยลดความเสี่ยงในส่วนที่บกพร่อง และต้องกำหนดการแก้ไข
ไม่มีการควบคุม (No Control)	ไม่พบการควบคุมสำหรับสาเหตุ เหตุการณ์ หรือผลกระทบที่พิจารณา	ประเมินโดยไม่อ้างผลลดความเสี่ยงจากการควบคุมที่ยังไม่มี
ยังไม่สามารถยืนยันประสิทธิผล (Not Yet Verified)	หลักฐานไม่เพียงพอ ไม่ครอบคลุมช่วงเวลา หรือยังไม่ได้ทดสอบจนสามารถสรุปผลได้	บันทึกข้อจำกัด ไม่ถือว่ามีประสิทธิผลเต็มที่ และกำหนดผู้รับผิดชอบกับเวลาตรวจสอบเพิ่มเติม

การไม่มีหลักฐานเพียงพอแตกต่างจากการมีหลักฐานว่าการควบคุมไม่มีประสิทธิผล จึงต้องบันทึกสถานะให้ตรงกับข้อเท็จจริง อย่างไรก็ตาม ทั้งสองกรณีไม่ควรนำมาอ้างว่าการควบคุมช่วยลดความเสี่ยงได้เต็มที่

หากสรุปผลการควบคุมหลายรายการร่วมกัน ต้องพิจารณาความสำคัญและการพึ่งพากันของแต่ละรายการ ไม่เฉลี่ยผลโดยจนทำให้ข้อบกพร่องของการควบคุมสำคัญถูกลดทอน

ผลประเมินการควบคุมใช้ประกอบดุลยพินิจในการกำหนด **โอกาสเกิดคงเหลือ (Residual Likelihood)** และ **ผลกระทบคงเหลือ (Residual Impact)** โดยอธิบายว่าการควบคุมใดช่วยลดองค์ประกอบใดและมีหลักฐานอย่างไร ตามวิธีประเมินในคู่มือฉบับนี้ ไม่ให้นำคะแนนหรือร้อยละประสิทธิผลของการควบคุมไปหักออกจากคะแนนความเสี่ยงโดยตรง

4.8.5 การคำนวณคะแนนและตารางระดับความเสี่ยง (Risk Score and Risk Matrix)

มหาวิทยาลัยใช้คะแนนโอกาสเกิดและผลกระทบระดับ 1–5 คำนวณดังนี้

คะแนนความเสี่ยง (Risk Score) = โอกาสเกิด (Likelihood: L) × ผลกระทบ (Impact: I) ให้ใช้สูตรเดียวกันสำหรับความเสี่ยงโดยธรรมชาติ ความเสี่ยงคงเหลือ และความเสี่ยงคงเหลือเป้าหมาย โดยแยกสถานะ วันที่ประเมิน และสมมติฐานให้ชัดเจน

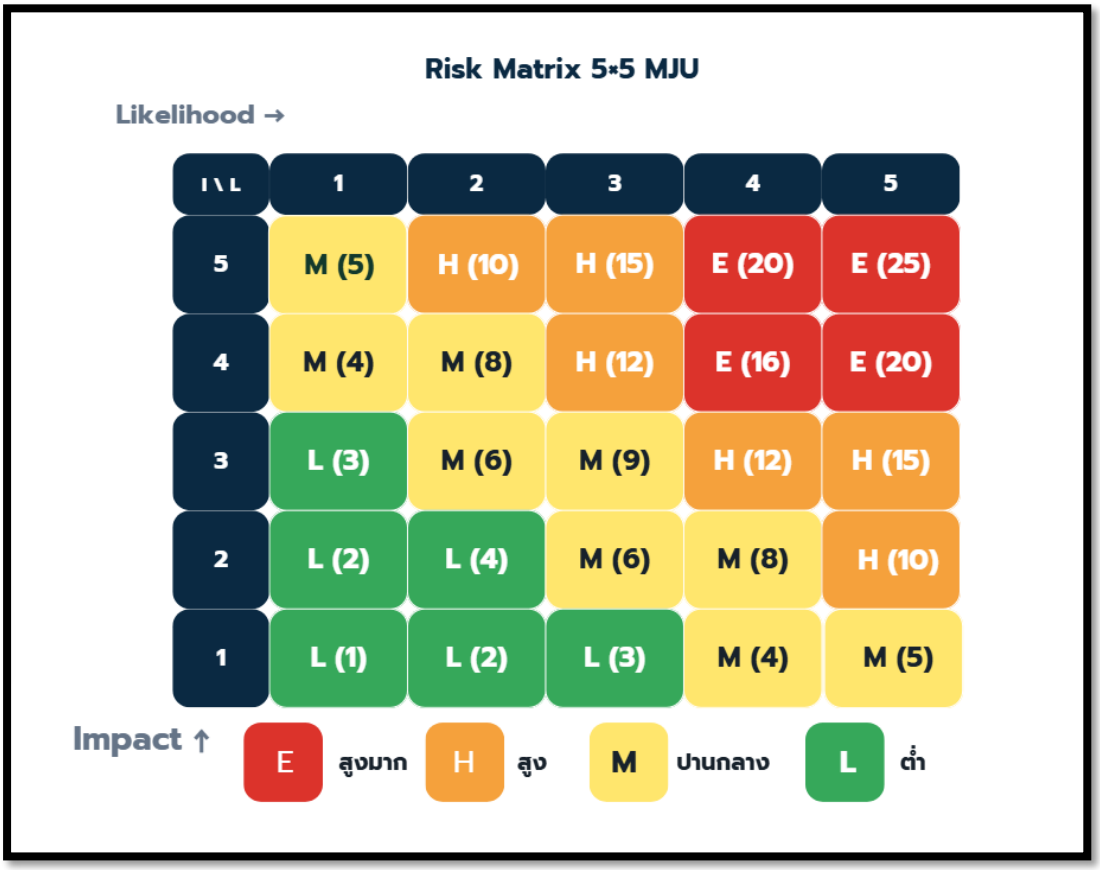
ตารางที่ 4-16 ***ตารางแสดงเกณฑ์ระดับความเสี่ยงและแนวทางดำเนินการ***

คะแนน	ระดับความเสี่ยง	รหัส	แนวทางดำเนินการขั้นต่ำ
1–4	ต่ำ (Low)	L	ยอมรับได้เมื่ออยู่ภายใน RA/RT และอำนาจที่ได้รับมอบหมาย พร้อมรักษาการควบคุมและติดตามตามรอบ
5–9	ปานกลาง (Medium)	M	พิจารณาความเพียงพอของการควบคุม กำหนดมาตรการตามความจำเป็น และติดตามโดยเจ้าของความเสี่ยง
10–15	สูง (High)	H	จัดทำแผนจัดการความเสี่ยง รายงานฝ่ายบริหาร และพิจารณาการยอมรับตามอำนาจและเงื่อนไข
16–25	สูงมาก (Extreme)	E	ยกระดับทันที เร่งดำเนินมาตรการ และติดตามอย่างใกล้ชิดตามข้อกำหนด

ภาพที่ 4-3

ภาพแสดงเกณฑ์ระดับความเสี่ยง การกตอบสนองและอำนาจการตัดสินใจ

ภาพที่ 4-3 ภาพแสดงตารางประเมินระดับความเสี่ยงแบบ 5 × 5



ตัวอย่าง 4 × 4 = 16 ต้องแสดงเป็นระดับสูงมาก (E) อย่างสอดคล้องกันในทะเบียนความเสี่ยง แบบฟอร์ม แผงสรุปข้อมูล และรายงาน ส่วนอำนาจยอมรับความเสี่ยงต้องพิจารณาตามข้อ 3.9 ไม่สรุปจากคะแนนเพียงอย่างเดียว

คะแนนเท่ากันอาจต้องตอบสนองต่างกัน เช่น 1 × 5 และ 5 × 1 มีคะแนน 5 เท่ากัน แต่กรณีผลกระทบระดับ 5 ต้องใช้เกณฑ์ Override ขณะที่เหตุการณ์ผลกระทบต่ำแต่เกิดซ้ำบ่อยต้องพิจารณาผลกระทบสะสมด้วย

เกณฑ์ยกระดับเป็นกรณีพิเศษและเงื่อนไขการยกระดับ (Override and Escalation Criteria) ให้ใช้คะแนนร่วมกับเกณฑ์ตามข้อ 2.13 ข้อ 3.6 และข้อ 3.10 ดังต่อไปนี้

1. ผลกระทบระดับ 5: ใช้แนวทางตอบสนองอย่างน้อยเทียบเท่าความเสี่ยงระดับสูง แม้คะแนนรวมต่ำกว่า 10 โดยคงคะแนนและระดับตามสูตรไว้

2. เหตุ Zero Tolerance: รายงานและตอบสนองเทียบเท่าความเสี่ยงระดับสูงมากทันที ไม่รอการคำนวณคะแนน และไม่จำเป็นต้องเปลี่ยนคะแนนเป็น 16–25 หากผลประเมินตามข้อเท็จจริงเป็นอย่างอื่น

3. KRI เกิน RT หรือการจัดการเกินอำนาจ: ดำเนินมาตรการและยกระดับตามเงื่อนไขที่กำหนด แม้คะแนนรวมยังไม่อยู่ในระดับสูง

4. ผลกระทบข้ามส่วนงานหรือเชิงยุทธศาสตร์: เสนอผู้มีอำนาจพิจารณาความจำเป็นในการจัดการระดับมหาวิทยาลัยและการบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัย (Enterprise Risk) โดยไม่ถือว่าเกิดขึ้นโดยอัตโนมัติ

5. สถานการณ์ที่ต้องพิจารณาเพิ่มเติม: ความเสี่ยงที่ส่งผลรวดเร็ว การควบคุมสำคัญไม่ทำงาน หรืออาจมีผลกระทบที่ฟื้นฟูไม่ได้ ต้องพิจารณาการตอบสนองที่เร่งด่วนขึ้น หากข้อมูลมีความไม่แน่นอนสูงและอาจมีผลกระทบรุนแรง ให้พิจารณามาตรการป้องกันและการยกระดับ พร้อมบันทึกข้อจำกัด

6. ข้อกำหนดเฉพาะ: หากกฎหมาย แผนฉุกเฉิน หรือนโยบายเฉพาะด้านกำหนดเกณฑ์หรือเวลาที่เข้มงวดกว่า ให้ปฏิบัติตามข้อกำหนดนั้น รวมถึงผู้รับรายงานและช่องทางที่กำหนด

การใช้ Override ต้องบันทึกเหตุผล หลักฐาน ผู้เสนอ ผู้พิจารณา วันที่ตัดสินใจ ระดับการตอบสนอง มาตรการ ผู้รับผิดชอบ และกำหนดทบทวนในทะเบียนความเสี่ยงหรือบันทึกการยกระดับ โดยแสดง **ระดับตามคะแนน** แยกจาก **ระดับการตอบสนองตามเกณฑ์พิเศษ**

4.8.6 ตัวอย่างการวิเคราะห์และประเมินความเสี่ยง (Illustrative Risk Analysis and Evaluation)

ตัวอย่างต่อไปนี้เป็นข้อมูลสมมติเพื่ออธิบายวิธีประเมิน ไม่ใช่ผลประเมินจริงหรือเกณฑ์ที่มหาวิทยาลัยอนุมัติ

ตารางที่ 4-10 ***ตัวอย่างการประเมินความเสี่ยงด้านยุทธศาสตร์เกี่ยวกับ AI และดิจิทัล***

รายการ	ตัวอย่างการประเมินและเหตุผล
เหตุการณ์ความเสี่ยง (Risk Event)	มหาวิทยาลัยอาจปรับขีดความสามารถและนำ AI มาใช้สนับสนุนงานสำคัญไม่ทันต่อแผนยุทธศาสตร์
กรอบเวลา (Time Horizon)	ปีงบประมาณ พ.ศ. 2570

รายการ	ตัวอย่างการประเมินและเหตุผล
โอกาสเกิดโดยธรรมชาติ (Inherent Likelihood)	**4** โดยสมมติว่าผลวิเคราะห์ช่องว่างสมรรถนะ ความพร้อมของข้อมูล และกำหนดการขับเคลื่อนงานชี้ว่ามีแนวโน้มไม่ทันแผน หากยังไม่พิจารณาผลของการควบคุม
ผลกระทบโดยธรรมชาติ (Inherent Impact)	**4** โดยสมมติว่าความล่าช้ากระทบผลลัพธ์เชิงยุทธศาสตร์สำคัญตามเกณฑ์ผลกระทบที่ใช้
ความเสี่ยงโดยธรรมชาติ (Inherent Risk)	**4 × 4 = 16 ระดับสูงมาก (E)**
การควบคุมที่มีอยู่ (Existing Controls)	การกำกับโครงการนำร่อง การพัฒนาสมรรถนะ และการสอบทานความพร้อมของระบบและข้อมูล โดยระบุเจ้าของ ขอบเขต ความถี่ และหลักฐาน
ผลประเมินการควบคุม (Control Effectiveness)	**มีประสิทธิผลบางส่วน** สมมติว่ามีหลักฐานว่าช่วยให้โครงการนำร่องดำเนินงานได้ดีขึ้น แต่ยังไม่ครอบคลุมทุกงานสำคัญ
โอกาสเกิดคงเหลือ (Residual Likelihood)	**3** โดยสมมติว่าผลทดสอบและข้อมูลความพร้อมสนับสนุนการลดโอกาสไม่ทันแผนจากระดับ 4 เป็น 3
ผลกระทบคงเหลือ (Residual Impact)	**4** เนื่องจากหากยังเกิดเหตุ ผลกระทบต่อเป้าหมายสำคัญยังไม่ลดลง และไม่มีหลักฐานรองรับการลดคะแนน
ความเสี่ยงคงเหลือ (Residual Risk)	**3 × 4 = 12 ระดับสูง (H)**
ความเสี่ยงคงเหลือเป้าหมายเบื้องต้น (Preliminary Target Residual Risk)	**2 × 3 = 6 ระดับปานกลาง (M)** ภายในสิ้นปีงบประมาณ พ.ศ. 2570 โดยต้องยืนยันร่วมกับแผนในขั้นตอนที่ 5 และมีมาตรการที่รองรับทั้งการลดโอกาสเกิดและผลกระทบ
สถานะเทียบ RA/RT (RA/RT Status)	เปรียบเทียบกับกรอบที่อนุมัติและผล KRI ณ วันที่ประเมิน พร้อมพิจารณาข้อจำกัดและสถานการณ์อื่น ไม่สรุปจากคะแนน 12 หรือ KRI ตัวเดียว
ลำดับความสำคัญ (Priority)	ต้องจัดทำแผนและรายงานฝ่ายบริหาร เพราะความเสี่ยงคงเหลืออยู่ในระดับสูงและเกี่ยวข้องกับเป้าหมายเชิงยุทธศาสตร์
ประเด็นยกระดับ (Escalation Issues)	ต้องใช้การตัดสินใจและทรัพยากรระดับมหาวิทยาลัย รวมถึงยกระดับเมื่อ KRI เกิน RT หรือมาตรการสำคัญล่าช้าตามเกณฑ์

หากหลักฐานไม่รองรับการลดโอกาสเกิดจาก 4 เป็น 3 ต้องทบทวนผลประเมินความเสี่ยงคงเหลือ ไม่ใช้ค่าตามตัวอย่างโดยอัตโนมัติ เช่นเดียวกัน หากมาตรการเพิ่มเติมลดได้เฉพาะโอกาสเกิด แต่ไม่ลดผลกระทบ ต้องปรับความเสี่ยงคงเหลือเป้าหมายให้สอดคล้องกับผลที่คาดว่าจะเกิดจริง

4.8.7 ผลผลิตขั้นต่ำของขั้นตอนที่ 4 (Minimum Outputs of Step 4)

เมื่อสิ้นสุดขั้นตอนนี้ ต้องมีข้อมูลและหลักฐานอย่างน้อยดังต่อไปนี้

1. ผลประเมินความเสี่ยงโดยธรรมชาติ (Inherent Risk Assessment): คะแนนโอกาสเกิด ผลกระทบ ระดับความเสี่ยง และเหตุผล

2. ผลประเมินการควบคุม (Control Assessment): ผลด้านการออกแบบ การนำไปใช้ และประสิทธิผล พร้อมเจ้าของการควบคุม หลักฐาน และช่องว่าง

3. ผลประเมินความเสี่ยงคงเหลือ (Residual Risk Assessment): คะแนน ระดับ วันที่ประเมิน และเหตุผลที่เชื่อมโยงกับผลของการควบคุม

4. ผลเปรียบเทียบกับ RA/RT (RA/RT Comparison): สถานะตามกรอบและตัวชี้วัดที่เกี่ยวข้อง พร้อมข้อจำกัดในการตีความ

5. ลำดับความสำคัญและข้อเสนอการจัดการ (Priorities and Management Recommendations)

6. เกณฑ์พิเศษและระดับการตอบสนอง (Override Criteria and Response Level)

7. รายการที่ต้องยกระดับ (Escalation Items): เหตุผล ผู้รับรายงาน และเวลาที่ต้องดำเนินการ

8. ข้อมูล หลักฐาน สมมติฐาน และข้อจำกัด (Data, Evidence, Assumptions and Limitations)

9. ระดับความเสี่ยงคงเหลือเป้าหมายเบื้องต้น หากจัดทำแล้ว (Preliminary Target Residual Risk): ระบุสมมติฐานและนำไปยืนยันกับมาตรการ ทรัพยากร และกำหนดเวลาในขั้นตอนที่ 5

ให้ปรับปรุงข้อมูลในทะเบียนความเสี่ยงหรือแบบ RISK-MJU-01 และนำผลการประเมินไปใช้เลือกแนวทางตอบสนองและจัดทำแผนบริหารความเสี่ยง โดยเหตุเร่งด่วนต้องรายงานและดำเนินมาตรการทันที ไม่รอการจัดทำแผนให้แล้วเสร็จ

4.9 ขั้นตอนที่ 5 การตอบสนองและจัดทำแผนบริหารความเสี่ยง (Risk Response and Treatment Planning)

การตอบสนองและจัดทำแผนบริหารความเสี่ยงเป็นการนำผลการวิเคราะห์และประเมินจากขั้นตอนที่ 4 มาเลือกแนวทางจัดการที่เหมาะสม พร้อมกำหนดมาตรการ ผู้รับผิดชอบ ทรัพยากร ระยะเวลา และวิธีติดตามผล เพื่อให้ความเสี่ยงสอดคล้องกับกรอบการยอมรับและสนับสนุนการบรรลุวัตถุประสงค์

มาตรการต้องตอบสนองต่อสาเหตุ เหตุการณ์ หรือผลกระทบที่ระบุไว้ โดยแสดงให้เห็นว่าจะช่วยลดโอกาสเกิด ลดผลกระทบ หรือเพิ่มความพร้อมในการตรวจพบ ตอบสนอง และฟื้นตัวอย่างไร การดำเนินกิจกรรมแล้วเสร็จเพียงอย่างเดียวไม่ถือเป็นหลักฐานว่าความเสี่ยงลดลง

4.9.1 ทางเลือกการตอบสนองต่อความเสี่ยง (Risk Response Options)

ตารางที่ 4-11 ***ตารางแสดงทางเลือกการตอบสนองต่อความเสี่ยง***

ทางเลือก	ความหมาย	ตัวอย่างการใช้
หลีกเลี่ยง (Avoid)	ไม่เริ่ม ยุติ หรือเปลี่ยนกิจกรรมที่เป็นแหล่งความเสี่ยง โดยพิจารณาผลกระทบจากการหยุดหรือเปลี่ยนกิจกรรมด้วย	ไม่ดำเนินโครงการที่ขัดต่อกฎหมาย หรือปรับรูปแบบโครงการที่มีความเสี่ยงเกินขีดความสามารถในการรองรับ
ลดหรือควบคุม (Reduce)	ลดโอกาสเกิดหรือผลกระทบผ่านการป้องกัน ตรวจพบ ตอบสนอง และฟื้นตัว	ปรับกระบวนงาน แบ่งแยกหน้าที่ ตรวจสอบสิทธิ สำรองและทดสอบกู้คืนระบบ หรือพัฒนาสมรรถนะ
แบ่งปันหรือถ่ายโอน (Share/Transfer)	แบ่งภาระหรือถ่ายโอนผลกระทบบางส่วนตามข้อตกลง โดยมหาวิทยาลัยยังต้องกำกับความเสี่ยงคงเหลือและรับผิดชอบหน้าที่ที่กฎหมายกำหนด	ประกันภัย ความร่วมมือ หรือการจ้างผู้ให้บริการภายนอก พร้อมข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) และการติดตามผู้ให้บริการ
ยอมรับ (Accept)	คงความเสี่ยงไว้โดยผู้มีอำนาจพิจารณาเหตุผลและเงื่อนไข พร้อมติดตามตามกรอบที่กำหนด	ไม่เพิ่มมาตรการเมื่อความเสี่ยงอยู่ภายใน RA/RT การควบคุมเพียงพอ และประโยชน์จากมาตรการเพิ่มเติมไม่คุ้มกับต้นทุน ทั้งนี้การคงความเสี่ยงที่เกินกรอบไว้ชั่วคราวต้องเป็นไปตามข้อ 3.8

ทางเลือก	ความหมาย	ตัวอย่างการใช้
ใช้ประโยชน์หรือเพิ่มโอกาส (Pursue/Enhance)	เลือกดำเนินการเพื่อเพิ่มโอกาสบรรลุผลลัพธ์ที่ดีขึ้น โดยประเมินและจัดการความเสี่ยงที่เกี่ยวข้องภายในข้อจำกัดที่อนุมัติ	ทดลองนวัตกรรมในโครงการนำร่อง (Pilot) หรือสภาพแวดล้อมทดลองที่ควบคุมขอบเขต (Sandbox) พร้อมขอบเขตควบคุม (Guardrails) เกณฑ์หยุด (Stop Criteria) และการประเมินก่อนขยายผล

การแบ่งปันหรือถ่ายโอนไม่ทำให้ความรับผิดชอบทั้งหมดสิ้นสุดลง ต้องประเมินข้อยกเว้นของประกันภัย ความสามารถของคู่สัญญา ความเสี่ยงจากการพึ่งพา และความเสี่ยงที่ยังคงอยู่ด้วย

ข้อพิจารณาในการเลือกแนวทาง (Response Selection Considerations) ให้พิจารณาอย่างน้อยดังต่อไปนี้

1. กรอบการยอมรับและขีดความสามารถ (RA/RT and Risk Capacity)
2. กฎหมาย ข้อกำหนด และเหตุที่ไม่ยอมรับ (Legal Requirements and Zero Tolerance)
3. ผลต่อวัตถุประสงค์และผู้มีส่วนได้ส่วนเสีย (Effects on Objectives and Stakeholders)
4. ต้นทุน ประโยชน์ และผลจากการไม่ดำเนินการ (Costs, Benefits and Consequences of Inaction)
5. ความเป็นไปได้และเวลาที่ต้องใช้ (Feasibility and Lead Time)
6. ทรัพยากร อำนาจ และสมรรถนะผู้รับผิดชอบ (Resources, Authority and Capability)
7. ความเสี่ยงใหม่ ผลข้างเคียง และการพึ่งพาที่เพิ่มขึ้น (New Risks, Side Effects and Dependencies)
8. ความเสี่ยงคงเหลือที่คาดการณ์และข้อจำกัดของข้อมูล (Expected Residual Risk and Information Limitations)

อาจใช้หลายทางเลือกร่วมกัน หากแนวทางเดียวไม่เพียงพอ ต้องบันทึกเหตุผลในการเลือกและทางเลือกสำคัญที่ไม่ได้เลือก โดยการเปรียบเทียบต้นทุนและประโยชน์ไม่เป็นเหตุให้ละเว้นหน้าที่ตามกฎหมายหรือข้อห้าม

4.9.2 องค์ประกอบของแผนบริหารความเสี่ยง (Risk Treatment Plan Components) แผนบริหารความเสี่ยงต้องระบุอย่างน้อยดังต่อไปนี้

1. ข้อมูลความเสี่ยงและวัตถุประสงค์ (Risk and Objective Information): รหัส ความเสี่ยง วัตถุประสงค์ สาเหตุ และปัจจัยที่มาตรการต้องตอบสนอง

2. ผลประเมินปัจจุบันและเป้าหมาย (Current Assessment and Target): ความเสี่ยงคงเหลือ ณ วันที่ประเมิน และความเสี่ยงคงเหลือเป้าหมาย พร้อมสมมติฐาน

3. แนวทางตอบสนองและเหตุผล (Response and Rationale)

4. มาตรการ กิจกรรม และผลส่งมอบ (Actions, Activities and Deliverables): ระบุผลที่ตรวจสอบได้และองค์ประกอบความเสี่ยงที่คาดว่าจะลดลง

5. เจ้าของมาตรการและการควบคุม (Action Owner and Control Owner): กำหนดผู้รับผิดชอบหลักหนึ่งรายหรือหนึ่งบทบาทต่อมาตรการ พร้อมหน่วยงานร่วม

6. กำหนดเวลาและจุดตรวจสอบความก้าวหน้า (Timeline and Milestones): วันที่เริ่มต้น วันแล้วเสร็จ และงานที่ต้องเสร็จก่อนดำเนินงานอื่น

7. ทรัพยากร งบประมาณ และสถานะการอนุมัติ (Resources, Budget and Approval Status)

8. ตัวชี้วัดที่เหมาะสม (Relevant Indicators): KPI ของผลการดำเนินมาตรการ KCI ของการควบคุมตามความจำเป็น และ KRI ของความเสี่ยง โดยไม่ต้องเพิ่มตัวชี้วัดทุกประเภทหากไม่ช่วยตัดสินใจ

9. รายละเอียดข้อมูล (Data Specifications): นิยาม สูตร หน่วยวัด แหล่งข้อมูล ความถี่ และเจ้าของข้อมูล

10. หลักฐานและเกณฑ์ยืนยันผล (Evidence and Verification Criteria)

11. ความเสี่ยงจากมาตรการและการจัดการ (Treatment-induced Risks and Responses)

12. มาตรการระหว่างรอหรือแผนสำรอง (Interim Controls and Contingency Plan)

13. จุดแจ้งเตือนและมาตรการแก้ไข (Triggers and Corrective Actions): เงื่อนไขเมื่อมาตรการล่าช้าหรือไม่เกิดผล พร้อมผู้รับผิดชอบและเวลาตอบสนอง

14. รอบติดตามและเกณฑ์ยกระดับ (Monitoring Schedule and Escalation Criteria)

15. ผู้พิจารณา ผู้อนุมัติ และเงื่อนไข (Reviewers, Approvers and Conditions)

ความเสี่ยงคงเหลือระดับสูงและสูงมากต้องมีแผนเป็นลายลักษณ์อักษร ส่วนความเสี่ยงระดับอื่นให้จัดทำตามสถานะ RA/RT เกณฑ์ Override และความจำเป็นในการปรับปรุง

การอนุมัติแผนไม่ถือเป็นการอนุมัติยอมรับความเสี่ยงโดยอัตโนมัติ หากจำเป็นต้องคงความเสี่ยงไว้ต้องเสนอผู้มีอำนาจตามข้อ 3.8 พร้อมเหตุผล เงื่อนไข ระยะเวลา และวันที่ทบทวน โดยกรณีระดับสูงหรือสูงมากต้องมีวันสิ้นสุดการยอมรับและไม่ต่ออายุโดยอัตโนมัติ

เหตุ Zero Tolerance ไม่อยู่ในอำนาจอนุมัติให้กระทำหรือเพิกเฉยต่อเหตุ ต้องระงับหรือจำกัดความเสียหาย รายงาน รักษาหลักฐาน ตรวจสอบข้อเท็จจริง และดำเนินการตามกฎหมายหรือนโยบายที่เกี่ยวข้องโดยไม่ชักช้า

4.9.3 ตัวอย่างแผนบริหารความเสี่ยงแบบย่อ (Illustrative Risk Treatment Plan)

ตัวอย่างนี้เป็นข้อมูลสมมติเพื่ออธิบายวิธีจัดทำแผน ไม่ใช่ผลประเมินจริง เกณฑ์ หรือการมอบหมายที่มหาวิทยาลัยอนุมัติแล้ว

ความเสี่ยงตัวอย่าง EX-S-01: มหาวิทยาลัยอาจปรับขีดความสามารถและใช้ AI กับเทคโนโลยีดิจิทัลสนับสนุนงานสำคัญไม่ทันต่อแผนยุทธศาสตร์

ตารางที่ 4-12 ข้อมูลสรุปแผนบริหารความเสี่ยงตัวอย่าง

รายการ	ตัวอย่าง
ความเสี่ยงคงเหลือปัจจุบัน (Residual Risk)	โอกาสเกิด 3 × ผลกระทบ 4 = **12 ระดับสูง (H)** โดยมีหลักฐานรองรับผลการควบคุม ณ วันที่ประเมิน
ความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk)	โอกาสเกิด 2 × ผลกระทบ 3 = **6 ระดับปานกลาง (M)** ภายในสิ้นปีงบประมาณ พ.ศ. 2570 โดยต้องทดสอบว่ามาตรการช่วยลดทั้งโอกาสเกิดและผลกระทบได้
แนวทางตอบสนอง (Response)	ลดความเสี่ยงควบคู่กับใช้ประโยชน์จากโอกาส
การติดตาม (Monitoring)	ติดตามความพร้อม การปฏิบัติตามกรอบกำกับดูแล ผลการใช้ AI และระดับความเสี่ยงร่วมกัน ไม่สรุปผลจากจำนวนผู้เข้าอบรมหรือ KRI ตัวเดียว
ผู้อนุมัติ (Approver)	ผู้มีอำนาจอนุมัติแผนและทรัพยากรตามการมอบอำนาจ ส่วนการยอมรับความเสี่ยงให้พิจารณาแยกตามข้อ 3.9

ตารางที่ 4-13 ***มาตรการและหลักฐานในแผนตัวอย่าง***

มาตรการ	ผู้รับผิดชอบและจุดตรวจสอบ	ผลส่งมอบและหลักฐาน	ผลต่อความเสี่ยงที่คาดหวัง
1. จัดทำกรอบการกำกับดูแลปัญญาประดิษฐ์ (AI Governance Framework) ครอบคลุมบทบาท ข้อมูล จริยธรรม ความปลอดภัย และการประเมินกรณีใช้งาน	เจ้าของมาตรการด้านกำกับดูแลที่ได้รับมอบหมาย ประสานหน่วยงานยุทธศาสตร์ ดิจิทัล และกฎหมาย **จุดตรวจสอบ:** ร่างกรอบ ⟶ รับฟังความคิดเห็น ⟶ ทดลองใช้ ⟶ อนุมัติ	กรอบและแนวปฏิบัติที่อนุมัติ แบบประเมินความเสี่ยง บันทึกการพิจารณา และหลักฐานการนำไปใช้	ลดโอกาสดำเนินงานไม่สอดคล้องกับทิศทางหรือข้อกำหนด
2. พัฒนาสมรรถนะ AI และดิจิทัลตามบทบาท เชื่อมโยงกับแผนพัฒนารายบุคคล (Individual Development Plan: IDP)	เจ้าของมาตรการด้านบุคลากร **จุดตรวจสอบ:** กำหนดสมรรถนะ ⟶ ประเมินช่องว่าง ⟶ พัฒนา ⟶ ทดสอบการปฏิบัติ	เกณฑ์สมรรถนะ แผนพัฒนา ผลทดสอบ และหลักฐานการนำไปใช้ในงาน	ลดโอกาสใช้เทคโนโลยีไม่ถูกต้องหรือไม่ทันต่อแผน
3. ทดลองกรณีใช้งาน AI (AI Use Cases) ในขอบเขตควบคุม พร้อมการตรวจสอบโดยบุคลากรและเกณฑ์หยุด	เจ้าของโครงการนำร่องแต่ละโครงการ **จุดตรวจสอบ:** ประเมินก่อนเริ่ม ⟶ ทดลอง ⟶ ตรวจผล ⟶ พิจารณาขยายผล	ผลประเมินความเสี่ยง ผลทดสอบความถูกต้อง ประโยชน์และต้นทุน เหตุการณ์ที่พบ และบันทึกการตัดสินใจ	เพิ่มโอกาสสร้างคุณค่าและลดโอกาสขยายระบบที่ยังไม่พร้อม
4. จัดทางเลือกสำรองและจำกัดผลกระทบ เช่น ใช้กระบวนงานเดิม การตรวจทานผลลัพธ์ และการย้อนกลับเมื่อระบบผิดพลาด	เจ้าของกระบวนงานร่วมกับเจ้าของการควบคุม **จุดตรวจสอบ:** ออกแบบ ⟶ ทดสอบ ⟶ แก้ไข ⟶ ยืนยันความพร้อม	ผลทดสอบทางเลือกสำรอง ความสามารถรักษาบริการ และเวลาที่ใช้กลับสู่กระบวนงานปลอดภัย	รองรับการลดผลกระทบจากระดับ 4 เป็น 3 หากผลทดสอบยืนยันตามเกณฑ์

หากไม่มีหลักฐานว่ามาตรการช่วยลดผลกระทบได้ ต้องคงหรือทบทวนคะแนนผลกระทบเป้าหมาย ไม่ลดจาก 4 เป็น 3 เพียงเพื่อให้ได้คะแนนรวมตามต้องการ

ตัวอย่างตัวชี้วัดและเงื่อนไขตอบสนอง (Indicators and Response Conditions)

- **ตัวชี้วัดความเสี่ยง (KRI):** ร้อยละบุคลากรกลุ่มเป้าหมายในงานสำคัญที่ผ่านเกณฑ์สมรรถนะ AI และดิจิทัล โดยวัดจากการทดสอบหรือประเมินการปฏิบัติ
- **สูตรคำนวณ (Formula):** จำนวนบุคลากรกลุ่มเป้าหมายที่ผ่านเกณฑ์ ÷ จำนวนบุคลากรกลุ่มเป้าหมายทั้งหมด × 100
- **เกณฑ์ปฏิบัติที่เชื่อมโยงกับ RA:** ตั้งแต่ร้อยละ 80 ขึ้นไป ณ จุดตรวจสอบที่กำหนด
- **ช่วงเฝ้าระวัง (Warning Band):** ตั้งแต่ร้อยละ 70 แต่ต่ำกว่าร้อยละ 80 ให้เร่งพัฒนาและติดตามใกล้ชิด
- **ขอบเขต RT:** ไม่ต่ำกว่าร้อยละ 70 ณ จุดตรวจสอบที่กำหนด หากต่ำกว่านี้ให้ดำเนินแผนแก้ไขและยกระดับ
- **เจ้าของข้อมูล (Data Owner):** ผู้รับผิดชอบข้อมูลสมรรถนะที่ได้รับมอบหมาย
- **หลักฐานผลการควบคุม:** ผลสอบทานว่ากรณีใช้งานผ่านการประเมินและปฏิบัติตามเงื่อนไขที่อนุมัติ
- **หลักฐานผลลัพธ์:** คุณภาพงาน ระยะเวลาบริการ หรือผลประโยชน์ที่เกิดขึ้นจริงจากโครงการนำร่อง

เกณฑ์ดังกล่าวต้องกำหนดวันหรือรอบตรวจสอบให้ชัดเจน และไม่ใช้เป็นข้อสรุปว่าความเสี่ยงทั้งรายการอยู่ภายใน RA/RT เพราะยังมีปัจจัยด้านการกำกับดูแล ข้อมูล และระบบที่ต้องติดตามร่วมกัน

จุดแจ้งเตือนและมาตรการแก้ไข (Triggers and Corrective Actions)

1. จุดตรวจสอบล่าช้า: ตัวอย่างเช่น ล่าช้าเกิน 30 วันจากแผนที่อนุมัติ ให้ประเมินผลต่อเป้าหมายและเสนอปรับทรัพยากรหรือแผน ทั้งนี้ หากผลกระทบเกิดก่อนครบ 30 วัน ต้องดำเนินการก่อน ไม่รอให้ถึงเกณฑ์ตัวอย่าง

2. KRI เกิน RT หรือคาดว่าจะเกิน: วิเคราะห์สาเหตุ จัดทำมาตรการแก้ไข ระบุผู้รับผิดชอบและกำหนดเวลา พร้อมยกระดับตามข้อ 3.6 และข้อ 3.10

3. ผลทดสอบไม่ผ่าน: ชะลอการขยายผล ปรับปรุงมาตรการ และทดสอบซ้ำก่อนเสนออนุมัติ

4. พบเหตุสำคัญด้านกฎหมาย ข้อมูล หรือความปลอดภัย: ใช้แผนเผชิญเหตุและข้อกำหนดเฉพาะทันที ไม่รอรอบติดตามแผน หากเข้าเกณฑ์ Zero Tolerance ให้ดำเนินการตามเส้นทางที่กำหนด

การปรับแผน ทรัพยากร หรือเป้าหมายต้องได้รับอนุมัติตามอำนาจ พร้อมบันทึกเหตุผล ผลกระทบ และฉบับที่เปลี่ยนแปลงในบันทึกการตัดสินใจ (Decision Log)

4.9.4 ผลผลิตขั้นต่ำของขั้นตอนที่ 5 (Minimum Outputs of Step 5) เมื่อสิ้นสุดขั้นตอนนี้ ต้องมีข้อมูลและหลักฐานอย่างน้อยดังต่อไปนี้

1. ผลการเลือกแนวทางตอบสนองและเหตุผล (Risk Response Decision and Rationale)
2. แผนบริหารความเสี่ยงที่ผ่านการพิจารณาตามอำนาจ (Reviewed Risk Treatment Plan)
3. เจ้าของมาตรการ เจ้าของการควบคุม และหน่วยงานร่วม (Action Owners, Control Owners and Supporting Units)
4. ทรัพยากร งบประมาณ และสถานะการอนุมัติ (Resources, Budget and Approval Status)
5. จุดตรวจสอบและกำหนดแล้วเสร็จ (Milestones and Completion Dates)
6. ตัวชี้วัด เกณฑ์ติดตาม และเจ้าของข้อมูล (Indicators, Monitoring Criteria and Data Owners)
7. ความเสี่ยงคงเหลือเป้าหมายพร้อมสมมติฐานและวิธียืนยันผล (Target Residual Risk, Assumptions and Verification Method)
8. หลักฐานและผลส่งมอบที่ต้องจัดทำ (Required Evidence and Deliverables)
9. จุดแจ้งเตือน มาตรการแก้ไข และเกณฑ์ยกระดับ (Triggers, Corrective Actions and Escalation Criteria)
10. หลักฐานการอนุมัติแผนและเงื่อนไข (Plan Approval and Conditions)
11. บันทึกการยอมรับความเสี่ยง หากเกี่ยวข้อง (Risk Acceptance Record)

หากทรัพยากรยังไม่ได้รับอนุมัติ ให้ระบุสถานะ ผู้รับผิดชอบ และกำหนดเวลาเสนอพิจารณา พร้อมมาตรการระหว่างรอ ไม่ถือว่าแผนพร้อมดำเนินการครบถ้วน และไม่ใช้แผนดังกล่าวเป็นเหตุลดความเสี่ยงคงเหลือปัจจุบัน

4.10 ขั้นตอนที่ 6 การดำเนินการควบคุมและมาตรการ (Implementation of Controls and Risk Treatment Actions)

การดำเนินการควบคุมและมาตรการเป็นการนำแผนบริหารความเสี่ยงที่ผ่านการพิจารณาตามอำนาจไปปฏิบัติ พร้อมรักษาการควบคุมที่มีอยู่ ทดสอบผล และแก้ไขข้อบกพร่อง เพื่อให้มาตรการเกิดผลต่อความเสี่ยงและสนับสนุนการบรรลุวัตถุประสงค์

เจ้าของความเสี่ยง (Risk Owner) รับผิดชอบกำกับภาพรวมและติดตามผล **เจ้าของการควบคุม (Control Owner)** รับผิดชอบให้การควบคุมทำงานตามที่กำหนด และ **เจ้าของมาตรการ (Action Owner)** รับผิดชอบดำเนินมาตรการเพิ่มเติมให้ได้ผลส่งมอบตามแผน โดยต้องจัดเก็บหลักฐานที่ตรวจสอบย้อนกลับได้

เมื่อมาตรการเพิ่มเติมพัฒนาเป็นการควบคุมประจำ ต้องส่งมอบวิธีปฏิบัติ ทรัพยากร และความรับผิดชอบให้เจ้าของการควบคุมอย่างชัดเจน เพื่อให้การควบคุมดำเนินต่อเนื่องหลังสิ้นสุดโครงการ

4.10.1 ประเภทการควบคุมตามวัตถุประสงค์ (Control Types by Purpose)

1. การควบคุมเชิงป้องกัน (Preventive Control): ป้องกันหรือลดโอกาสเกิดเหตุ เช่น การแบ่งแยกหน้าที่ การอนุมัติตามอำนาจ การกำหนดสิทธิ์เข้าถึงระบบ การตรวจสอบคุณสมบัติ และการแก้ไขช่องโหว่ก่อนถูกใช้โจมตี

2. การควบคุมเชิงตรวจจับ (Detective Control): ตรวจพบข้อผิดพลาด เหตุผิดปกติ หรือการไม่ปฏิบัติตามข้อกำหนด เช่น การกระทบยอดบัญชี รายงานข้อยกเว้น การตรวจสอบบันทึกระบบ การตรวจนับทรัพย์สิน และการติดตามสัญญาณเตือนไซเบอร์

3. การควบคุมเชิงแก้ไขและฟื้นฟู (Corrective and Recovery Control): จำกัดความเสียหาย แก้ไขข้อบกพร่อง และฟื้นคืนการดำเนินงาน เช่น การระงับบัญชีที่ถูกยึดครอง การกู้คืนข้อมูล การใช้แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan: DRP) และการแก้ไขสาเหตุเพื่อป้องกันการเกิดซ้ำ

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

การควบคุมหนึ่งรายการอาจมีหลายหน้าที่ ให้จำแนกตามวัตถุประสงค์หลักและระบุหน้าที่ที่เกี่ยวข้องเพิ่มเติมได้ เช่น การสำรองข้อมูลเป็นการเตรียมความพร้อมเพื่อลดผลกระทบและสนับสนุน

การกู้คืน ไม่ได้ป้องกันการโจมตีหรือการสูญหายของข้อมูลต้นทางโดยตรง จึงต้องพิจารณาร่วมกับการป้องกันและการทดสอบกู้คืน

4.10.2 รายละเอียดที่ต้องกำหนดสำหรับการควบคุม (Control Specifications) การควบคุมแต่ละรายการต้องระบุอย่างน้อยดังต่อไปนี้

1. วัตถุประสงค์ของการควบคุม (Control Objective)
2. ความเสี่ยง สาเหตุ หรือผลกระทบที่ต้องจัดการ (Related Risk, Cause or Impact)
3. เจ้าของการควบคุมและผู้ปฏิบัติ (Control Owner and Operator)
4. ขอบเขต วิธีดำเนินการ และความถี่ (Scope, Procedure and Frequency)
5. หลักฐานที่ต้องจัดเก็บ (Required Evidence)
6. เกณฑ์ผ่าน–ไม่ผ่านและการจัดการข้อยกเว้น (Pass/Fail Criteria and Exception Handling)
7. วิธีทดสอบ ช่วงเวลาที่ทดสอบ และผู้ประเมิน (Testing Method, Period and Assessor)
8. ผู้รับผิดชอบและกำหนดเวลาแก้ไขข้อบกพร่อง (Corrective Action Owner and Due Date)
9. เงื่อนไขและเส้นทางรายงานเมื่อการควบคุมไม่ทำงาน (Failure Triggers and Reporting Routes)

การมีนโยบาย ระเบียบ คู่มือ หรือคำสั่งเพียงอย่างเดียวไม่เพียงพอที่จะยืนยันประสิทธิผล ต้องมีหลักฐานว่าการควบคุมถูกนำไปใช้ ครอบคลุมขอบเขต ปฏิบัติสม่ำเสมอ และทำงานตามวัตถุประสงค์ โดยประเมินตามข้อ 4.8.4

4.10.3 การดำเนินมาตรการและติดตามผล (Action Implementation and Follow-up) เจ้าของมาตรการต้องดำเนินงานตามแผน บันทึกผลส่งมอบและปัญหา พร้อมแจ้งเจ้าของความเสี่ยงเมื่อมีความล่าช้าหรือผลไม่เป็นไปตามคาด การเปลี่ยนขอบเขต งบประมาณ กำหนดเวลา หรือผู้รับผิดชอบต้องได้รับความเห็นชอบตามอำนาจและเก็บประวัติการเปลี่ยนแปลง ให้ติดตามแยกกันระหว่าง

- **ความก้าวหน้าของมาตรการ (Action Progress):** งานหรือผลส่งมอบดำเนินการถึงขั้นใด
- **ผลของการควบคุม (Control Performance):** การควบคุมทำงานตามเกณฑ์หรือไม่

- **ผลต่อความเสี่ยง (Risk Outcome):** โอกาสเกิด ผลกระทบ และแนวโน้มความเสี่ยงเปลี่ยนแปลงอย่างไร

ตัวอย่างเช่น การติดตั้งระบบสำรองเสร็จแล้วแสดงความก้าวหน้าของงาน แต่ต้องทดสอบกู้คืนและตรวจสอบความถูกต้องของข้อมูลก่อนสรุปว่าช่วยลดผลกระทบจากการหยุดชะงักได้

4.10.4 ตัวอย่างการควบคุมด้านไซเบอร์และข้อมูลส่วนบุคคล (Cybersecurity and Personal Data Protection Controls)

ตารางที่ 4-14 ***ตัวอย่างการควบคุม เจ้าของ หลักฐาน และเกณฑ์ยืนยันผล***

เกณฑ์และบทบาทในตารางเป็นตัวอย่าง ต้องกำหนดให้เหมาะสมและได้รับความเห็นชอบตามอำนาจก่อนใช้ ไม่ถือเป็นเกณฑ์หรือโครงสร้างที่มหาวิทยาลัยอนุมัติแล้ว

ประเภท	ตัวอย่างการควบคุม	เจ้าของการควบคุม	ความถี่และหลักฐาน	เกณฑ์ยืนยันผล
เชิงป้องกัน (Preventive)	ติดตั้งชุดปรับปรุงความมั่นคงปลอดภัย (Security Patch) ตามระดับความรุนแรงและความสำคัญของระบบ	ผู้รับผิดชอบระบบที่ได้รับมอบหมาย	ตามกำหนดแก้ไขช่องโหว่ และสรุปรายเดือน; รายการระบบ รายงานติดตั้ง และผลตรวจสอบช่องโหว่	ตัวอย่าง: ระบบที่ถึงกำหนดได้รับการปรับปรุงไม่น้อยกว่าร้อยละ 95 โดยช่องโหว่วิกฤตที่ยังค้างต้องพิจารณาแยกและมีมาตรการระหว่างรอ
เชิงป้องกัน (Preventive)	จำกัดสิทธิ์เข้าถึงข้อมูลส่วนบุคคลตามความจำเป็น และทบทวนเมื่อเปลี่ยนหน้าที่หรือพ้นสภาพ	เจ้าของระบบและผู้รับผิดชอบอนุมัติสิทธิ์ตามบทบาท	เมื่อเปลี่ยนแปลงและตามรอบที่กำหนด; คำขอสิทธิ์ รายการบัญชี และผลทบทวน	สิทธิ์ตรงกับหน้าที่ บัญชีที่ไม่จำเป็นถูกยกเลิกภายในเวลาที่กำหนด และข้อยกเว้นได้รับการจัดการ
เชิงตรวจจับ (Detective)	ตรวจสอบสัญญาณเตือนจากอุปกรณ์ป้องกันเครือข่ายและระบบรวบรวมวิเคราะห์เหตุการณ์	ผู้รับผิดชอบเฝ้าระวังที่ได้รับมอบหมาย	ต่อเนื่องหรือตามความสำคัญของระบบ; บันทึกสัญญาณเตือนและรายการติดตามเหตุ	สัญญาณเตือนรุนแรงได้รับการคัดกรอง ตรวจสอบ และยกระดับภายในเวลาที่กำหนด พร้อมบันทึกผล

ประเภท	ตัวอย่างการควบคุม	เจ้าของการควบคุม	ความถี่และหลักฐาน	เกณฑ์ยืนยันผล
	ความปลอดภัย (Firewall/SIEM)			
เชิงแก้ไขและฟื้นฟู (Corrective and Recovery)	จำกัดการเข้าถึงที่ผิดปกติ ระงับบัญชีที่ถูกยึดครอง และกู้คืนระบบจากข้อมูลสำรองที่ตรวจสอบแล้ว	ทีมตอบสนองเหตุและผู้รับผิดชอบกู้คืนระบบตามแผน	เมื่อเกิดเหตุและเมื่อทดสอบแผน; รายงานเหตุ ผลกู้คืน และบันทึกเวลา	จำกัดเหตุภายในเวลาตอบสนองที่กำหนด แยกต่างหาก และฟื้นคืนบริการตามเป้าหมายระยะเวลากู้คืน (RTO) พร้อมตรวจสอบข้อมูลตามเป้าหมายจุดกู้คืน (RPO)
เชิงแก้ไขและป้องกันการเกิดซ้ำ (Corrective and Preventive)	วิเคราะห์สาเหตุรากและดำเนินแผนแก้ไขและป้องกัน (CAPA)	เจ้าของความเสี่ยงและเจ้าของมาตรการที่เกี่ยวข้อง	หลังเหตุหรือข้อบกพร่อง; ผลวิเคราะห์สาเหตุ แผนแก้ไข และหลักฐานทดสอบซ้ำ	มาตรการตอบสนองสาเหตุสำคัญและมีผลตรวจสอบยืนยัน ไม่ปิดงานจากการส่งเอกสารเพียงอย่างเดียว
เชิงกำกับหรือชี้นำ (Directive)	สื่อสารแนวปฏิบัติด้านไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล พร้อมพัฒนาความรู้ตามบทบาท	ผู้รับผิดชอบด้านดิจิทัล ข้อมูลส่วนบุคคล และบุคลากรตามการมอบหมาย	ก่อนเริ่มงาน เมื่อข้อกำหนดเปลี่ยนและตามรอบ; เนื้อหา รายชื่อ ผลทดสอบ และผลประเมินการปฏิบัติ	ตัวอย่าง: กลุ่มเป้าหมายเข้าร่วมไม่น้อยกว่าร้อยละ 90 และผ่านเกณฑ์ความรู้หรือการปฏิบัติที่กำหนด โดยติดตามผู้ที่ยังไม่ผ่าน

เป้าหมายระยะเวลากู้คืน (Recovery Time Objective: RTO) ใช้กับการฟื้นคืนกิจกรรมหรือบริการ ไม่ใช้แทนกำหนดเวลาคัดกรองหรือควบคุมเหตุ ส่วนเป้าหมายจุดกู้คืนข้อมูล (Recovery Point Objective: RPO) ใช้กำหนดช่วงข้อมูลสูญเสียที่ยอมรับได้ ทั้งสองค่าต้องอ้างอิงแผนและความสำคัญของบริการที่เกี่ยวข้อง

ตัวอย่างการจัดการข้อบกพร่อง (Control Deficiency Example) หากผลตรวจสอบพบว่าระบบที่ถึงกำหนดได้รับการติดตั้งชุดปรับปรุงเพียงร้อยละ 88 เทียบกับเกณฑ์ตัวอย่างร้อยละ 95 ให้บันทึกว่า **ไม่ผ่านเกณฑ์ความครอบคลุม** และวิเคราะห์ระบบที่ยังค้าง ระดับช่องโหว่ การเปิดรับการโจมตี และมาตรการชดเชย

การสรุปว่า “มีประสิทธิผลบางส่วน” ต้องมีหลักฐานว่าการควบคุมทำงานได้ในส่วนที่ดำเนินการแล้ว หากส่วนที่ค้างเป็นระบบสำคัญหรือช่องโหว่วิกฤต อาจมีผลต่อประสิทธิผลโดยรวมมากกว่าที่ร้อยละความครอบคลุมแสดง และอาจต้องยกระดับทันที

ให้จัดทำ **มาตรการแก้ไข (Corrective Action)** ระบุเจ้าของ กำหนดเวลา และการทดสอบยืนยัน พร้อมประเมินความเสี่ยงคงเหลือจากสภาพจริง ไม่ลดคะแนนเพียงเพราะเปิดรายการแก้ไขหรือมีแผนติดตั้งเพิ่มเติม ทั้งนี้ หากบางส่วนมีหลักฐานว่าช่วยลดความเสี่ยงได้ ให้พิจารณาเฉพาะผลที่ยืนยันได้ตามข้อ 4.8

4.10.5 ผลผลิตขั้นต่ำของขั้นตอนที่ 6 (Minimum Outputs of Step 6) เมื่อดำเนินขั้นตอนนี้ ต้องมีข้อมูลและหลักฐานอย่างน้อยดังต่อไปนี้

1. หลักฐานการดำเนินการควบคุมและมาตรการ (Control and Action Implementation Evidence)
2. สถานะ ผลส่งมอบ และความก้าวหน้าตามแผน (Status, Deliverables and Progress)
3. ผลทดสอบหรือประเมินการควบคุม (Control Testing or Assessment Results)
4. รายการข้อบกพร่อง ข้อยกเว้น และผลกระทบ (Deficiencies, Exceptions and Impacts)
5. แผนแก้ไข ผู้รับผิดชอบ และกำหนดแล้วเสร็จ (Corrective Actions, Owners and Due Dates)
6. ผลการติดตามและทดสอบซ้ำ (Follow-up and Retesting Results)
7. หลักฐานการเปลี่ยนแปลงแผนและการอนุมัติ หากมี (Plan Changes and Approvals)
8. บันทึกการรายงานหรือยกระดับเมื่อเข้าเงื่อนไข (Reporting or Escalation Records)

ให้บันทึกหรือเชื่อมโยงข้อมูลในทะเบียนความเสี่ยงและแบบ RISK-MJU-01 เพื่อใช้ประกอบการรายงานและประเมินความเสี่ยงคงเหลือ หากการควบคุมสำคัญไม่ทำงานหรือพบเหตุเร่งด่วน ต้องตอบสนองและยกระดับตามข้อกำหนดโดยไม่รอรอบติดตามปกติ

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

การสื่อสาร การรายงาน และการยกระดับมีวัตถุประสงค์เพื่อให้ผู้เกี่ยวข้องได้รับข้อมูลความเสี่ยงที่เหมาะสมกับบทบาทและทันต่อการตัดสินใจ สามารถดำเนินมาตรการ จัดสรรทรัพยากร และตอบสนองต่อสถานการณ์ได้อย่างเหมาะสม

การสื่อสารต้องเปิดโอกาสให้แลกเปลี่ยนข้อมูลและปรึกษาหารือระหว่างเจ้าของความเสี่ยง ผู้ปฏิบัติงาน หน่วยงานกำกับเฉพาะด้าน และผู้มีส่วนได้ส่วนเสียตามความจำเป็น โดยดำเนินการตลอดกระบวนการ ไม่จำกัดเฉพาะการส่งรายงานตามรอบ

4.11.1 หลักการของข้อมูลความเสี่ยง (Risk Information Principles) ข้อมูลความเสี่ยงต้องถูกต้อง ครบถ้วน ทันเวลา สอดคล้องกัน มีเจ้าของข้อมูล และตรวจสอบย้อนกลับได้ พร้อมได้รับการคุ้มครองตามระดับชั้นความลับ สิทธิการเข้าถึง และกฎหมายที่เกี่ยวข้อง ให้ระบุวันที่หรือช่วงเวลาของข้อมูล แหล่งข้อมูล นิยาม วิธีคำนวณ และข้อจำกัดที่สำคัญ หากข้อมูลยังไม่ครบถ้วน ให้แยกข้อเท็จจริงที่ยืนยันแล้ว ข้อมูลเบื้องต้น และสมมติฐานอย่างชัดเจน โดยไม่ชะลอการแจ้งเหตุเร่งด่วนเพื่อรอข้อมูลสมบูรณ์ รายงานต้องแสดงระดับและแนวโน้มความเสี่ยง สาเหตุ ผลกระทบ ประสิทธิผลของการควบคุม สถานะเทียบกับกรอบ RA/RT และประเด็นที่ต้องตัดสินใจ โดยติดตามความก้าวหน้าของมาตรการควบคู่กับผลต่อความเสี่ยง ไม่ใช้จำนวนกิจกรรมหรือร้อยละงานแล้วเสร็จเป็นข้อสรุปว่าความเสี่ยงลดลง

4.11.2 การกำหนดตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator Specification) ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ต้องเชื่อมโยงกับสาเหตุ ปัจจัยขับเคลื่อน การเปิดรับความเสี่ยง เหตุการณ์ หรือผลกระทบ และช่วยให้ผู้รับผิดชอบตัดสินใจได้ว่าต้องดำเนินการเมื่อใด ให้กำหนดหรือทบทวน KRI ตั้งแต่ขั้นตอนการกำหนดเกณฑ์ การประเมิน และการจัดทำแผน โดยในขั้นตอนนี้เน้นการรวบรวมผล การตีความ การสื่อสาร และการตอบสนอง ตัวชี้วัดแต่ละตัวต้องมีอย่างน้อยดังต่อไปนี้

1. ชื่อและนิยามตัวชี้วัด (Indicator Name and Definition)
2. วัตถุประสงค์และความเสี่ยงที่เชื่อมโยง (Related Objective and Risk)
3. สูตร หน่วยวัด และทิศทางความเสี่ยง (Formula, Unit and Risk Direction): ระบุว่าค่าสูงขึ้นหรือต่ำลงสะท้อนความเสี่ยงที่เพิ่มขึ้น
4. แหล่งข้อมูลและเจ้าของข้อมูล (Data Source and Data Owner)

5. ช่วงเวลาที่วัด ความถี่ และกำหนดส่งข้อมูล (Measurement Period, Frequency and Deadline)

6. ค่าฐาน ค่าจริง และแนวโน้ม (Baseline, Actual Value and Trend)

7. เกณฑ์ที่เชื่อมโยงกับ RA/RT และช่วงสถานะ (RA/RT-linked Thresholds and Status Bands)

8. จุดแจ้งเตือนและเงื่อนไขดำเนินการ (Trigger and Action)

9. ผู้รับผิดชอบตอบสนอง ผู้รับรายงาน และผู้มีอำนาจตัดสินใจ (Action Responsibility, Recipient and Decision Authority)

10. วิธีตรวจสอบข้อมูลและจัดการข้อมูลขาดหาย (Validation and Missing-data Handling)

ช่วงสถานะต้องไม่ซ้อนทับหรือมีช่องว่าง ข้อมูลที่ขาดหายต้องแสดงว่า “ยังไม่มีข้อมูล” หรือ “อยู่ระหว่างตรวจสอบ” ไม่แสดงเป็นสถานะปกติโดยอัตโนมัติ

ตัวชี้วัดนำและตัวชี้วัดตาม (Leading and Lagging Indicators)

- **ตัวชี้วัดนำ (Leading Indicator):** สะท้อนปัจจัยหรือเงื่อนไขที่อาจเพิ่มความเสี่ยงก่อนเกิดผลกระทบ เช่น จำนวนช่องโหว่รุนแรงที่ยังไม่แก้ไข จำนวนสัญญาณเตือนสำคัญที่ค้างเกินเวลา หรือสัดส่วนงานสำคัญที่ไม่มีผู้ปฏิบัติงานทดแทน
- **ตัวชี้วัดตาม (Lagging Indicator):** สะท้อนเหตุการณ์หรือผลกระทบที่เกิดขึ้นแล้ว เช่น จำนวนเหตุข้อมูลรั่วไหล ระยะเวลาระบบหยุดชะงัก หรือมูลค่าความเสียหาย

ควรเลือกใช้ทั้งสองลักษณะตามความจำเป็น อัตราการติดตั้งชุดปรับปรุงระบบอาจใช้เป็น **ตัวชี้วัดการควบคุมที่สำคัญ (Key Control Indicator: KCI)** และใช้เป็น KRI นำได้หากอธิบายความสัมพันธ์กับการเปิดรับความเสี่ยงไว้ชัดเจน ส่วนจำนวนผู้ผ่านการอบรมเพียงอย่างเดียวไม่ยืนยันความพร้อม ต้องพิจารณาสมรรถนะหรือการปฏิบัติจริงร่วมด้วย

ตัวอย่างการกำหนดตัวชี้วัดด้านความมั่นคงปลอดภัยไซเบอร์

ตัวอย่างนี้ใช้เพื่ออธิบายวิธีกำหนดตัวชี้วัด ไม่ใช่เกณฑ์ที่มหาวิทยาลัยอนุมัติแล้ว

รายการ	ตัวอย่าง
ความเสี่ยง (Risk)	ระบบสารสนเทศสำคัญอาจถูกโจมตีหรือหยุดชะงัก ส่งผลต่อข้อมูลและความต่อเนื่องของพันธกิจ
ตัวชี้วัดนำ/ตัวชี้วัดการควบคุม (Leading KRI/KCI)	ร้อยละของระบบสำคัญที่ถึงกำหนดติดตั้งชุดปรับปรุงความมั่นคงปลอดภัยและดำเนินการได้ภายในเวลาที่กำหนด
สูตร (Formula)	จำนวนระบบสำคัญที่ติดตั้งชุดปรับปรุงครบรายการที่ถึงกำหนดภายในเวลา ÷ จำนวนระบบสำคัญที่มีรายการถึงกำหนดในรอบรายงาน × 100
ขอบเขตข้อมูล (Data Scope)	ระบุรายการระบบ ระดับความรุนแรง กำหนดเวลา และวิธีจัดการระบบที่มีหลายรายการปรับปรุง หากไม่มีรายการถึงกำหนด ให้แสดง “ไม่เกี่ยวข้องในรอบนี้” ไม่คำนวณเป็นร้อยละ 100
เจ้าของข้อมูล (Data Owner)	ผู้รับผิดชอบข้อมูลระบบและช่องโหว่ที่ได้รับมอบหมาย
ความถี่ (Frequency)	สรุปรายเดือน โดยรายการวิกฤตติดตามตามความเร่งด่วน ไม่รอรอบรายเดือน
เกณฑ์ปฏิบัติที่เชื่อมโยงกับ RA	ตั้งแต่ร้อยละ 95 ขึ้นไป โดยยังต้องตรวจสอบช่องโหว่วิกฤตและข้อยกเว้นแยกต่างหาก
ช่วงเฝ้าระวัง (Warning Band)	ตั้งแต่ร้อยละ 90 แต่ต่ำกว่าร้อยละ 95
ขอบเขต RT (RT Boundary)	ไม่ต่ำกว่าร้อยละ 90 ณ รอบวัดที่กำหนด
เกิน RT (RT Breach)	ต่ำกว่าร้อยละ 90
จุดแจ้งเตือนและการตอบสนอง (Trigger and Action)	ต่ำกว่าร้อยละ 95 ให้วิเคราะห์รายการค้างและเร่งแก้ไข ต่ำกว่าร้อยละ 90 ให้ยกระดับภายใน 3 วันทำการ หรือเร็วกว่านั้นเมื่อเข้าเงื่อนไขเร่งด่วน
ตัวชี้วัดตาม (Lagging KRI)	จำนวนเหตุละเมิดข้อมูลที่มีผลกระทบรุนแรง และระยะเวลาหยุดชะงักของระบบสำคัญ โดยกำหนดนิยามและเกณฑ์แยกแต่ละตัว

ค่ารวมที่ผ่านเกณฑ์ไม่ยืนยันว่าความเสี่ยงอยู่ในระดับยอมรับได้ทั้งหมด หากยังมีช่องโหว่ วิกฤตในระบบสำคัญหรือมีหลักฐานการโจมตี ต้องพิจารณาและตอบสนองตามเหตุการณ์นั้นโดยเฉพาะ

4.11.3 องค์ประกอบขั้นต่ำของรายงาน (Minimum Report Contents) รายงานให้มีสาระอย่างน้อยดังต่อไปนี้ โดยปรับรายละเอียดให้เหมาะสมกับผู้รับและระดับการตัดสินใจ

1. ภาพรวมสถานะความเสี่ยง (University/Unit Risk Profile): ความเสี่ยงสำคัญ วัตถุประสงค์ และเจ้าของความเสี่ยง
2. ผลการประเมินความเสี่ยง (Risk Assessment): ความเสี่ยงโดยธรรมชาติ ความเสี่ยงคงเหลือ และความเสี่ยงคงเหลือเป้าหมาย โดยแยกสถานะและวันที่ชัดเจน
3. แนวโน้มและการเปลี่ยนแปลง (Trends and Changes): เปรียบเทียบกับรอบก่อนพร้อมสาเหตุ
4. ผลตัวชี้วัดและสถานะ RA/RT (Indicator Results and RA/RT Status)
5. ประสิทธิผลและข้อบกพร่องของการควบคุม (Control Effectiveness and Deficiencies)
6. ความก้าวหน้าและผลของมาตรการ (Action Progress and Results): รวมรายการล่าช้าและแผนแก้ไข
7. เหตุการณ์ ความเสียหาย และเหตุการณ์เกือบเกิดความเสียหาย (Incidents, Losses and Near Misses)
8. ความเสี่ยงเกิดใหม่ (Emerging Risks)
9. ความสัมพันธ์ การกระจุกตัว และผลกระทบสะสม (Interdependencies, Concentration and Cumulative Impacts)
10. ประเด็นที่ต้องตัดสินใจ (Decision Requests): ทางเลือก ข้อเสนอ ทรัพยากร และเวลาที่ต้องได้รับคำตัดสิน
11. คุณภาพและข้อจำกัดของข้อมูล (Data Quality and Limitations)
12. สถานะข้อสั่งการและการยอมรับความเสี่ยงชั่วคราว หากมี (Decision Follow-up and Temporary Acceptance Status)

เจ้าของข้อมูลรับผิดชอบคุณภาพข้อมูล เจ้าของความเสี่ยงรับผิดชอบการตีความและข้อเสนอการตอบสนอง ส่วนหน่วยบริหารความเสี่ยงรวบรวม วิเคราะห์ และสอบทานความสอดคล้อง โดยไม่รับรองข้อมูลแทนเจ้าของข้อมูลหรือเจ้าของความเสี่ยง

4.11.4 เกณฑ์เวลาในการรายงานและยกระดับ (Reporting and Escalation Timelines) ให้ใช้เส้นทางและระยะเวลาตามข้อ 3.6 และเงื่อนไขตามข้อ 3.10 โดยสรุปดังตารางที่ 4-24 ระยะเวลาสำหรับเหตุหรือการเปลี่ยนแปลงสำคัญให้นับตั้งแต่พบหรือรับทราบข้อมูลที่เข้าเกณฑ์ ไม่รอการรับรองรายงานหรือการสอบสวนให้เสร็จ

ตารางที่ 4-15 ***สรุประยะเวลาการรายงานและการติดตามความเสี่ยง***

เหตุหรือระดับความเสี่ยง	การแจ้งหรือรายงาน	การติดตาม
เหตุ Zero Tolerance เหตุวิกฤต หรือภัยคุกคามรุนแรงต่อชีวิต ข้อมูล หรือพันธกิจสำคัญ	แจ้งทันที และจัดทำรายงานเบื้องต้น ไม่เกิน 24 ชั่วโมง	ตามความเร่งด่วนและคำสั่งผู้มีอำนาจ
ความเสี่ยงคงเหลือระดับสูงมาก 16–25 (E)	แจ้งยกระดับทันที และจัดทำรายงาน ไม่เกิน 24 ชั่วโมง	อย่างน้อยรายเดือน หรือถี่กว่าตามสถานการณ์
ความเสี่ยงคงเหลือระดับสูง 10–15 (H) หรือผลกระทบระดับ 5 ที่คะแนนอยู่ต่ำกว่าระดับสูง	ภายใน 3 วันทำการเมื่อพบหรือเปลี่ยนแปลงเข้าเกณฑ์ หากเป็นภัยคุกคามเร่งด่วนให้แจ้งทันที	อย่างน้อยรายไตรมาส หรือถี่กว่าตามเกณฑ์เฉพาะ
KRI เกิน RT การควบคุมสำคัญไม่ทำงาน หรือมาตรการสำคัญล่าช้าจนกระทบเป้าหมาย	ภายใน 3 วันทำการ หรือเร็วกว่าตาม Trigger และความรุนแรง	ตามแผนแก้ไขและกำหนดเวลาที่ผู้มีอำนาจสั่งการ
ความเสี่ยงระดับปานกลาง 5–9 (M)	ตามรอบรายงานที่กำหนด อย่างน้อยรายไตรมาส	อย่างน้อยรายไตรมาส
ความเสี่ยงระดับต่ำ 1–4 (L)	ตามรอบการบริหารงานและรายงานปกติ	ทบทวนอย่างน้อยรายไตรมาส และเมื่อมีการเปลี่ยนแปลงสำคัญ

ระยะเวลา 24 ชั่วโมงหมายถึงชั่วโมงต่อเนื่อง ส่วน 3 วันทำการให้นับตามวันทำการ ทั้งนี้ต้องใช้เกณฑ์ที่มหาวิทยาลัยอนุมัติและประกาศกำหนด หากกฎหมาย แผนฉุกเฉิน แผนเผชิญเหตุ หรือข้อกำหนดเฉพาะกำหนดเวลาสั้นกว่า ให้ใช้เวลาที่สั้นกว่า พร้อมปฏิบัติตามผู้รับและช่องทางที่

กำหนด การรายงานภายในไม่ทดแทนการแจ้งหน่วยงานภายนอกตามกฎหมาย การมีผลกระทบระดับ 5 เป็นการกำหนดระดับการตอบสนองอย่างน้อยเทียบเท่าความเสี่ยงระดับสูง ไม่ได้ทำให้ทุกกรณีเป็นเหตุวิกฤตโดยอัตโนมัติ ต้องพิจารณาว่าเป็นความเสี่ยงที่อาจเกิดขึ้นหรือเหตุจริง รวมถึงความเร่งด่วนร่วมด้วย การรายงานไม่ทดแทนการระงับเหตุ ผู้รับผิดชอบต้องคุ้มครองชีวิต จำกัดความเสียหาย รักษาข้อมูล ทรัพย์สิน ความต่อเนื่อง และพยานหลักฐานควบคู่กัน โดยเหตุเร่งด่วนให้รายงานตรงต่อผู้มีอำนาจ พร้อมแจ้งหน่วยงานเฉพาะด้านและหน่วยบริหารความเสี่ยง ไม่ให้การรวบรวมข้อมูลเป็นจุดผ่านที่ทำให้ล่าช้า

4.11.5 ตัวอย่างการรายงานและยกระดับ (Reporting and Escalation Example)

สมมติว่าตัวชี้วัดการติดตั้งชุดปรับปรุงระบบลดลงจากร้อยละ 97 เป็นร้อยละ 93 และร้อยละ 88 ในสามรอบรายเดือน โดยใช้เกณฑ์ตัวอย่างตามตารางที่ 4-23

- **ร้อยละ 97:** ผ่านเกณฑ์ปฏิบัติ แต่ยังต้องตรวจสอบรายการวิกฤตหรือข้อยกเว้น
- **ร้อยละ 93:** เข้าช่วงเฝ้าระวัง ต้องวิเคราะห์สาเหตุและเร่งแก้ไขตั้งแต่รอบนี้
- **ร้อยละ 88:** เกิน RT ต้องยกระดับ ไม่จำเป็นต้องรอให้ต่ำกว่าเกณฑ์ติดต่อกันหลายเดือน

<u>เมื่อเกิน RT ให้ดำเนินการดังต่อไปนี้</u>

1. **เจ้าของข้อมูล (Data Owner):** ตรวจสอบสูตร ขอบเขต รายการค้าง และความถูกต้อง พร้อมระบุข้อมูลที่ยังไม่ยืนยัน

2. **เจ้าของการควบคุม (Control Owner):** จัดลำดับแก้ไขตามความรุนแรงและความสำคัญของระบบ พร้อมมาตรการชดเชยระหว่างรอ

3. **เจ้าของความเสี่ยง (Risk Owner):** ประเมินการเปิดรับการโจมตี ผลกระทบ และความเสี่ยงคงเหลือจากสภาพจริง

4. **เจ้าของมาตรการ (Action Owner):** จัดทำแผนแก้ไข ระบุผลส่งมอบ กำหนดเวลา และวิธีทดสอบยืนยัน

5. **การรายงานและยกระดับ:** แจ้งผู้บริหารที่กำกับและหน่วยบริหารความเสี่ยงภายใน 3 วันทำการ หรือทันทีหากมีช่องโหว่วิกฤตที่เข้าเงื่อนไขเร่งด่วน

6. **การติดตามข้อสั่งการ:** บันทึกผลการตัดสินใจและติดตามจนมีหลักฐานว่าการแก้ไขเกิดผล

หากพบการโจมตีหรือเหตุละเมิดข้อมูล ให้ใช้แผนเผชิญเหตุและประเมินเกณฑ์รายงานเฉพาะทันที ไม่รอรอบ KRI ทั้งนี้ เหตุไซเบอร์หรือข้อมูลรั่วไหลไม่เป็นเหตุ Zero Tolerance ทุกกรณีโดยอัตโนมัติ ต้องพิจารณาลักษณะเหตุ ความรุนแรง และนโยบายที่เกี่ยวข้อง

4.11.6 ผลผลิตขั้นต่ำของขั้นตอนที่ 7 (Minimum Outputs of Step 7)

1. ผลตัวชี้วัดและแผงสรุปข้อมูลตามความจำเป็น (Indicator Results and KRI Dashboard)

2. รายงานความเสี่ยงและข้อเสนอเพื่อการตัดสินใจ (Risk Report and Decision Requests)

3. บันทึกเหตุการณ์หรือการยกระดับ พร้อมเวลารับทราบและรายงาน (Incident/Escalation Record)

4. มาตรการแก้ไข ผู้รับผิดชอบ และกำหนดเวลา (Corrective Actions, Owners and Due Dates)

5. บันทึกการตัดสินใจและข้อสั่งการ (Decision Log)

6. สถานะการติดตามข้อสั่งการและกำหนดรายงานครั้งถัดไป (Decision Follow-up and Next Reporting Date)

ให้เชื่อมโยงข้อมูลกับทะเบียนความเสี่ยงหรือแบบ RISK-MJU-01 โดยจำกัดการเข้าถึงตามหน้าที่ และใช้ข้อมูลชุดเดียวกันสำหรับรายงานแต่ละระดับเท่าที่เหมาะสม เพื่อให้ข้อมูลสอดคล้องกันและลดการจัดทำรายงานซ้ำซ้อน

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

การติดตามและทบทวนมีวัตถุประสงค์เพื่อประเมินการเปลี่ยนแปลงของบริบท ระดับความเสี่ยง และประสิทธิผลของการควบคุม ตรวจสอบว่ามาตรการดำเนินการตามแผนและเกิดผลตามที่คาดหวังหรือไม่ และนำข้อมูลไปปรับปรุงการบริหารความเสี่ยงอย่างต่อเนื่อง

ความก้าวหน้าหรือการดำเนินกิจกรรมครบถ้วนไม่ทำให้ความเสี่ยงลดลงโดยอัตโนมัติ การเปลี่ยนระดับความเสี่ยงคงเหลือ (Residual Risk) ต้องมีข้อมูลและหลักฐานรองรับผลต่อโอกาสเกิดหรือผลกระทบ โดยแยกจากความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk) ซึ่งเป็นค่าคาดการณ์ในอนาคต

4.12.1 การติดตามโดยฝ่ายบริหาร (Management Monitoring) เจ้าของความเสี่ยง (Risk Owner) ต้องกำกับติดตามข้อมูลจากเจ้าของการควบคุม เจ้าของมาตรการ และเจ้าของข้อมูลอย่างน้อยในประเด็นดังต่อไปนี้

1. ระดับและแนวโน้มความเสี่ยง (Risk Levels and Trends): ความเสี่ยงคงเหลือ การเปลี่ยนแปลงจากรอบก่อน และความก้าวหน้าเทียบกับระดับเป้าหมาย รวมทั้งทบทวนความเสี่ยงโดยธรรมชาติเมื่อบริบทหรือปัจจัยเสี่ยงเปลี่ยนแปลง
2. ผลตัวชี้วัดและสถานะ RA/RT (Indicator Results and RA/RT Status)
3. ประสิทธิผลและข้อบกพร่องของการควบคุมสำคัญ (Key Control Effectiveness and Deficiencies)
4. ความก้าวหน้า คุณภาพ และความล่าช้าของมาตรการ (Action Progress, Quality and Delays)
5. เหตุการณ์ ความเสียหาย และเหตุการณ์เกือบเกิดความเสียหาย (Incidents, Losses and Near Misses)
6. การเปลี่ยนแปลงบริบทและสมมติฐาน (Context and Assumption Changes): รวมกฎหมาย เทคโนโลยี และความต้องการของผู้มีส่วนได้ส่วนเสีย
7. ความเสี่ยงเกิดใหม่และความสัมพันธ์ระหว่างความเสี่ยง (Emerging Risks and Interdependencies)
8. ประเด็นที่ต้องตัดสินใจหรือสนับสนุนเพิ่มเติม (Decision and Resource Needs)
9. ข้อสั่งการและเงื่อนไขการยอมรับความเสี่ยง (Management Decisions and Acceptance Conditions): รวมวันสิ้นสุดและกำหนดทบทวน

ตารางที่ 4-16 ***ความถี่ขั้นต่ำในการติดตามตามระดับความเสี่ยงคงเหลือ***

ระดับความเสี่ยง	ความถี่ขั้นต่ำ	แนวทางดำเนินการ
สูงมาก 16–25 (E)	อย่างน้อยรายเดือน หรือถี่กว่าตามสถานการณ์	เร่งดำเนินมาตรการ ติดตามใกล้ชิด และรายงานผู้บริหารตามข้อกำหนด
สูง 10–15 (H)	อย่างน้อยรายไตรมาส หรือถี่กว่าตาม KRI และความเร่งด่วน	ติดตามแผนจัดการความเสี่ยง สถานะ RA/RT และประเด็นที่ต้องตัดสินใจ

ระดับความเสี่ยง	ความถี่ขั้นต่ำ	แนวทางดำเนินการ
ปานกลาง 5–9 (M)	อย่างน้อยรายไตรมาส หรือถี่กว่าตามเกณฑ์เฉพาะ	ติดตามโดยเจ้าของความเสี่ยงและปรับมาตรการตามความจำเป็น
ต่ำ 1–4 (L)	ทบทวนอย่างน้อยรายไตรมาส โดยติดตามงานประจำตามความเหมาะสม	รักษาการควบคุมและเฝ้าระวังการเปลี่ยนแปลง การยอมรับต้องอยู่ภายในกรอบและอำนาจ

ความถี่ในตารางเป็นรอบติดตาม ไม่ใช่ระยะเวลาที่อนุญาตให้รอแจ้งเหตุ เมื่อ KRI เกิน RT พบเหตุ Zero Tolerance การควบคุมสำคัญไม่ทำงาน หรือเข้าเงื่อนไขเร่งด่วน ต้องตอบสนองและยกระดับตามข้อ 3.6 ข้อ 3.9 และข้อ 4.11 โดยไม่รอรอบปกติ

ตัวอย่าง: หากตัวชี้วัดการติดตั้งชุดปรับปรุงระบบลดลงจากร้อยละ 97 เป็นร้อยละ 93 และร้อยละ 88 โดยใช้เกณฑ์สมมติว่าตั้งแต่ร้อยละ 95 ขึ้นไปเป็นเกณฑ์ปฏิบัติ และต่ำกว่าร้อยละ 90 เป็นการเกิน RT ต้องเริ่มแก้ไขเมื่อเข้าสู่ช่วงร้อยละ 93 และยกระดับเมื่อพบร้อยละ 88 ไม่ต้องรอให้เกินเกณฑ์ติดต่อกันหลายรอบ พร้อมตรวจสอบความรุนแรงของรายการค้างและประเมินความเสี่ยงคงเหลือจากสภาพจริง

4.12.2 การทบทวนทะเบียนความเสี่ยง (Risk Register Review) ทะเบียนความเสี่ยงต้องได้รับการทบทวนตามรอบติดตามและเมื่อเกิดเงื่อนไขกระตุ้น (Trigger) อย่างน้อยดังต่อไปนี้

1. วัตถุประสงค์ ยุทธศาสตร์ KPI หรือเป้าหมายเปลี่ยนแปลง
2. มีกฎหมาย นโยบาย มาตรฐาน หรือข้อกำหนดใหม่ที่เกี่ยวข้อง
3. เกิดเหตุการณ์ เหตุการณ์เกือบเกิดความเสียหาย ข้อร้องเรียน หรือความเสียหายสำคัญ
4. การควบคุมสำคัญล้มเหลวหรือไม่ทำงานตามวัตถุประสงค์
5. KRI เข้าช่วงเตือนตามเงื่อนไขที่กำหนดหรือเกิน RT
6. โครงการ การลงทุน ระบบงาน โครงสร้างองค์กร หรือผู้ให้บริการสำคัญเปลี่ยนแปลง
7. พบความเสี่ยงเกิดใหม่หรือความเสี่ยงที่เชื่อมโยงหลายส่วนงาน
8. ผลตรวจสอบหรือการให้ความเชื่อมั่นพบข้อบกพร่องสำคัญ
9. สมมติฐานที่ใช้ประเมินไม่สอดคล้องกับข้อเท็จจริง
10. เงื่อนไขการยอมรับความเสี่ยงเปลี่ยนแปลงหรือใกล้สิ้นสุดระยะเวลาที่อนุมัติ

<u>การทบทวนต้องบันทึกอย่างน้อยดังต่อไปนี้</u>

- วันที่ กรอบเวลา และเกณฑ์ที่ใช้ (Assessment Date, Time Horizon and Criteria)
- ข้อมูล หลักฐาน สมมติฐาน และข้อจำกัด (Data, Evidence, Assumptions and Limitations)
- ผู้ประเมิน เจ้าของความเสี่ยง และผู้พิจารณาตามอำนาจ (Assessor, Risk Owner and Review Authority)
- การเปลี่ยนแปลงของสาเหตุ เหตุการณ์ และผลกระทบ (Changes in Causes, Events and Impacts)
- คะแนนเดิม คะแนนใหม่ และเหตุผล (Previous and Revised Scores with Rationale)
- ผลประเมินการควบคุม (Control Assessment Results)
- สถานะตัวชี้วัดและมาตรการ (Indicator and Action Status)
- การตัดสินใจ การยอมรับ หรือการยกระดับ (Decisions, Acceptance or Escalation)
- ผู้รับผิดชอบและกำหนดติดตามครั้งถัดไป (Responsible Roles and Next Review Date)

ห้ามลดคะแนนเพียงเพราะมาตรการได้รับอนุมัติหรือมีความก้าวหน้า หากมาตรการดำเนินการบางส่วนและมีหลักฐานว่าช่วยลดความเสี่ยงได้จริง สามารถพิจารณาเฉพาะผลที่ยืนยันได้ โดยไม่จำเป็นต้องรอให้ทุกกิจกรรมแล้วเสร็จ แต่ต้องบันทึกส่วนที่ยังไม่ครอบคลุมและความเสี่ยงที่ยังคงอยู่

ตัวอย่าง: ระบบสำคัญมีความเสี่ยงโดยธรรมชาติ 20 คะแนน และความเสี่ยงคงเหลือ 15 คะแนน แม้โครงการปรับปรุงระบบสำรองได้รับอนุมัติแล้ว แต่ยังไม่ติดตั้งและทดสอบ จึงไม่สามารถอ้างโครงการนั้นเพื่อลดคะแนนได้ หากข้อมูลและเงื่อนไขเดิมไม่เปลี่ยนแปลง ให้คงผลประเมินที่ 15 คะแนน ส่วนค่าคาดการณ์ 8 คะแนนให้บันทึกเป็นความเสี่ยงคงเหลือเป้าหมาย จนมีหลักฐานรองรับการประเมินใหม่

4.12.3 การติดตามและการให้ความเชื่อมั่นตามหลัก Three Lines (Monitoring and Assurance under the Three Lines Model) การติดตามของฝ่ายบริหารและการให้ความเชื่อมั่นต้องประสานกัน โดยรักษาความรับผิดชอบและระดับความเป็นอิสระของแต่ละบทบาท ดังนี้

บทบาท	หน้าที่ในการติดตามและให้ความเชื่อมั่น
สายงานที่หนึ่ง (First Line Roles)	เจ้าของความเสี่ยง เจ้าของการควบคุม และเจ้าของมาตรการ ติดตามการปฏิบัติงาน ประเมินการควบคุม และรับผิดชอบการแก้ไขในงานที่ตนกำกับ
สายงานที่สอง (Second Line Roles)	หน่วยงานบริหารความเสี่ยง การควบคุมภายใน กฎหมายและการปฏิบัติตาม กฎเกณฑ์ ไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล ความปลอดภัย และหน้าที่กำกับเฉพาะด้าน สนับสนุนมาตรฐาน ให้คำปรึกษา ติดตาม สอบทาน และเสนอข้อสังเกต โดยไม่รับผิดชอบแทนเจ้าของความเสี่ยง
สายงานที่สาม (Third Line Roles)	กองตรวจสอบภายในให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระและเที่ยงธรรมต่อการกำกับดูแล การบริหารความเสี่ยง และการควบคุม โดยไม่ตัดสินใจ ออกแบบ หรือดำเนินการควบคุมแทนฝ่ายบริหาร
ผู้ให้ความเชื่อมั่นอื่น (Other Assurance Providers)	ผู้สอบบัญชี ผู้ประเมินภายนอก หน่วยรับรอง ผู้เชี่ยวชาญ และหน่วยงานกำกับดูแล ประเมินตามขอบเขต อำนาจหน้าที่ และระดับความเป็นอิสระของแต่ละแหล่ง โดยไม่ถือเป็นสายงานที่สามของมหาวิทยาลัย

การให้คำปรึกษาของกองตรวจสอบภายในสามารถรวมถึงข้อเสนอแนะเกี่ยวกับการออกแบบการควบคุมได้ แต่ฝ่ายบริหารต้องเป็นผู้เลือก อนุมัติ และนำไปปฏิบัติ พร้อมจัดมาตรการคุ้มครองความเป็นอิสระและความเที่ยงธรรมเมื่อจำเป็น

มหาวิทยาลัยให้จัดทำ **แผนผังการให้ความเชื่อมั่น (Assurance Map)** สำหรับความเสี่ยงสำคัญระดับมหาวิทยาลัยตามข้อ 2.10 เพื่อระบุแหล่งการประเมิน ขอบเขต ความถี่ ระดับความเป็นอิสระ ความซ้ำซ้อน และช่องว่าง ส่วนงานประยุกต์ใช้ตามสัดส่วนและความจำเป็น

ตัวอย่าง: เจ้าของการควบคุมรายงานว่ามีการสำรองข้อมูลทุกวัน หน่วยงานสายงานที่สองสอบทานบันทึกและยืนยันว่ามีการสำรองจริง แต่การตรวจสอบภายในพบจากหลักฐานการทดสอบกู้คืนว่าบางระบบไม่สามารถกลับมาให้บริการภายในเป้าหมายระยะเวลากู้คืน จึงต้องแยกข้อสรุปว่า “สำรองข้อมูลครบตามรอบ” ออกจาก “กู้คืนได้ตามเป้าหมาย” พร้อมให้ฝ่ายบริหารจัดทำมาตรการแก้ไขและทดสอบซ้ำ

4.12.4 ความต่อเนื่องและความยืดหยุ่นขององค์กร (Business Continuity and Organizational Resilience) ความเสี่ยงที่อาจทำให้พันธกิจสำคัญหยุดชะงักต้องเชื่อมโยงกับการเตรียมพร้อมและการฟื้นตัว ได้แก่

1. การวิเคราะห์ผลกระทบต่อการดำเนินงาน (Business Impact Analysis: BIA)

2. การบริหารความต่อเนื่องขององค์กร (Business Continuity Management: BCM)
3. แผนความต่อเนื่องในการดำเนินงาน (Business Continuity Plan: BCP)
4. การสื่อสารภาวะวิกฤต (Crisis Communication)
5. การตอบสนองต่อเหตุการณ์ (Incident Response)
6. แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan: DRP)
7. เป้าหมายระยะเวลาการกู้คืน (Recovery Time Objective: RTO)
8. เป้าหมายจุดการกู้คืนข้อมูล (Recovery Point Objective: RPO)

ส่วนงานต้องกำหนดภารกิจสำคัญ ระดับบริการขั้นต่ำ ทรัพยากร ผู้รับผิดชอบ วิธีดำเนินงานทดแทน ช่องทางติดต่อ และลำดับการกู้คืน พร้อมทดสอบตามแผนที่กำหนด วิเคราะห์ช่องว่าง และติดตามการแก้ไข การมีเอกสาร BCP หรือ DRP โดยไม่มีหลักฐานการทดสอบไม่เพียงพอที่จะยืนยันความพร้อม

ตัวอย่างสมมติ: ระบบทะเบียนนักศึกษามีเป้าหมาย RTO ไม่เกิน 4 ชั่วโมง และ RPO ไม่เกิน 1 ชั่วโมง แต่ผลทดสอบใช้เวลากู้คืนบริการ 7 ชั่วโมง และจุดข้อมูลล่าสุดที่กู้คืนได้อยู่ก่อนเวลาเกิดเหตุ 3 ชั่วโมง จึงไม่ผ่านทั้งสองเกณฑ์ ต้องวิเคราะห์สาเหตุ ปรับปรุงวิธีกู้คืนและสำรองข้อมูล และทดสอบซ้ำ โดยตัวเลขนี้ไม่ใช่ค่าเป้าหมายที่รับรองว่ามหาวิทยาลัยอนุมัติแล้ว

4.12.5 การเรียนรู้และปรับปรุง (Learning and Improvement) มหาวิทยาลัยและส่วนงานต้องใช้ข้อมูลจากเหตุการณ์ ข้อร้องเรียน เหตุการณ์เกือบเกิดความเสียหาย ผลตรวจสอบ การทดสอบแผน ข้อมูลคู่เทียบ และผลการดำเนินงาน วิเคราะห์สาเหตุราก (Root Cause Analysis) ตามความสำคัญของประเด็น และนำไปปรับปรุงอย่างน้อยในเรื่องดังต่อไปนี้

- นโยบายและกระบวนงาน (Policies and Processes)
- การควบคุมและมาตรการ (Controls and Actions)
- ตัวชี้วัดและเกณฑ์ตอบสนอง (Indicators and Response Criteria)
- ระบบและคุณภาพข้อมูล (Information Systems and Data Quality)
- สมรรถนะบุคลากร (People Competencies)
- ความต่อเนื่องและการกู้คืน (Continuity and Recovery)
- วัฒนธรรมความเสี่ยง (Risk Culture)
- บทบาทและอำนาจตัดสินใจ (Roles and Decision Authority)

การปรับ RA/RT หรือเกณฑ์สำคัญต้องมีเหตุผล หลักฐาน และอนุมัติตามอำนาจ ไม่ปรับย้อนหลังเพื่อทำให้ผลที่เกินเกณฑ์กลับเป็นผลที่ยอมรับได้

ตัวอย่าง: ภายหลังส่งข้อมูลส่วนบุคคลทางอีเมลผิดผู้รับ ให้วิเคราะห์กระบวนการเลือกผู้รับ สิทธิ์เข้าถึง การตรวจสอบก่อนส่ง และข้อจำกัดของระบบ แล้วเลือกมาตรการที่ตอบสนองสาเหตุ เช่น การยืนยันผู้รับ การจำกัดการส่งข้อมูล การเข้ารหัส หรือระบบป้องกันข้อมูลรั่วไหล (Data Loss Prevention: DLP) ตามความเหมาะสม พร้อมทดสอบการทำงาน ไม่สรุปผลจากการอบรมซ้ำหรือจำนวนเหตุที่ลดลงเพียงอย่างเดียว เพราะอาจมีการรายงานไม่ครบถ้วน

การปิดมาตรการหรือข้อบกพร่องต้องมีหลักฐานว่าผลส่งมอบครบ การควบคุมทำงาน และประเด็นได้รับการจัดการตามเกณฑ์ที่กำหนด หากยังมีความเสี่ยงคงเหลือ ให้ระบุการติดตามหรือการยอมรับตามอำนาจต่อไป การปิดงานไม่ทำให้ความเสี่ยงหรือหน้าที่ตามกฎหมายสิ้นสุดลงโดยอัตโนมัติ

4.12.6 ผลผลิตขั้นต่ำของขั้นตอนที่ 8 (Minimum Outputs of Step 8)

1. ทะเบียนความเสี่ยงฉบับปรับปรุง (Updated Risk Register): พร้อมวันที่ หลักฐาน เหตุผลการเปลี่ยนแปลง และผู้ยืนยันข้อมูล

2. ผลการติดตามตัวชี้วัด การควบคุม และมาตรการ (Indicator, Control and Action Monitoring Results)

3. ข้อมูลสรุปสถานะและภาพรวมความเสี่ยงที่ปรับปรุงตามขอบเขต (Updated Risk Profile and Portfolio View)

4. รายงานหรือบันทึกการทบทวนโดยฝ่ายบริหาร (Management Review Record): ข้อสรุป ข้อสั่งการ ผู้รับผิดชอบ และกำหนดเวลา

5. ข้อค้นพบและสถานะการแก้ไขจากการให้ความเชื่อมั่น (Assurance Findings and Remediation Status)

6. ผลทดสอบแผนความต่อเนื่องและการกู้คืนตามความเกี่ยวข้อง (Continuity and Recovery Test Results)

7. บทเรียนและผลวิเคราะห์สาเหตุตามความจำเป็น (Lessons Learned and Root Cause Analysis)

8. แผนปรับปรุงพร้อมวิธียืนยันผล (Improvement Plan and Verification Criteria)

ผลการทบทวนให้ใช้เป็นข้อมูลป้อนกลับเพื่อปรับบริบท วัตถุประสงค์ เกณฑ์ รายการความเสี่ยง และมาตรการในขั้นตอนก่อนหน้า รวมถึงประกอบการทบทวนยุทธศาสตร์และกรอบการบริหารความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4.13 การควบคุมคุณภาพข้อมูลและเอกสารความเสี่ยง (Risk Data and Documentation Quality Control)

ก่อนเสนอทะเบียนความเสี่ยง รายงานผล หรือแผนบริหารความเสี่ยงต่อผู้บริหารหรือคณะกรรมการ ผู้จัดทำ เจ้าของข้อมูล และเจ้าของความเสี่ยงต้องตรวจสอบและยืนยันข้อมูลตามบทบาท ส่วนหน่วยบริหารความเสี่ยงสอบทานความครบถ้วน ความสอดคล้อง และการใช้เกณฑ์กลาง โดยไม่รับรองข้อมูลหรือผลการประเมินแทนผู้รับผิดชอบ

การตรวจสอบคุณภาพต้องช่วยให้ข้อมูลเหมาะสมต่อการตัดสินใจและตรวจสอบย้อนกลับได้ โดยไม่ทำให้การแจ้งเหตุฉุกเฉินหรือการยกระดับเร่งด่วนล่าช้า

4.13.1 เกณฑ์ตรวจสอบคุณภาพ (Quality Review Criteria)

ตารางที่ 4-17 ***เกณฑ์การควบคุมคุณภาพข้อมูลและเอกสารความเสี่ยง***

ประเด็น	เกณฑ์คุณภาพ	ตัวอย่างการตรวจสอบ
ความเชื่อมโยงกับวัตถุประสงค์ (Objective Linkage)	ระบุวัตถุประสงค์ KPI เป้าหมาย และเจ้าของความเสี่ยงชัดเจน	ความเสี่ยงระบบหยุดชะงักเชื่อมโยงกับเป้าหมายความต่อเนื่องของบริการสำคัญ
ข้อความความเสี่ยง (Risk Statement)	แสดงสาเหตุ–เหตุการณ์–ผลกระทบ และมีขอบเขตที่จัดการได้	ไม่ใช้เพียงคำว่า “ระบบล่ม” หรือ “เทคโนโลยีมีปัญหา”
คะแนนความเสี่ยง (Risk Score)	ใช้เกณฑ์และกรอบเวลาเดียวกัน มีข้อมูลเหตุผล และหลักฐานรองรับ	ตรวจสถิติเหตุการณ์ ช่องโหว่ ผลทดสอบ และเหตุผลของคะแนนโอกาสเกิดกับผลกระทบ
ผลกระทบและเกณฑ์พิเศษ (Impact and Override)	ประเมินมิติที่เกี่ยวข้อง ใช้คะแนนสูงสุดที่มีหลักฐานรองรับ และแยกระดับการตอบสนองจากระดับตามคะแนน	ผลกระทบระดับ 5 ได้รับการตอบสนองอย่างน้อยเทียบเท่าระดับสูง แม้คะแนนรวมต่ำกว่า 10
ผลประเมินการควบคุม (Control Assessment)	แยกการออกแบบ การนำไปใช้ และประสิทธิผล พร้อมเจ้าของและหลักฐาน	มีผลทดสอบกู้คืนจริง ไม่ใช้เพียงรายงานว่ามีระบบสำรอง

ประเด็น	เกณฑ์คุณภาพ	ตัวอย่างการตรวจสอบ
ตัวชี้วัดและข้อมูล (Indicators and Data)	มีนิยาม สูตร หน่วยวัด แหล่งข้อมูล เจ้าของข้อมูล ความถี่ เกณฑ์สถานะ และ Trigger/Action	ตัวชี้วัดการติดตั้งชุดปรับปรุงมีตัวหารที่ถูกต้อง และไม่แสดงข้อมูลขาดหายเป็นสถานะปกติ
มาตรการ (Treatment Actions)	ตอบสนองสาเหตุหรือผลกระทบ มีผลส่งมอบ ผู้รับผิดชอบ ทรัพยากร และกำหนดเวลา	ระบุการปรับระบบสำรองและทดสอบกู้คืน แทนข้อความว่า “เฝ้าระวัง” เพียงอย่างเดียว
สถานะความเสี่ยง (Risk Assessment States)	แยกความเสี่ยงโดยธรรมชาติ ความเสี่ยงคงเหลือ และความเสี่ยงคงเหลือเป้าหมาย	ไม่ลดความเสี่ยงคงเหลือจากมาตรการที่ยังเป็นแผน
การรายงานและยกระดับ (Reporting and Escalation)	เมื่อเข้าเงื่อนไข มีหลักฐานการแจ้ง ผู้รับรายงาน เวลา ข้อสั่งการ และการติดตาม	มีบันทึกการยกระดับและบันทึกการตัดสินใจเมื่อ KRI เกิน RT
ภาพรวมความเสี่ยง (Portfolio View)	ใช้รหัสและนิยามร่วม ลดรายการซ้ำ และวิเคราะห์ความสัมพันธ์กับการกระจุกตัว	เชื่อมโยงความเสี่ยงไซเบอร์หลายส่วนงาน โดยไม่บวกคะแนนหรือรวมรายการจนสูญเสียเจ้าของและรายละเอียด
การควบคุมเอกสาร (Document Control)	มีฉบับ วันที่ ผู้จัดทำ ผู้สอบทาน ผู้อนุมัติ ตามอำนาจ และแหล่งอ้างอิง	ตรวจสอบได้ว่าใครเปลี่ยนคะแนนเมื่อใด และด้วยเหตุผลใด
การคุ้มครองข้อมูล (Information Protection)	กำหนดสิทธิ์เข้าถึง ชั้นความลับ วิธีจัดเก็บ และระยะเวลาเก็บตามข้อกำหนด	รายละเอียดเหตุข้อมูลรั่วไหลหรือผู้ร้องเรียนเปิดเผยเฉพาะผู้มีหน้าที่เกี่ยวข้อง

4.13.2 ตัวอย่างการปรับปรุงคุณภาพข้อความ (Risk Statement Quality Example)

ข้อความเดิมที่ยังไม่เพียงพอ “ความเสี่ยงด้านเทคโนโลยี: ระบบอาจมีปัญหา จึงจัดอบรมบุคลากรและสำรองข้อมูล” ข้อความนี้ยังไม่ระบุเหตุการณ์ สาเหตุ และผลกระทบอย่างชัดเจน และนำมาตรการมารวมกับข้อความความเสี่ยง ควรแยกประเด็นตามเหตุการณ์ที่ต้องจัดการ เช่น

ตัวอย่างที่ 1 ความเสี่ยงต่อการถูกโจมตี “เนื่องจากระบบสำคัญบางส่วนยังมีช่องโหว่ที่ไม่ได้รับการแก้ไขตามกำหนด อาจเกิดการเข้าถึงระบบโดยไม่ได้รับอนุญาต ส่งผลให้ข้อมูลสำคัญถูกเปิดเผยหรือเสียหายและบริการหยุดชะงัก”

ตัวอย่างที่ 2 ความเสี่ยงต่อการกู้คืนไม่ทันเป้าหมาย “เนื่องจากระบบสำรองและวิธีกู้คืนยังมีข้อบกพร่องตามผลทดสอบ อาจทำให้ไม่สามารถกู้คืนบริการและข้อมูลตามเป้าหมายที่กำหนดเมื่อเกิดเหตุหยุดชะงัก ส่งผลให้พันธกิจสำคัญหยุดดำเนินการนานกว่าระยะเวลาที่รองรับได้”

ทั้งสองรายการอาจเชื่อมโยงกัน แต่มีมาตรการและหลักฐานยืนยันผลต่างกัน หากบันทึกรวมต้องแสดงสถานการณ์ การควบคุม และผู้รับผิดชอบให้ชัดเจน ข้อมูลประกอบต้องระบุวัตถุประสงค์ เจ้าของความเสี่ยง เจ้าของการควบคุม ผลประเมินความเสี่ยง กรอบ RA/RT ตัวชี้วัด มาตรการ ผู้รับผิดชอบ กำหนดเวลา และหลักฐานตามขั้นตอนที่เกี่ยวข้อง

4.13.3 การจัดการข้อบกพร่องของข้อมูลและเอกสาร (Data and Documentation Deficiency Management) หากพบข้อบกพร่องที่มีนัยสำคัญ ให้แจ้งเจ้าของความเสี่ยงหรือเจ้าของข้อมูลแก้ไข พร้อมระบุรายการที่ต้องแก้ ผู้รับผิดชอบ และกำหนดเวลา ก่อนเสนอรายงานฉบับสมบูรณ์ตามกระบวนการปกติ

กรณีต้องตัดสินใจเร่งด่วน ให้รายงานข้อมูลที่มีพร้อมแสดงสถานะการยืนยัน ข้อจำกัด และความเสี่ยงจากการใช้ข้อมูลนั้น แล้วติดตามปรับปรุงภายหลัง ไม่ระงับการแจ้งเหตุเพียงเพราะข้อมูลยังไม่ครบถ้วน และไม่ใช้ข้อมูลที่ยังไม่มีหลักฐานเพียงพอเป็นฐานลดระดับความเสี่ยง ให้เก็บประวัติการแก้ไขข้อมูล คะแนน เกณฑ์ และข้อสั่งการ โดยระบุวันที่ ผู้แก้ไข เหตุผล และผู้ให้ความเห็นชอบตามอำนาจ เพื่อให้ตรวจสอบย้อนหลังได้

4.14 ผลลัพธ์ของกรอบการบริหารความเสี่ยง (Outcomes of the Risk Management Framework)

การประเมินผลของกรอบการบริหารความเสี่ยงต้องพิจารณาว่าระบบช่วยให้มหาวิทยาลัยตัดสินใจ จัดการความไม่แน่นอน คุ้มครองพันธกิจ และใช้ประโยชน์จากโอกาสได้ดีขึ้นเพียงใด โดยใช้หลักฐานทั้งด้านการดำเนินงานและผลลัพธ์

4.14.1 ผลลัพธ์ที่คาดหวังและหลักฐาน (Expected Outcomes and Evidence)

ตารางที่ 4-18 ***ผลลัพธ์ที่คาดหวังของกรอบการบริหารความเสี่ยง***

ผลลัพธ์ที่คาดหวัง	ตัวอย่างหลักฐานและข้อพิจารณา
ความเสี่ยงสำคัญเชื่อมโยงกับยุทธศาสตร์และผลการดำเนินงาน	ทะเบียนความเสี่ยงระบุวัตถุประสงค์ KPI และผลลัพธ์เชิงยุทธศาสตร์ พร้อมแสดงว่าข้อมูลถูกใช้ทบทวนแผนหรือทางเลือก
ผู้มีอำนาจได้รับข้อมูลเพียงพอและทันเวลา	รายงานแสดงแนวโน้ม KRI สถานะ RA/RT และประเด็นตัดสินใจ พร้อมหลักฐานเวลารายงานและการตอบสนอง
ความเสี่ยงที่เข้าเกณฑ์ได้รับการยกระดับและจัดการ	บันทึกการยกระดับ ข้อสั่งการ ผู้รับผิดชอบ และผลติดตาม ไม่พิจารณาเพียงว่ามีการส่งรายงาน
การควบคุมและมาตรการมีผลที่ยืนยันได้	ผลทดสอบการควบคุม บันทึกระบบ การทดสอบตัวอย่างรายการ และผลทดสอบ BCP/DRP
การจัดสรรทรัพยากรคำนึงถึงความเสี่ยง	เหตุผลการอนุมัติงบประมาณหรือบุคลากรที่พิจารณาความสำคัญเชิงยุทธศาสตร์ ความเร่งด่วน กฎหมาย ผลกระทบ และประโยชน์ ไม่จัดลำดับจากคะแนนเพียงอย่างเดียว
องค์กรเรียนรู้และพร้อมต่อเหตุหยุดชะงัก	ผลวิเคราะห์สาเหตุ บทเรียน การแก้ไข และผลทดสอบซ้ำที่แสดงความพร้อมตามเป้าหมาย
วัฒนธรรมความเสี่ยงและขีดความสามารถของระบบพัฒนา	คุณภาพและความทันเวลาของการรายงาน การแก้ไขสาเหตุซ้ำ ความตรงเวลาของมาตรการ และผลประเมินพฤติกรรมจากหลายแหล่ง
มหาวิทยาลัยสร้าง รักษา และเพิ่มคุณค่า	หลักฐานการใช้ข้อมูลความเสี่ยงประกอบยุทธศาสตร์ โครงการ การลงทุน และโอกาส พร้อมผลต่อคุณภาพ ประสิทธิภาพ ความต่อเนื่อง หรือผู้มีส่วนได้ส่วนเสีย

ผลลัพธ์ไม่ควรประเมินจากจำนวนแบบฟอร์ม การประชุม หรือกิจกรรมเพียงอย่างเดียว และไม่กำหนดว่าคะแนนความเสี่ยงต้องลดลงทุกกรณี เพราะความเสี่ยงอาจเพิ่มขึ้นจากบริบทหรือการรับรู้ข้อมูลที่ดีขึ้น ต้องพิจารณาความเหมาะสมของการตอบสนองและความสามารถในการบรรลุวัตถุประสงค์ร่วมด้วย

4.14.2 ตัวอย่างภาพรวมผลลัพธ์ (Illustrative Outcome Example)

ตัวอย่างสมมตินี้ไม่ใช่ผลประเมินจริงหรือเกณฑ์ที่มหาวิทยาลัยอนุมัติ เดิมความเสี่ยงด้านความต่อเนื่องของระบบสารสนเทศมีความเสี่ยงคงเหลือ **โอกาสเกิด 3 × ผลกระทบ 5 = 15 ระดับสูง**

และตัวชี้วัดการติดตั้งชุดปรับปรุงต่ำกว่าขอบเขต RT หลังฝ่ายบริหารอนุมัติทรัพยากร มอบหมายผู้รับผิดชอบ และดำเนินมาตรการ พบว่า

1. **การควบคุมช่องโหว่ดีขึ้น:** อัตราติดตั้งตามกำหนดเพิ่มจากร้อยละ 88 เป็นร้อยละ 97 โดยตรวจสอบรายการวิกฤตที่ค้างแยกต่างหาก

2. **การกู้คืนผ่านเป้าหมาย:** ผลทดสอบยืนยันว่าบริการกลับมาได้ภายใน RTO และจุดข้อมูลที่กู้คืนสอดคล้องกับ RPO

3. **ข้อบกพร่องได้รับการแก้ไข:** ผลทดสอบซ้ำครอบคลุมระบบและสถานการณ์ที่กำหนด และไม่พบข้อบกพร่องสำคัญในขอบเขตนั้น

4. **ประเมินความเสี่ยงใหม่จากหลักฐาน:** โอกาสเกิดลดเป็น 2 และผลกระทบลดเป็น 4 ตามเกณฑ์และสมมติฐานที่บันทึก ทำให้ความเสี่ยงคงเหลือเป็น **2 × 4 = 8 ระดับปานกลาง**

5. **มีหลักฐานการตัดสินใจ:** รายงานและบันทึกการตัดสินใจแสดงการยกระดับ การอนุมัติทรัพยากร และผลติดตามครบถ้วน

กรณีนี้แสดงความเชื่อมโยงระหว่างข้อมูล การตัดสินใจ การดำเนินมาตรการ และผลต่อความเสี่ยง อย่างไรก็ตาม ต้องติดตามต่อว่าผลยังคงอยู่เมื่อใช้งานจริง และไม่ใช้ร้อยละการติดตั้งหรือการทดสอบครั้งเดียวเป็นข้อสรุปว่าความเสี่ยงทั้งหมดได้รับการจัดการแล้ว

4.14.3 การตรวจสอบความพร้อมก่อนประกาศใช้และการทบทวนกรอบ (Pre-issuance Readiness and Framework Review) ก่อนประกาศใช้คู่มือ ให้หน่วยงานเจ้าของเอกสารตรวจสอบความพร้อมดังต่อไปนี้

1. เกณฑ์กลางและหลักฐานอนุมัติ (Common Criteria and Approval Evidence): ตารางระดับความเสี่ยง เกณฑ์ Override กรอบ RA/RT และระยะเวลารายงาน ต้องมีสถานะการอนุมัติชัดเจน หากได้รับอนุมัติแล้วให้ระบุเอกสารอ้างอิง หากยังเป็นข้อเสนอให้ดำเนินการตามอำนาจก่อนใช้บังคับ

2. อำนาจยอมรับและตัดสินใจ (Acceptance and Decision Authority): ตรวจให้ตรงกับกฎหมาย ข้อบังคับ กฎบัตร และคำสั่งมอบอำนาจ คู่มือไม่ให้อำนาจเพิ่มเติมโดยตัวเอง

3. เกณฑ์ผลกระทบเฉพาะมิติ (Dimension-specific Impact Criteria): ตรวจฐานคำนวณ หน่วยวัด ช่วงคะแนน และความสอดคล้องกับฐานะการเงิน ข้อกำหนดเฉพาะ แผนฉุกเฉิน และบริบท ก่อนอนุมัติใช้

4. โครงสร้างและสายการรายงาน (Governance Structure and Reporting Routes): ตรวจชื่อคณะกรรมการ บทบาท และผู้รับรายงานให้ตรงกับเอกสารที่มีผลใช้บังคับ

5. ความสอดคล้องทั้งเล่ม (Manual-wide Consistency): ตรวจคำศัพท์ รหัส S O F C D สูตรและระดับคะแนน เลขหัวข้อ ตาราง ภาพ แบบฟอร์ม การอ้างข้ามข้อ และรอบรายงานให้สอดคล้องกับภาคผนวก

6. ความชัดเจนของตัวอย่าง (Illustrative Example Status): ระบุตัวอย่างสมมติให้ชัดเจน และแยกจากผลจริง เกณฑ์ หรือการมอบหมายที่ได้รับอนุมัติ

7. การควบคุมเอกสาร (Document Control): กำหนดเจ้าของเอกสาร เลขที่เอกสาร ฉบับ วันที่อนุมัติ วันที่มีผล ผู้อนุมัติ รอบทบทวน และประวัติการแก้ไข พร้อมจัดการฉบับที่ยกเลิก

หากข้อความในคู่มือขัดกับกฎหมายหรือข้อบังคับที่มีผลใช้บังคับ ให้ยึดกฎหมายหรือข้อบังคับนั้น และเสนอปรับปรุงคู่มือโดยเร็ว ส่วนข้อกำหนดเฉพาะด้านที่ใช้ร่วมกันได้ ให้ปฏิบัติให้ครบถ้วน โดยใช้เกณฑ์หรือระยะเวลาที่เข้มงวดกว่าเมื่อเกี่ยวข้อง ให้ทบทวนกรอบอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อยุทธศาสตร์ โครงสร้าง กฎหมาย มาตรฐาน ระบบงาน หรือบริบทความเสี่ยงเปลี่ยนแปลงอย่างมีนัยสำคัญ พร้อมใช้ผลการทบทวนปรับปรุงคู่มือ เครื่องมือ และการถ่ายทอดแนวทางไปสู่ส่วนงาน

ส่วนที่ 5

การกำหนดระดับความเสี่ยงที่ยอมรับได้ ตัวชี้วัดความเสี่ยง และเกณฑ์การตัดสินใจ

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

ส่วนนี้อธิบายการกำหนดและใช้กรอบการยอมรับความเสี่ยง ตัวชี้วัด และเงื่อนไขการตอบสนอง เพื่อให้มหาวิทยาลัยและส่วนงานสามารถตอบคำถามสำคัญได้ว่า ยินดีรับความเสี่ยงประเภทใดและเพียงใด ใช้ข้อมูลใดติดตาม ใครต้องดำเนินการ และเมื่อใดต้องรายงานหรือยกระดับ กรอบดังกล่าวต้องเชื่อมโยงกับวัตถุประสงค์และอำนาจตัดสินใจ โดยใช้ร่วมกับกระบวนการในส่วนที่ 4 และหลักการยอมรับกับการยกระดับความเสี่ยงในส่วนที่ 3

5.1 หลักการและวัตถุประสงค์ (Principles and Objectives)

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) และตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) เป็นเครื่องมือเชื่อมโยงยุทธศาสตร์ วัตถุประสงค์ ความเสี่ยง การตัดสินใจ และการติดตามผล โดยมีวัตถุประสงค์ดังต่อไปนี้

1. **กำหนดท่าทีต่อความเสี่ยง:** ระบุประเภทและระดับความเสี่ยงที่มหาวิทยาลัยยินดีรับเพื่อบรรลุวัตถุประสงค์
2. **สนับสนุนการตัดสินใจ:** ใช้ประกอบการเลือกยุทธศาสตร์ การลงทุน การอนุมัติโครงการ และการจัดสรรทรัพยากร
3. **สร้างการเตือนล่วงหน้า:** ตรวจพบการเปลี่ยนแปลงก่อนความเสี่ยงส่งผลกระทบอย่างมีนัยสำคัญ
4. **กำหนดการตอบสนองร่วมกัน:** เชื่อมโยงเกณฑ์สถานะ มาตรการ ผู้รับผิดชอบ เวลา และเส้นทางการรายงาน
5. **ควบคุมการยอมรับความเสี่ยง:** ป้องกันการตัดสินใจเกินอำนาจ เกินขีดความสามารถ หรือขัดต่อกฎหมายและข้อห้าม
6. **ใช้ข้อมูลประกอบทางเลือก:** พิจารณาประโยชน์ ต้นทุน สมมติฐาน และความไม่แน่นอนของทั้งภัยคุกคามและโอกาส

7. **กำหนดความรับผิดชอบ:** เชื่อมโยงบทบาทเจ้าของความเสี่ยง เจ้าของการควบคุม เจ้าของมาตรการ และเจ้าของข้อมูล

8. **บริหารภาพรวมความเสี่ยง:** พิจารณาความสัมพันธ์ ผลกระทบสะสม และการกระจุกตัวระหว่างส่วนงาน

RA/RT ต้องนำไปใช้ในการตัดสินใจและติดตามจริง พร้อมมีหลักฐานว่าการเข้าใกล้หรือเกินเกณฑ์นำไปสู่การดำเนินการอย่างไร ไม่กำหนดไว้เพื่อประกอบเอกสารเพียงอย่างเดียว

5.2 คำศัพท์และความสัมพันธ์ (Definitions and Relationships)

ตารางที่ 5-1 ***คำศัพท์และความหมายในการใช้งาน***

คำศัพท์	ความหมาย
ความสามารถในการรองรับความเสี่ยง (Risk Capacity)	ขีดความสามารถสูงสุดในการรองรับความเสี่ยงหรือผลกระทบ โดยพิจารณาทรัพยากร ภาระผูกพัน ความต่อเนื่อง และข้อจำกัดสำคัญ ทั้งนี้ ไม่เป็นอำนาจให้ฝ่าฝืนกฎหมาย
ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA)	ประเภทและระดับความเสี่ยงที่มหาวิทยาลัยยินดีรับในการดำเนินยุทธศาสตร์และบรรลุวัตถุประสงค์
ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT)	ขอบเขตความเบี่ยงเบนที่อนุญาตจากระดับหรือเป้าหมายที่กำหนด ซึ่งสอดคล้องกับ RA และอยู่ภายใต้เงื่อนไขการจัดการที่ได้รับอนุมัติ
ขีดจำกัดความเสี่ยง (Risk Limit)	ข้อจำกัดเชิงปฏิบัติสำหรับกิจกรรม การเปิดรับความเสี่ยง หรือทรัพยากร เช่น วงเงินลงทุนหรือเพดานการพึ่งพาคู่สัญญา โดยระบุผู้รับผิดชอบและการตอบสนองเมื่อเกินขีดจำกัด
ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI)	ตัววัดที่สะท้อนปัจจัยขับเคลื่อน การเปิดรับความเสี่ยง เหตุการณ์ ผลกระทบ หรือแนวโน้มความเสี่ยง เพื่อสนับสนุนการตอบสนองและการตัดสินใจ
จุดแจ้งเตือนหรือเงื่อนไขดำเนินการ (Trigger)	ค่า เหตุการณ์ หรือแนวโน้มที่กำหนดให้ต้องตรวจสอบ แจ้งเตือน ดำเนินมาตรการ หรือยกระดับ โดยเชื่อมโยงกับผู้รับผิดชอบและเวลา
ความเสี่ยงคงเหลือเป้าหมาย (Target Residual Risk)	ระดับความเสี่ยงที่คาดว่าจะเหลือหลังมาตรการเพิ่มเติมเกิดผลภายในเวลาที่กำหนด พร้อมสมมติฐานและวิธียืนยันผล
เหตุหรือพฤติกรรมที่ไม่ยอมรับ (Zero Tolerance Event/Behaviour)	เหตุหรือพฤติกรรมตามนโยบายที่มหาวิทยาลัยไม่อนุญาตให้กระทำเพิกเฉย หรือคงไว้โดยไม่ดำเนินการ ต้องตอบสนอง รายงาน และตรวจสอบตามข้อกำหนด

ความสัมพันธ์ในการใช้งาน (Operational Relationships)

- **Risk Capacity** แสดงข้อจำกัดของสิ่งที่มหาวิทยาลัยรองรับได้ ส่วน **RA** แสดงสิ่งที่มหาวิทยาลัยยินดีรับ ทั้งสองจึงไม่ใช่ค่าเดียวกัน
- **RT** กำหนดขอบเขตความเบี่ยงเบนที่อนุญาต ไม่ใช่ช่วงเฝ้าระวังโดยตัวเอง ช่วงเฝ้าระวังอาจกำหนดไว้ก่อนถึงขอบเขต RT
- **Risk Limit** ใช้ควบคุมกิจกรรมหรือการเปิดรับความเสี่ยงเฉพาะเรื่อง อาจช่วยให้ดำเนินงานภายใน RA/RT แต่ไม่จำเป็นต้องมีค่าเดียวกับ RT
- **KRI** ใช้ติดตามค่าจริง แนวโน้ม หรือค่าคาดการณ์เทียบกับเกณฑ์ที่เกี่ยวข้อง
- **Trigger** เชื่อมโยงผลการติดตามกับการดำเนินการ ผู้รับผิดชอบ ผู้รับรายงาน และเวลาตอบสนอง
- **Target Residual Risk** เป็นเป้าหมายในอนาคต ไม่ใช้แทนความเสี่ยงคงเหลือ ณ วันที่ประเมิน

RA ไม่ใช่ค่าเป้าหมายผลการดำเนินงานหรือ KPI แม้จะใช้ข้อมูลเดียวกันประกอบได้ ส่วนค่า KRI ที่เรียกว่า “ภายใน RA” เป็นเกณฑ์ปฏิบัติที่ถ่ายทอดจากถ้อยแถลง RA ไม่ได้แสดงว่าความเสี่ยงทั้งรายการอยู่ในกรอบโดยอัตโนมัติ

การอยู่ภายใน RT ไม่อนุญาตให้ละเว้นมาตรฐานหรือหน้าที่ตามกฎหมาย และการเกิน Risk Limit ไม่สามารถแก้ไขด้วยการอนุมัติย้อนหลัง หากขีดจำกัดนั้นเป็นข้อห้ามตามกฎหมายหรือเป็นเงื่อนไขที่ไม่มีอำนาจยกเว้น

5.3 หลักการกำหนดความสามารถในการรองรับความเสี่ยง (Risk Capacity Setting)

การกำหนด Risk Capacity ต้องใช้ข้อมูลเกี่ยวกับขีดความสามารถ ทรัพยากร และข้อจำกัดจริง โดยพิจารณาอย่างน้อยดังต่อไปนี้

1. **การเงินและภาระผูกพัน (Finance and Obligations):** สภาพคล่อง เงินสำรอง ภาระชำระ และแหล่งเงินที่เข้าถึงได้
2. **ชีวิต สุขภาพ และความปลอดภัย (Life, Health and Safety):** มาตรฐานการคุ้มครองและความพร้อมในการป้องกันกับตอบสนอง ไม่กำหนดเป็นจำนวนการเสียชีวิตหรือบาดเจ็บที่อนุญาต

3. **ความต่อเนื่องของพันธกิจ (Mission Continuity):** ระยะเวลาและระดับบริการที่สามารถรักษาได้เมื่อเกิดการหยุดชะงัก

4. **ข้อจำกัดทางกฎหมายและการกำกับดูแล (Legal and Regulatory Constraints)**

5. **ระบบ ข้อมูล และโครงสร้างพื้นฐาน (Systems, Data and Infrastructure):** ขีดความสามารถ ความพร้อมใช้ และการกู้คืน

6. **กำลังคนและสมรรถนะ (Workforce and Competencies)**

7. **ชื่อเสียง ความเชื่อมั่น และความชอบธรรม (Reputation, Trust and Legitimacy)**

8. **ข้อผูกพันต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder Commitments)**

9. **ความสามารถตอบสนองและฟื้นตัว (Response and Recovery Capability)**

10. **ความสัมพันธ์และผลกระทบพร้อมกัน (Dependencies and Concurrent Impacts):** เช่น รายได้ลดลงพร้อมกับค่าใช้จ่ายฟื้นฟูระบบเพิ่มขึ้น

ให้ระบุกรอบเวลา สมมติฐาน แหล่งข้อมูล และข้อจำกัด พร้อมพิจารณาสถานการณ์กดดันที่เหมาะสม ไม่กำหนด Risk Capacity จากระดับความเสี่ยงที่ผู้บริหารประสงค์จะรับ และไม่ใช้คะแนนจากตารางความเสี่ยงเพียงอย่างเดียวแทนการวิเคราะห์ขีดความสามารถ

ตัวอย่างด้านสภาพคล่อง: ประเมินเงินสดที่พร้อมใช้เทียบกับเงินเดือน ภาระผูกพัน ค่าใช้จ่ายจำเป็น และแหล่งเงินสำรองภายใต้สถานการณ์รายรับลดลง เพื่อพิจารณาจุดที่ไม่สามารถรักษาพันธกิจสำคัญได้ จากนั้นกำหนด RA/RT และจุดเตือนให้มีระยะห่างเพียงพอสำหรับการแก้ไข ไม่ใช้จำนวนวันเงินสดตัวเดียวเป็นข้อสรุปว่าเกิน Risk Capacity

ค่าทางการเงินบางชนิดยิ่งต่ำยิ่งเสี่ยง ขณะที่การเปิดรับความเสี่ยงบางชนิดยิ่งสูงยิ่งเสี่ยง จึงต้องอธิบายทิศทางและขอบเขตให้ชัดเจน ไม่เรียงค่าตัวเลขของ Risk Capacity, RA และ RT ในลำดับเดียวกันทุกกรณี

5.4 ระดับความเสี่ยงที่ยอมรับได้ของมหาวิทยาลัย (University Risk Appetite)

5.4.1 ระดับและลักษณะของการยอมรับความเสี่ยง (Appetite Levels and Characteristics)

ตารางที่ 5-2 ***ระดับ RA และความหมาย***

ระดับ RA	ความหมายและเงื่อนไข
ไม่ยอมรับ (Zero)	ไม่อนุญาตให้กระทำ เพิกเฉย หรือคงเหตุหรือพฤติกรรมที่กำหนดไว้ ต้องป้องกัน ตรวจพบ รายงาน และจัดการ โดยไม่ได้หมายความว่าโอกาสเกิดเป็นศูนย์
ต่ำ (Low)	ยินดีรับความไม่แน่นอนหรือผลกระทบได้จำกัด ให้ความสำคัญกับการป้องกันและการควบคุม พร้อมหลักฐานยืนยันความเพียงพอ
ปานกลาง (Moderate)	ยินดีรับความไม่แน่นอนในขอบเขตที่กำหนดเมื่อมีเหตุผล คุณค่าหรือประโยชน์เหมาะสม และมีมาตรการติดตามกับตอบสนอง
สูง (High)	ยินดีรับความไม่แน่นอนมากขึ้นเพื่อสร้างคุณค่า โดยต้องมีเหตุผล ทางเลือก ขอบเขตควบคุม (Guardrails) และเงื่อนไขหยุด ไม่เกินขีดความสามารถหรือข้อจำกัดที่เกี่ยวข้อง
แตกต่างตามบริบท (Selective/Variable)	ลักษณะการกำหนด RA ที่แตกต่างตามกิจกรรม โครงการ หรือมิติผลกระทบ โดยต้องระบุระดับและเงื่อนไขของแต่ละบริบทให้ชัดเจน

ระดับ RA ในตารางเป็น **ท่าทีต่อการรับความเสี่ยง** ไม่ใช่ระดับคะแนนต่ำ ปานกลาง สูง และสูงมากจากสูตร L × I จึงไม่ใช้แทนกันโดยตรง

Selective/Variable ไม่ใช่ระดับที่อยู่เหนือหรือต่ำกว่า High เช่น อาจกำหนด RA ปานกลางต่อความไม่แน่นอนของผลวิจัย แต่ไม่ยอมรับการปลอมแปลงข้อมูลหรือการฝ่าฝืนจริยธรรมการวิจัย

5.4.2 กรอบเสนอระดับ RA ตามพันธกิจและประเด็นสำคัญ (Proposed Appetite by Mission and Key Topic) ตารางต่อไปนี้เป็น **กรอบเสนอเบื้องต้นสำหรับการพิจารณา** ไม่ใช่ข้อยืนยันว่าได้รับอนุมัติแล้ว และไม่ใช่การเพิ่มประเภทความเสี่ยงหลักนอกเหนือจาก S O F C D แต่เป็นการกำหนดท่าทีตามพันธกิจและมิติที่เกี่ยวข้อง

ตารางที่ 5-3 กรอบเสนอระดับความเสี่ยงที่ยอมรับได้

พันธกิจหรือประเด็น	ระดับ RA ที่เสนอ	ขอบเขตและเงื่อนไขสำคัญ
การจัดการศึกษาและคุณภาพบัณฑิต	**ต่ำ**	จำกัดความเสี่ยงต่อคุณภาพและความต่อเนื่องของการศึกษา พร้อมรักษามาตรฐานและสิทธิของผู้เรียน

พันธกิจหรือประเด็น	ระดับ RA ที่เสนอ	ขอบเขตและเงื่อนไขสำคัญ
		การทดลองรูปแบบการเรียนรู้ต้องมีการประเมินและติดตาม
การวิจัยและนวัตกรรม	**ปานกลาง**	รับความไม่แน่นอนของผลวิจัยหรือความสำเร็จของนวัตกรรมได้ในขอบเขตที่อนุมัติ โดยไม่อนุญาตการประพฤติมิชอบหรือฝ่าฝืนข้อกำหนดจริยธรรม
การเงินและสภาพคล่อง	**ต่ำสำหรับสภาพคล่องและภาระผูกพัน; ปานกลางสำหรับกิจกรรมลงทุนหรือสร้างรายได้บางประเภท**	ต้องแยกเกณฑ์ตามกิจกรรม ประเมินความคุ้มค่าและไม่ทำให้ความสามารถชำระภาระผูกพันหรือรักษาพันธกิจเกินขอบเขตที่อนุมัติ
กฎหมาย การทุจริต และจริยธรรม	**ไม่ยอมรับการกระทำผิดหรือเพิกเฉยต่อหน้าที่**	ไม่อนุญาตการทุจริต รับสินบน หรือฝ่าฝืนข้อห้าม การประเมินโอกาสเกิดการไม่ปฏิบัติตามกฎหมายยังต้องดำเนินการเพื่อกำหนดการป้องกันและตอบสนอง
ความมั่นคงปลอดภัยไซเบอร์และข้อมูลส่วนบุคคล	**ต่ำ**	กำหนดการควบคุมตามความสำคัญและความอ่อนไหวของข้อมูล เหตุรุนแรงต้องตอบสนองและรายงานทันที ไม่ถือว่าเหตุไซเบอร์หรือข้อมูลรั่วไหลทุกกรณีเป็น Zero Tolerance โดยอัตโนมัติ
ชื่อเสียงและความเชื่อมั่น	**ต่ำ**	จำกัดผลกระทบที่รุนแรงหรือยืดเยื้อ พร้อมการติดตามและสื่อสารที่ถูกต้อง ไม่ใช้การปกปิดข้อมูลหรือจำกัดการรายงานโดยสุจริตเป็นมาตรการรักษาชื่อเสียง
ชีวิต สุขภาพ และความปลอดภัย	**ต่ำมากต่อความเสี่ยงรุนแรงและไม่ยอมรับการละเลยหรือฝ่าฝืนมาตรการสำคัญ**	เหตุเสียชีวิต บาดเจ็บร้ายแรง หรือภัยคุกคามต่อชีวิตต้องตอบสนองและยกระดับทันที โดยไม่รอผลวินิจฉัยความรับผิด และไม่ตีความว่ามีจำนวนความสูญเสียที่อนุญาต
นวัตกรรมและการเปลี่ยนผ่านดิจิทัล	**ปานกลาง**	ทดลองได้ในขอบเขตที่อนุมัติ พร้อมโครงการนำร่อง การกำกับดูแลข้อมูลและ AI การตรวจสอบผล และเกณฑ์หยุดหรือย้อนกลับ
สิ่งแวดล้อมและความยั่งยืน	**ต่ำต่อผลกระทบสิ่งแวดล้อม; ปานกลางต่อ**	แยกความไม่แน่นอนของผลโครงการออกจากผลกระทบต่อสิ่งแวดล้อมและชุมชน ไม่อนุญาตการ

พันธกิจหรือประเด็น	ระดับ RA ที่เสนอ	ขอบเขตและเงื่อนไขสำคัญ
	ความไม่แน่นอนของโครงการพัฒนา	ฝ่าฝืนข้อกำหนด และต้องตอบสนองเร่งด่วนเมื่อเกิดผลกระทบรุนแรง

คำว่า “ต่ำมาก” ในประเด็นความปลอดภัยใช้แสดงความระมัดระวังภายใต้ระดับ **ต่ำ** ไม่ใช่ระดับ RA เพิ่มเติม ส่วนเหตุหรือพฤติกรรมที่จะกำหนดเป็น Zero Tolerance ต้องระบุขอบเขตในนโยบายให้ชัดเจน ไม่ใช้ความรุนแรงของผลกระทบเป็นข้อสรุปว่ามีผู้กระทำผิดโดยอัตโนมัติ

ระดับที่เสนอทั้งหมดต้องผ่านการกลั่นกรองและอนุมัติตามโครงสร้างและอำนาจที่มีผลใช้บังคับ โดยเสนอคณะกรรมการ ผู้บริหาร หรือสภามหาวิทยาลัยตามขั้นตอนที่เกี่ยวข้อง ก่อนถ่ายทอดเป็น RT ขีดจำกัด ตัวชี้วัด และเงื่อนไขตอบสนองของส่วนงาน

การอนุมัติ RA ไม่ทดแทนการอนุมัติโครงการ งบประมาณ หรือการยอมรับความเสี่ยงเฉพาะกรณี และไม่ให้อำนาจยกเว้นกฎหมายหรือข้อห้าม

5.5 การกำหนดระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance Setting)

ระดับความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance: RT) ต้องเชื่อมโยงกับกรอบระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และวัตถุประสงค์ โดยถ่ายทอดเป็นขอบเขตที่วัด ติดตาม และใช้ตัดสินใจได้ พร้อมกำหนดช่วงเฝ้าระวังและเงื่อนไขตอบสนองก่อนหรือเมื่อเกินขอบเขต ให้พิจารณาทิศทางของตัวชี้วัดดังต่อไปนี้

1. **ค่ายิ่งสูงยิ่งดี (Higher Is Better):** ค่าที่ลดลงสะท้อนความเสี่ยงเพิ่มขึ้น เช่น สัดส่วนรายได้ที่ไม่ใช่ค่าเล่าเรียน ความพร้อมของบุคลากร หรืออัตราการแก้ไขช่องโหว่ตามกำหนด
2. **ค่ายิ่งต่ำยิ่งดี (Lower Is Better):** ค่าที่เพิ่มขึ้นสะท้อนความเสี่ยงเพิ่มขึ้น เช่น จำนวนข้อบกพร่องสำคัญที่ค้าง ระยะเวลาหยุดชะงัก หรือมูลค่าความเสียหาย
3. **ค่าต้องอยู่ในช่วง (Within a Defined Range):** ค่าที่ต่ำหรือสูงนอกช่วงอาจเพิ่มความเสี่ยง เช่น ภาระงานหรืออัตราส่วนทางการเงินบางประเภท โดยต้องกำหนดขอบเขตและการตอบสนองทั้งสองด้าน
4. **เหตุหรือพฤติกรรมที่ไม่ยอมรับ (Zero Tolerance):** ไม่มีช่วงที่อนุญาตให้กระทำหรือคงเหตุไว้ ต้องตอบสนองเมื่อพบเหตุหรือข้อมูลที่มีมูลตามเงื่อนไข ไม่รอการยืนยันความผิดให้แล้วเสร็จ

ทุกเกณฑ์ต้องระบุช่วงเวลาที่วัด วันหรือจุดตรวจสอบ หน่วยวัด และเงื่อนไขที่ขอบเขตให้ชัดเจน ช่วงเฝ้าระวังไม่ใช่ RT โดยตัวเอง แต่เป็นช่วงสถานะที่กำหนดเพื่อให้ดำเนินการก่อนเกินขอบเขต RT

ตัวอย่างความเชื่อมโยงระหว่างวัตถุประสงค์ ตัวชี้วัด เกณฑ์ และการตอบสนอง

ตัวเลขในตารางเป็นตัวอย่างหรือกรอบเสนอ ต้องตรวจสอบข้อมูลฐาน ความเหมาะสม และอนุมัติตามอำนาจก่อนใช้ ไม่ถือเป็นเกณฑ์ที่มหาวิทยาลัยอนุมัติแล้ว

วัตถุประสงค์หรือความเสี่ยง	ตัวชี้วัดตัวอย่าง	เกณฑ์ปฏิบัติที่เชื่อมโยงกับ RA	ช่วงเฝ้าระวังที่ยังไม่เกิน RT	เกิน RT หรือเข้าเงื่อนไขยกระดับ	การตอบสนอง
ความยั่งยืนทางการเงิน	สัดส่วนรายได้ที่ไม่ใช่ค่าเล่าเรียน (Non-tuition Revenue Ratio)	ตั้งแต่ร้อยละ 30 ขึ้นไป	ตั้งแต่ร้อยละ 25 แต่ต่ำกว่าร้อยละ 30	ต่ำกว่าร้อยละ 25 ณ จุดตรวจสอบที่กำหนด	วิเคราะห์แหล่งรายได้และประมาณการ จัดทำแผนแก้ไขรายได้ และยกระดับเมื่อเกินเกณฑ์
การรักษาสภาพคล่อง	จำนวนวันที่ดำเนินงานได้ด้วยเงินสดที่พร้อมใช้ (Days Cash on Hand)	ตั้งแต่ 180 วันขึ้นไป	ตั้งแต่ 120 วัน แต่ต่ำกว่า 180 วัน โดยอาจแบ่งช่วงเตือนย่อย	ต่ำกว่า 120 วัน	ทบทวนกระแสเงินสด ดำเนินแผนสภาพคล่อง และยกระดับ หากคาดว่าจะชำระภาระจำเป็นไม่ได้ให้ตอบสนองเร่งด่วน
ความพร้อมของบุคลากร	ร้อยละบุคลากรกลุ่มเป้าหมายที่ผ่านเกณฑ์สมรรถนะหลังพัฒนาทักษะ (Competency	ตั้งแต่ร้อยละ 85 ขึ้นไป	ตั้งแต่ร้อยละ 75 แต่ต่ำกว่าร้อยละ 85	ต่ำกว่าร้อยละ 75	วิเคราะห์ช่องว่างพัฒนากลุ่มที่ยังไม่ผ่าน ประเมินซ้ำและรายงานผู้บริหารตามเกณฑ์

วัตถุประสงค์หรือความเสี่ยง	ตัวชี้วัดตัวอย่าง	เกณฑ์ปฏิบัติที่เชื่อมโยงกับ RA	ช่วงเฝ้าระวังที่ยังไม่เกิน RT	เกิน RT หรือเข้าเงื่อนไขยกระดับ	การตอบสนอง
	Achievement Rate)				
ความพร้อมด้านไซเบอร์และข้อมูลส่วนบุคคล	ร้อยละบุคลากรกลุ่มเป้าหมายที่ผ่านเกณฑ์ความรู้และการปฏิบัติตามบทบาท	ตั้งแต่ร้อยละ 90 ขึ้นไป	ตั้งแต่ร้อยละ 80 แต่ต่ำกว่าร้อยละ 90	ต่ำกว่าร้อยละ 80	แก้ไขช่องว่างและทดสอบซ้ำ โดยติดตามการควบคุมทางเทคนิคและกระบวนงานร่วมด้วย
การป้องกันการทุจริต	จำนวนกรณีทุจริตที่ยืนยันข้อเท็จจริง ใช้ติดตามผลร่วมกับข้อมูลการตรวจพบ	0 กรณี	ไม่มีช่วงที่อนุญาต	พบเหตุหรือข้อมูลที่มีมูล ไม่ต้องรอให้ยืนยันครบ 1 กรณี	ระงับหรือจำกัดความเสียหาย รักษาหลักฐาน รายงาน และตรวจสอบตามแนวทาง Zero Tolerance

สัดส่วนรายได้ต้องระบุฐานรายได้และรายการที่รวม ส่วนตัวชี้วัดบุคลากรต้องกำหนดกลุ่มเป้าหมายและเกณฑ์สมรรถนะล่วงหน้า ไม่ใช้จำนวนผู้เข้าร่วมอบรมแทนความสามารถในการปฏิบัติงาน

กรณีค่าคาดการณ์หรือแนวโน้มชี้ว่าจะเกิน RT ก่อนรอบถัดไป ให้ดำเนินการตามจุดเตือนล่วงหน้า ไม่จำเป็นต้องรอค่าจริงเกินเกณฑ์ ส่วนการอยู่ภายในเกณฑ์ตัวชี้วัดหนึ่งตัวไม่ยืนยันว่าความเสี่ยงทั้งรายการอยู่ในกรอบ RA/RT

5.6 การกำหนดและบริหารตัวชี้วัดความเสี่ยงที่สำคัญ (KRI Design and Management)

KRI ต้องช่วยอธิบายการเปลี่ยนแปลงของปัจจัยเสี่ยง การเปิดรับความเสี่ยง เหตุการณ์ หรือผลกระทบ และเชื่อมโยงกับการดำเนินการได้ ไม่ใช้ตัวชี้วัดกิจกรรมที่ไม่มีความสัมพันธ์ชัดเจนกับความเสี่ยง

5.6.1 องค์ประกอบของตัวชี้วัด (Indicator Specifications) KRI แต่ละตัวต้องมีอย่างน้อยดังต่อไปนี้

1. ชื่อ นิยาม และวัตถุประสงค์ (Name, Definition and Purpose)
2. ความเสี่ยง สาเหตุ หรือปัจจัยขับเคลื่อนที่เชื่อมโยง (Related Risk, Cause or Driver)
3. ลักษณะตัวชี้วัดนำหรือตาม (Leading or Lagging Indicator)
4. สูตร หน่วยวัด และทิศทางความเสี่ยง (Formula, Unit and Risk Direction)
5. ขอบเขตข้อมูลและช่วงเวลาที่วัด (Data Scope and Measurement Period)
6. แหล่งข้อมูลและวิธีตรวจสอบ (Data Source and Validation Method)
7. เจ้าของข้อมูล (Data Owner)
8. ความถี่จัดเก็บและกำหนดเวลารายงาน (Collection Frequency and Reporting Deadline)
9. ค่าฐานพร้อมวันที่อ้างอิง (Baseline and Reference Date)
10. เกณฑ์ที่เชื่อมโยงกับ RA/RT และช่วงสถานะ (RA/RT-linked Thresholds and Status Bands)
11. จุดแจ้งเตือนและเงื่อนไขตอบสนอง (Trigger and Action)
12. ผู้รับผิดชอบตอบสนอง ผู้รับรายงาน และผู้มีอำนาจ (Action Owner, Recipient and Decision Authority)
13. หลักฐาน วันที่ปรับปรุง และข้อจำกัดข้อมูล (Evidence, Update Date and Limitations)

ต้องกำหนดวิธีจัดการตัวหารเป็นศูนย์ ข้อมูลขาดหาย และข้อมูลที่ยังไม่ยืนยัน ไม่แสดงสถานะปกติโดยอัตโนมัติ หากเปลี่ยนนิยาม สูตร หรือขอบเขต ต้องบันทึกฉบับและพิจารณาว่าค่าเดิมกับค่าใหม่ยังเปรียบเทียบกันได้หรือไม่

5.6.2 ตัวอย่างตัวชี้วัดที่มีรายละเอียดครบถ้วน (Complete Indicator Example)

ตัวอย่างตัวชี้วัดการติดตั้งชุดปรับปรุงความมั่นคงปลอดภัยข้อมูลและเกณฑ์ต่อไปนี้เป็นตัวอย่างสมมติ

รายการ	ตัวอย่าง
ความเสี่ยง (Risk)	ระบบสารสนเทศสำคัญอาจถูกโจมตีจากช่องโหว่ที่ยังไม่ได้รับการแก้ไข ส่งผลต่อข้อมูลและความต่อเนื่อง

รายการ	ตัวอย่าง
ชื่อตัวชี้วัด (Indicator Name)	ร้อยละระบบสำคัญที่ติดตั้งชุดปรับปรุงความมั่นคงปลอดภัย (Security Patch) ครบรายการที่ถึงกำหนดภายในเวลาที่กำหนด
ลักษณะ (Type)	ตัวชี้วัดนำ (Leading Indicator) และตัวชี้วัดการควบคุมที่สำคัญ (KCI) โดยใช้ผลการควบคุมเป็นข้อมูลประกอบการเปิดรับความเสี่ยง
สูตร (Formula)	จำนวนระบบสำคัญที่ติดตั้งครบรายการที่ถึงกำหนดภายในเวลา ÷ จำนวนระบบสำคัญที่มีรายการถึงกำหนดในรอบรายงาน × 100
ขอบเขตและวิธีนับ (Scope and Counting Rules)	กำหนดรายการระบบและเวลาตามระดับช่องโหว่ ระบบหนึ่งถือว่าผ่านเมื่อดำเนินการครบรายการที่ถึงกำหนด หากไม่มีระบบถึงกำหนดให้แสดง “ไม่เกี่ยวข้องในรอบนี้”
หน่วยและทิศทาง (Unit and Direction)	ร้อยละ ค่ายิ่งต่ำสะท้อนความเสี่ยงเพิ่มขึ้น
แหล่งข้อมูล (Data Source)	ระบบบริหารช่องโหว่ (Vulnerability Management System) รายงานติดตั้ง และผลตรวจสอบหลังติดตั้ง
เจ้าของข้อมูล (Data Owner)	ผู้รับผิดชอบข้อมูลระบบและช่องโหว่ที่ได้รับมอบหมาย
ความถี่ (Frequency)	สรุปรายเดือน และติดตามรายการวิกฤตตามกำหนดเฉพาะโดยไม่รอสิ้นเดือน
ค่าฐาน (Baseline)	สมมติร้อยละ 88 ในรอบอ้างอิงที่ระบุ พร้อมจำนวนระบบและขอบเขตข้อมูล
เกณฑ์ปฏิบัติที่เชื่อมโยงกับ RA	ตั้งแต่ร้อยละ 95 ขึ้นไป
ช่วงเฝ้าระวัง (Warning Band)	ตั้งแต่ร้อยละ 90 แต่ต่ำกว่าร้อยละ 95
ขอบเขต RT (RT Boundary)	ไม่ต่ำกว่าร้อยละ 90
เกิน RT (RT Breach)	ต่ำกว่าร้อยละ 90
จุดแจ้งเตือนและการตอบสนอง (Trigger and Action)	ต่ำกว่าร้อยละ 95 ให้เร่งแก้ไข ต่ำกว่าร้อยละ 90 ให้จัดทำมาตรการแก้ไขและยกระดับภายใน 3 วันทำการ หรือเร็วกว่านั้นตามความรุนแรง
เงื่อนไขเร่งด่วน (Urgent Conditions)	พบช่องโหว่วิกฤตที่เปิดรับการโจมตีหรือมีหลักฐานการโจมตี ให้ตอบสนองตามเกณฑ์เฉพาะ แม้ค่ารวมผ่านร้อยละ 95
ผู้รับรายงาน (Recipients)	เจ้าของความเสี่ยง ผู้บริหารที่กำกับ หน่วยงานเฉพาะด้าน และหน่วยบริหารความเสี่ยงตามสายรายงาน
หลักฐาน (Evidence)	บันทึกติดตั้ง รายงานช่องโหว่ รายการค้าง เหตุผลข้อยกเว้น และมาตรการชดเชย

ควรใช้ตัวชี้วัดนำร่วมกับตัวชี้วัดตามตามความจำเป็น เช่น

- **ตัวชี้วัดนำ (Leading KRI):** จำนวนช่องโหว่รุนแรงในระบบสำคัญที่ค้างเกินกำหนด
- **ตัวชี้วัดตาม (Lagging KRI):** จำนวนเหตุโจมตีที่ทำให้บริการหยุดชะงักหรือข้อมูลถูกเปิดเผย โดยกำหนดนิยามความรุนแรงและช่วงเวลาชัดเจน

ค่าร้อยละรวมต้องพิจารณาร่วมกับความสำคัญของระบบและรายการค้าง ไม่ใช้กลบความเสี่ยงจากช่องโหว่วิกฤตเพียงรายการเดียว

5.7 สถานะตัวชี้วัดและเกณฑ์แจ้งเตือน (KRI Status and Trigger Criteria)

ให้ใช้สถานะ 4 ระดับเพื่อสื่อสารความเร่งด่วนของตัวชี้วัด โดยกำหนดเกณฑ์และการตอบสนองล่วงหน้าตามอำนาจ สถานะสีของ KRI ต้องแยกจากระดับความเสี่ยงตามคะแนน L × I และแสดงทั้งข้อความกับสีเพื่อให้เข้าใจตรงกัน

ตารางที่ 5-4 สถานะ KRI และการดำเนินการขั้นต่ำ

สถานะ	ความหมาย	การดำเนินการขั้นต่ำ
เขียว — ตามเกณฑ์ (Green)	ค่าตัวชี้วัดเป็นไปตามเกณฑ์ปฏิบัติที่เชื่อมโยงกับ RA และไม่พบเงื่อนไขเร่งด่วนของตัวชี้วัดนั้น	รักษาการควบคุมและติดตามตามรอบ ไม่สรุปว่าความเสี่ยงทั้งหมดหมดไป
เหลือง — เฝ้าระวัง (Yellow)	เบี่ยงเบนจากเกณฑ์ปฏิบัติ แต่ยังไม่เกินขอบเขต RT หรือเข้าเงื่อนไขเตือนล่วงหน้าที่กำหนด	วิเคราะห์สาเหตุ ดำเนินมาตรการภายในอำนาจ และเพิ่มความถี่ติดตามตามความจำเป็น
ส้ม — ต้องแก้ไขและยกระดับ (Orange)	เกิน RT หรือเข้าเงื่อนไขจากแนวโน้ม/ค่าคาดการณ์ที่กำหนดให้ตอบสนองระดับนี้ โดยยังไม่เข้าเกณฑ์แดง	จัดทำมาตรการแก้ไข รายงานผู้บริหารตามกำหนด และทบทวนความเสี่ยงคงเหลือ
แดง — เร่งด่วน (Red)	เข้าเงื่อนไขวิกฤต เหตุ Zero Tolerance ภัยคุกคามรุนแรง หรือเกินขีดจำกัดที่กำหนดให้ตอบสนองเร่งด่วน	คุ้มครองและจำกัดความเสียหาย แจ้งผู้มีอำนาจทันที และดำเนินการตามแผนเฉพาะ

การเกิน Risk Limit ต้องดำเนินการตามข้อกำหนดของขีดจำกัดนั้น ไม่ถือว่าทุกกรณีเป็นเหตุวิกฤตโดยอัตโนมัติ ส่วนการใช้แนวโน้มเสื่อมลงต้องระบุเงื่อนไข เช่น จำนวนรอบ ความเร็วในการ

เปลี่ยนแปลง หรือค่าคาดการณ์ ไม่กำหนดสีจากดุลยพินิจย้อนหลังเมื่อเห็นผลแล้ว ตัวชี้วัดบางตัวอาจมีเพียงบางสถานะ เช่น ตัวชี้วัดเหตุ Zero Tolerance อาจไม่มีช่วงเหลืองหรือส้ม ไม่จำเป็นต้องสร้างช่วงตัวเลขให้ครบ 4 สี หากไม่สอดคล้องกับลักษณะความเสี่ยง หากยังไม่มีข้อมูล ข้อมูลล้าสมัย หรืออยู่ระหว่างตรวจสอบ ให้แสดง **"ยังไม่สามารถประเมินสถานะ (Not Assessable)"** แยกจากสถานะสีทั้ง 4 พร้อมผู้รับผิดชอบและกำหนดส่งข้อมูล หากการขาดข้อมูลเป็นเงื่อนไขเตือนสำคัญ ให้ดำเนินการตาม Trigger ที่กำหนดไว้

การพิจารณาตัวชี้วัดหลายตัวร่วมกัน (Multiple-indicator Assessment) เมื่อ KRI ของความเสี่ยงเดียวกันมีสถานะแตกต่างกัน ให้แสดงค่ารายตัวและพิจารณาสัญญาณที่รุนแรงที่สุดร่วมกับความสำคัญ แนวโน้ม และคุณภาพข้อมูล โดยไม่ใช้ค่าเฉลี่ยเพื่อลดทอนสัญญาณสำคัญ หากกำหนดสถานะสรุป ต้องมีหลักเกณฑ์การรวมที่ชัดเจนและได้รับความเห็นชอบ การมีตัวชี้วัดหนึ่งตัวเป็นสีแดงต้องไม่ถูกกลบด้วยตัวอื่นที่เป็นสีเขียว และไม่ทำให้ความเสี่ยงเป็น Enterprise Risk หรือเปลี่ยนคะแนน L × I โดยอัตโนมัติ แต่ต้องนำไปพิจารณาการตอบสนอง การประเมินใหม่ และการยกระดับตามข้อกำหนด

5.8 ความเชื่อมโยงระหว่างกรอบการยอมรับความเสี่ยงกับตารางประเมินระดับความเสี่ยง (RA/RT and Risk Matrix Alignment)

ตารางประเมินระดับความเสี่ยง กรอบ RA/RT และ KRI มีหน้าที่ต่างกัน แต่ต้องใช้ร่วมกันในการตัดสินใจ ดังนี้

- **ตารางประเมินระดับความเสี่ยง (Risk Matrix):** ใช้คะแนนโอกาสเกิดและผลกระทบประเมินระดับความเสี่ยงและประกอบการจัดลำดับความสำคัญ
- **กรอบ RA/RT:** กำหนดท่าทีและขอบเขตการยอมรับ พร้อมเงื่อนไขการตอบสนอง
- **ตัวชี้วัดความเสี่ยงที่สำคัญ (KRI):** ติดตามค่าจริง แนวโน้ม และสัญญาณการเปลี่ยนแปลงระหว่างรอบประเมิน
- **เกณฑ์ยกระดับเป็นกรณีพิเศษ (Override Criteria):** กำหนดการตอบสนองที่เข้มงวดขึ้นเมื่อคะแนนเพียงอย่างเดียวไม่สะท้อนความสำคัญหรือความเร่งด่วนเพียงพอ

คะแนนต่ำไม่หมายความว่ายอมรับได้เสมอ หากขัดต่อกฎหมาย เกินกรอบที่เกี่ยวข้อง หรือเข้าเกณฑ์ Zero Tolerance ส่วนคะแนนสูงไม่หมายความว่าต้องยุติกิจกรรมทุกกรณี แต่ต้องจัดการรายงาน และพิจารณาตามอำนาจ

ตารางที่ 5-7 เกณฑ์ระดับความเสี่ยงตามคะแนนโอกาสเกิด × ผลกระทบ

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

ให้ใช้เกณฑ์เดียวกับข้อ 4.8.5 อย่างสอดคล้องกันทั้งทะเบียน แบบฟอร์ม และรายงาน โดยระดับ RA ไม่ใช่ระดับคะแนนจากตารางนี้ และสถานะสีของ KRI ไม่เปลี่ยนคะแนน L × I โดยอัตโนมัติ เมื่อเครื่องมือให้สัญญาณต่างกัน ให้รักษาผลแต่ละรายการไว้ และใช้เงื่อนไขการตอบสนองที่เข้มงวดที่สุดที่เกี่ยวข้องเป็นฐานการดำเนินการ พร้อมตรวจสอบสาเหตุของความแตกต่าง ไม่ปรับคะแนนหรือเกณฑ์เพื่อทำให้ผลตรงกันโดยไม่มีหลักฐาน

ตัวอย่าง: ความเสี่ยงไซเบอร์มีความเสี่ยงคงเหลือ 9 คะแนน ระดับปานกลาง แต่พบเหตุข้อมูลสำคัญรั่วไหลที่เข้าเกณฑ์รายงานเร่งด่วน ต้องแจ้งและตอบสนองทันที ไม่รอรอบไตรมาส ส่วนการจัดเป็น Zero Tolerance ต้องพิจารณาตามขอบเขตนโยบาย และประเมินความเสี่ยงในอนาคตใหม่จากข้อมูลเหตุการณ์นั้น

5.9 เกณฑ์เหตุที่ไม่ยอมรับและการยกระดับเป็นกรณีพิเศษ (Zero Tolerance and Override Criteria)

5.9.1 เหตุหรือพฤติกรรมที่ไม่ยอมรับ (Zero Tolerance Events and Behaviours) มหาวิทยาลัยไม่อนุญาตให้กระทำ เพิกเฉย ปกปิด หรือคงเหตุและพฤติกรรมที่นโยบายกำหนดไว้โดยไม่จัดการ เช่น

1. การทุจริต การรับสินบน หรือการใช้ทรัพย์สินโดยมิชอบ
2. การฝ่าฝืนกฎหมายหรือข้อห้ามโดยเจตนา
3. การละเลยหรือฝ่าฝืนมาตรการคุ้มครองชีวิตและความปลอดภัยที่สำคัญ
4. การล่วงละเมิดหรือคุกคามทางเพศตามขอบเขตที่นโยบายกำหนด
5. การเลือกปฏิบัติหรือการละเมิดสิทธิมนุษยชน

6. การปลอมแปลงข้อมูล ผลงาน หรือการประพฤติมิชอบทางการวิจัย

7. การนำข้อมูลไปใช้หรือเปิดเผยโดยมิชอบตามข้อห้ามที่เกี่ยวข้อง

8. การปกปิด ทำลายหลักฐาน หรือรายงานข้อมูลอันเป็นเท็จต่อผู้กำกับดูแล

รายการนี้เป็นกรอบสำหรับตรวจสอบกับนโยบายและข้อกำหนดที่มีผลใช้บังคับ ไม่ใช้จำกัดการตอบสนองต่อเหตุอื่นที่กฎหมายกำหนดให้ต้องดำเนินการ

เมื่อพบเหตุหรือข้อมูลที่มีมูล ให้คุ้มครองผู้ได้รับผลกระทบ ระงับหรือจำกัดความเสียหาย รักษาหลักฐาน รายงาน และตรวจสอบข้อเท็จจริงโดยไม่ชักช้า การดำเนินการคุ้มครองไม่ต้องรอข้อยุติความผิด แต่การวินิจฉัยและดำเนินการต่อบุคคลต้องเป็นไปตามกฎหมายและหลักความเป็นธรรม Zero Tolerance ไม่ได้หมายความว่าโอกาสเกิดเหตุเป็นศูนย์ และไม่เป็นเหตุให้ปกปิดข้อมูลเพื่อให้รายงานแสดงว่าไม่มีเหตุเกิดขึ้น

5.9.2 เหตุรุนแรงและเกณฑ์ยกระดับ (Severe Events and Escalation Criteria) เหตุเสียชีวิต บาดเจ็บร้ายแรง ภัยคุกคามต่อชีวิต หรือเหตุละเมิดข้อมูลที่มีผลกระทบรุนแรง ต้องตอบสนองและรายงานเร่งด่วนตามแผนเฉพาะ ไม่รอพิจารณาว่าเกิดจากการละเลยหรือเข้าเกณฑ์ Zero Tolerance หรือไม่ ให้ใช้เกณฑ์เพิ่มเติมดังต่อไปนี้

1. ผลกระทบระดับ 5: ตอบสนองอย่างน้อยเทียบเท่าความเสี่ยงระดับสูง แม้คะแนนรวมต่ำกว่า 10 โดยคงคะแนนตามข้อเท็จจริง

2. เหตุ Zero Tolerance: ตอบสนองและยกระดับเทียบเท่าระดับสูงมากทันที โดยไม่ต้องเปลี่ยนคะแนนให้เป็น 16–25

3. KRI เกิน RT หรือ Risk Limit: ดำเนินการตามเงื่อนไขของตัวชี้วัดหรือขีดจำกัดนั้น ไม่ถือว่าการเกินทุกกรณีเป็นเหตุวิกฤตโดยอัตโนมัติ

4. ผลกระทบข้ามส่วนงานหรือเชิงยุทธศาสตร์: ประสานและเสนอการตัดสินใจระดับมหาวิทยาลัยตามความจำเป็น

5. การควบคุมสำคัญไม่ทำงาน: ประเมินผลต่อการเปิดรับความเสี่ยง กำหนดมาตรการระหว่างรอ และยกระดับตามความรุนแรง

6. เกินอำนาจหรือขีดความสามารถ: เสนอผู้มีอำนาจจัดสรรทรัพยากรหรือสั่งการ

7. ข้อกำหนดเฉพาะเข้มงวดกว่า: ปฏิบัติตามกฎหมาย แผน และช่องทางที่เกี่ยวข้อง

การใช้ Override ต้องบันทึกเหตุผล หลักฐาน ผู้พิจารณา ระดับการตอบสนอง มาตรการ และกำหนดทบทวน แยกจากระดับตามคะแนน ส่วนการบรรจุเป็นความเสี่ยงระดับมหาวิทยาลัยต้องผ่านการพิจารณาตามอำนาจ ไม่เกิดขึ้นโดยอัตโนมัติจากการยกระดับ

5.10 อำนาจการยอมรับความเสี่ยง (Risk Acceptance Authority)

การยอมรับความเสี่ยงต้องใช้ความเสี่ยงคงเหลือ ณ วันที่ตัดสินใจ ร่วมกับ RA/RT ประสิทธิผลของการควบคุม ข้อจำกัดตามกฎหมาย และอำนาจที่ได้รับมอบหมาย ความเสี่ยงโดยธรรมชาติใช้เป็นข้อมูลประกอบได้ แต่ไม่ใช้แทนระดับปัจจุบัน และห้ามใช้ความเสี่ยงคงเหลือเป้าหมายเสมือนเป็นผลที่เกิดขึ้นแล้ว ให้ยึดข้อ 3.9 เป็นหลัก โดยตารางต่อไปนี้เป็นกรอบสรุปข้อเสนอ ไม่ให้อำนาจเพิ่มเติมและต้องตรวจสอบกับเอกสารมอบอำนาจก่อนใช้

ตารางที่ 5-6 ***กรอบอำนาจยอมรับความเสี่ยงคงเหลือ***

ระดับ	กรอบผู้มีอำนาจที่เสนอ	เงื่อนไขสำคัญ
ต่ำ 1–4 (L)	เจ้าของความเสี่ยงหรือหัวหน้าส่วนงาน เฉพาะเมื่อมีอำนาจที่ได้รับมอบหมาย	อยู่ภายใน RA/RT ไม่มีข้อห้าม มีการควบคุมและกำหนดการทบทวน
ปานกลาง 5–9 (M)	หัวหน้าส่วนงานหรือผู้บริหารที่ได้รับมอบหมาย	มีเหตุผล หลักฐาน ตัวชี้วัด และเงื่อนไขติดตาม หากเกินกรอบหรืออำนาจต้องยกระดับ
สูง 10–15 (H)	อธิการบดีหรือผู้บริหารระดับมหาวิทยาลัยที่ได้รับมอบอำนาจ ผ่านการกลั่นกรองตามโครงสร้าง	มีแผนจัดการ เป้าหมาย ทรัพยากร และกำหนดเวลา การคงไว้ต้องมีเงื่อนไขและวันสิ้นสุด
สูงมาก 16–25 (E)	ยกระดับทันที การคงไว้ชั่วคราวต้องได้รับอนุมัติจากผู้มีอำนาจตามเอกสารที่เกี่ยวข้อง และรายงานผู้กำกับดูแล	ไม่ยอมรับเป็นการดำเนินงานปกติ ต้องมีเหตุผลความจำเป็น มาตรการชดเชยหรือแผนฉุกเฉิน วันสิ้นสุด และการติดตามใกล้ชิด
เหตุ Zero Tolerance	ไม่อยู่ในอำนาจอนุมัติให้กระทำหรือเพิกเฉยต่อเหตุ	ต้องคุ้มครอง ระงับหรือจำกัดความเสียหาย รายงาน รักษาหลักฐาน และดำเนินการตามข้อกำหนด

การอนุมัติให้คงความเสี่ยงเกิน RT ไว้ชั่วคราวไม่เปลี่ยนสถานะว่าเกินเกณฑ์ และไม่ยกเว้นหน้าที่ตามกฎหมาย เจ้าของความเสี่ยงยังรับผิดชอบการจัดการ ส่วนผู้อนุมัติรับผิดชอบการตัดสินใจภายในอำนาจของตน

บันทึกการยอมรับความเสี่ยง (Risk Acceptance Record) ต้องมีข้อมูลอย่างน้อยดังต่อไปนี้

1. ความเสี่ยง วัตถุประสงค์ เจ้าของความเสี่ยง และผลประเมินปัจจุบันพร้อมวันที่
2. สถานะ RA/RT และเหตุผลที่เสนอให้ยอมรับ
3. การควบคุม หลักฐานประสิทธิผล และช่องว่าง
4. ทางเลือกที่พิจารณา ผลกระทบ ต้นทุน และประโยชน์
5. ผู้มีส่วนได้ส่วนเสียและผลกระทบที่ต้องคุ้มครอง
6. KRI จุดเตือน และเงื่อนไขที่ต้องทบทวนหรือยกระดับ
7. มาตรการชดเชย แผนสำรอง และผู้รับผิดชอบ
8. วันที่มีผล ระยะเวลา วันที่ทบทวน และวันสิ้นสุดตามเงื่อนไข
9. ผู้เสนอ ผู้กลั่นกรอง ผู้อนุมัติ และเอกสารอ้างอิงอำนาจ

การยอมรับระดับสูงหรือสูงมากต้องมีวันสิ้นสุด และเสนออนุมัติใหม่ก่อนครบกำหนดหากยังจำเป็นต้องคงไว้ ไม่ต่ออายุโดยอัตโนมัติ

ตัวอย่างสมมติ: ระบบทะเบียนมีความเสี่ยงระดับสูง แต่การหยุดทันทีจะกระทบการลงทะเบียน ผู้มีอำนาจอาจพิจารณาให้ใช้งานต่อชั่วคราวเมื่อไม่ขัดต่อกฎหมาย โดยเพิ่มการเฝ้าระวังจำกัดการเปิดรับความเสี่ยง จัดทางเลือกสำรอง และกำหนดช่วงหยุดเพื่อปรับปรุงระบบ (Maintenance Window) พร้อมวันสิ้นสุดและเงื่อนไขหยุดทันทีหากสถานการณ์รุนแรงขึ้น

5.11 การรายงานและยกระดับความเสี่ยง (Risk Reporting and Escalation)

ให้ใช้บทบาทและสายรายงานตามข้อ 3.6 เงื่อนไขตามข้อ 3.9 และแนวทางในข้อ 4.11 โดยไม่กำหนดสายรายงานใหม่ที่ขัดกับส่วนดังกล่าว

ตารางที่ 5-7 ***สรุปกำหนดเวลารายงานและการติดตาม***

เงื่อนไข	กำหนดเวลารายงาน
เหตุ Zero Tolerance เหตุวิกฤต หรือภัยคุกคามรุนแรงต่อชีวิต ข้อมูล หรือพันธกิจ	แจ้งทันที และจัดทำรายงานเบื้องต้นไม่เกิน 24 ชั่วโมง

เงื่อนไข	กำหนดเวลารายงาน
ความเสี่ยงคงเหลือระดับสูงมาก 16–25 (E)	แจ้งยกระดับทันที และจัดทำรายงานไม่เกิน 24 ชั่วโมง
ความเสี่ยงคงเหลือระดับสูง 10–15 (H) หรือ ผลกระทบระดับ 5 ที่คะแนนต่ำกว่าระดับสูง	ภายใน 3 วันทำการเมื่อพบหรือเปลี่ยนแปลงเข้าเกณฑ์ หากมีความเร่งด่วนให้แจ้งทันที
KRI เกิน RT การควบคุมสำคัญไม่ทำงาน หรือ มาตรการสำคัญล่าช้าจนกระทบเป้าหมาย	ภายใน 3 วันทำการ หรือเร็วกว่าตาม Trigger และความรุนแรง
ความเสี่ยงระดับปานกลาง 5–9 (M)	ตามรอบที่กำหนด อย่างน้อยรายไตรมาส
ความเสี่ยงระดับต่ำ 1–4 (L)	รายงานตามรอบปกติ และทบทวนอย่างน้อยรายไตรมาส

ให้นับเวลาตั้งแต่พบหรือรับทราบข้อมูลที่เข้าเกณฑ์ โดย 24 ชั่วโมงเป็นชั่วโมงต่อเนื่อง ไม่รอข้อมูลครบหรือการรับรองรายงานก่อนแจ้งเหตุเร่งด่วน และต้องใช้กำหนดเวลาที่มหาวิทยาลัยอนุมัติไว้ หากกฎหมายหรือแผนเฉพาะกำหนดเวลาสั้นกว่า ให้ใช้เวลาที่สั้นกว่า พร้อมปฏิบัติตามผู้รับและช่องทางที่กำหนด การรายงานภายในไม่ทดแทนการแจ้งภายนอกตามกฎหมาย และไม่ทดแทนการคุ้มครองชีวิต จำกัดความเสียหาย รักษาข้อมูล ทรัพย์สิน หลักฐาน และความต่อเนื่อง

5.12 การทบทวนและอนุมัติเกณฑ์ (Criteria Review and Approval)

5.12.1 รอบและเงื่อนไขการทบทวน (Review Frequency and Triggers) ให้ทบทวน Risk Capacity, RA, RT, Risk Limit และ KRI อย่างน้อยปีละหนึ่งครั้ง และเมื่อ

1. ยุทธศาสตร์ ฐานะการเงิน กฎหมาย เทคโนโลยี หรือบริบทเปลี่ยนแปลงอย่างมีนัยสำคัญ
2. เกิดเหตุรุนแรง เหตุ Zero Tolerance หรือพบข้อบกพร่องสำคัญ
3. KRI เกิน RT ต่อเนื่อง หรือเกณฑ์ไม่ช่วยเตือนและสนับสนุนการตัดสินใจ
4. ข้อมูลฐาน สูตร ขอบเขต หรือสมมติฐานเปลี่ยนแปลง
5. พบว่าตัวชี้วัดซ้ำซ้อน ไม่สัมพันธ์กับความเสี่ยง หรือมีข้อมูลไม่เพียงพอ

การเกินเกณฑ์ครั้งแรกยังต้องตอบสนองตามข้อกำหนด ไม่รอให้เกินต่อเนื่องก่อนดำเนินการ

5.12.2 บทบาทในการพิจารณาและอนุมัติ (Review and Approval Roles)

- **เจ้าของข้อมูล (Data Owner):** ยืนยันนิยาม คุณภาพ แหล่งข้อมูล และความเป็นไปได้ในการจัดเก็บ

- **เจ้าของความเสี่ยง (Risk Owner):** ยืนยันความสัมพันธ์กับความเสี่ยง ความเหมาะสมของเกณฑ์ และการตอบสนอง
- **หน่วยบริหารความเสี่ยง:** รวบรวม วิเคราะห์ สอบทานความสอดคล้อง และจัดทำข้อเสนอ
- **ฝ่ายบริหารและคณะกรรมการที่เกี่ยวข้อง:** กลั่นกรองหรืออนุมัติตามอำนาจหน้าที่
- **สภามหาวิทยาลัย:** พิจารณาถ้อยแถลง RA และหลักเกณฑ์สำคัญในเรื่องที่อยู่ในอำนาจ
- **กองตรวจสอบภายใน:** ให้ความเชื่อมั่นและคำปรึกษาอย่างเป็นอิสระ โดยไม่เป็นผู้กำหนดหรืออนุมัติ RA/RT แทนผู้มีอำนาจ

การเปลี่ยนเกณฑ์ต้องมีเหตุผล หลักฐาน ผลกระทบ ผู้อนุมัติ วันที่มีผล และประวัติฉบับ พร้อมถ่ายทอดให้ผู้เกี่ยวข้องทราบ ห้ามปรับย้อนหลังเพื่อทำให้ผลที่เกินเกณฑ์ดูเป็นผลที่ยอมรับได้ หากปรับสูตรหรือแก้ข้อมูลเดิม ต้องแยกการแก้ไขข้อมูลออกจากการเปลี่ยนเกณฑ์อย่างชัดเจน

5.12.3 ตัวอย่างการใช้เกณฑ์และการยกระดับครบวงจร (End-to-end Application Example)

ตัวอย่างนี้เป็นข้อมูลสมมติ ไม่ใช่เกณฑ์หรือผลประเมินที่มหาวิทยาลัยอนุมัติแล้ว ความเสี่ยงด้านไซเบอร์และข้อมูลส่วนบุคคลใช้ตัวชี้วัดนำ คือ **ร้อยละบุคลากรกลุ่มเป้าหมายที่ผ่านเกณฑ์ความรู้และการปฏิบัติตามบทบาท** โดยกำหนด

- **เกณฑ์ปฏิบัติที่เชื่อมโยงกับ RA:** ตั้งแต่ร้อยละ 90 ขึ้นไป
- **ช่วงเฝ้าระวัง:** ตั้งแต่ร้อยละ 80 แต่ต่ำกว่าร้อยละ 90
- **ขอบเขต RT:** ไม่ต่ำกว่าร้อยละ 80 ณ จุดตรวจสอบที่กำหนด
- **เกิน RT:** ต่ำกว่าร้อยละ 80

สมมติผลอยู่ที่ร้อยละ 76 ให้ดำเนินการดังนี้

1. เจ้าของข้อมูลตรวจสอบกลุ่มเป้าหมาย ผลทดสอบ และวิธีคำนวณ
2. เจ้าของความเสี่ยงวิเคราะห์ว่ากลุ่มที่ไม่ผ่านเกี่ยวข้องกับงานหรือข้อมูลสำคัญเพียงใด พร้อมพิจารณาการควบคุมอื่น
3. เจ้าของมาตรการจัดแผนพัฒนาหรือแก้ไขกระบวนงาน กำหนดเวลา และทดสอบซ้ำ
4. รายงานผู้บริหารที่กำกับและหน่วยบริหารความเสี่ยงภายในกำหนดเมื่อเกิน RT หรือทันทีหากมีภัยคุกคามเร่งด่วน
5. บันทึกข้อสั่งการ การสนับสนุนทรัพยากร และผู้รับผิดชอบในบันทึกการตัดสินใจ

6. ติดตามทั้งผลทดสอบ การปฏิบัติจริง และเหตุการณ์ที่เกี่ยวข้อง

หากผลเพิ่มเป็นร้อยละ 92 ให้บันทึกว่าตัวชี้วัดนี้ผ่านเกณฑ์ แต่ไม่ลดคะแนนความเสี่ยงคงเหลือโดยอัตโนมัติ ต้องตรวจสอบว่าความพร้อมดังกล่าวร่วมกับการควบคุมทางเทคนิคและกระบวนงานช่วยลดโอกาสเกิดหรือผลกระทบได้จริง ส่วนเหตุละเมิดข้อมูลหรือภัยคุกคามรุนแรงให้รายงานตามแผนเฉพาะ แม้ตัวชี้วัดบุคลากรยังเป็นสีเขียว

เกินขอบเขต RT: ต่ำกว่าร้อยละ 80 ณ จุดตรวจสอบที่กำหนด

สมมติผลการติดตามพบว่าบุคลากรกลุ่มเป้าหมายผ่านเกณฑ์ความรู้และการปฏิบัติหลังการอบรมร้อยละ 78 จึงมีสถานะ **สีส้ม — ต้องแก้ไขและยกระดับ (Orange)** ตามเกณฑ์ตัวอย่าง ให้ดำเนินการดังต่อไปนี้

1. **เจ้าของข้อมูล (Data Owner):** ตรวจสอบความถูกต้องของข้อมูล วิธีคำนวณ และรายชื่อกลุ่มที่ยังไม่ผ่านเกณฑ์

2. **เจ้าของความเสี่ยง (Risk Owner):** วิเคราะห์สาเหตุ ความสำคัญของงานที่กลุ่มดังกล่าวรับผิดชอบ และผลต่อความเสี่ยงคงเหลือ (Residual Risk) โดยพิจารณาการควบคุมอื่นร่วมด้วย

3. **เจ้าของมาตรการ (Action Owner):** จัดแผนพัฒนาหรืออบรมเพิ่มเติมให้ตรงกับช่องว่างพร้อมกำหนดเวลาและวิธีประเมินการปฏิบัติซ้ำ

4. **การแก้ไขและรายงาน:** จัดทำมาตรการแก้ไข (Corrective Action) และรายงานผู้บริหารที่กำกับกับหน่วยบริหารความเสี่ยงภายใน 3 วันทำการนับจากพบหรือรับทราบผลที่เข้าเกณฑ์ หรือเร็วกว่านั้นหากมีความเร่งด่วน

5. **การติดตาม:** เพิ่มความถี่ตามความจำเป็นจนผลกลับเข้าสู่เกณฑ์ที่กำหนดและมีหลักฐานว่าการแก้ไขเกิดผล ไม่พิจารณาเพียงจำนวนผู้เข้าอบรมเพิ่มขึ้น

หากระหว่างนั้นเกิดเหตุข้อมูลรั่วไหลที่มีผลกระทบรุนแรง ให้ตอบสนองและยกระดับทันทีตามแผนเผชิญเหตุและข้อกำหนดเฉพาะ โดยไม่รอผลการอบรมรอบถัดไป ส่วนการใช้เกณฑ์ **Zero Tolerance** ให้พิจารณาว่าเหตุหรือพฤติกรรมนั้นอยู่ในขอบเขตนโยบายที่กำหนดหรือไม่ ไม่จัดเป็น Zero Tolerance โดยอัตโนมัติจากผลกระทบรุนแรงเพียงอย่างเดียว

ตัวอย่างนี้แสดงว่า RA กำหนดท่าทีต่อการรับความเสี่ยง RT กำหนดขอบเขตความเบี่ยงเบนที่อนุญาต KRI ใช้ติดตามและส่งสัญญาณ และ Trigger เชื่อมผลกับการดำเนินการ ผู้รับผิดชอบ ระยะเวลา และการตัดสินใจ โดยอาจกำหนดช่วงเฝ้าระวังไว้ก่อนถึงขอบเขต RT เพื่อให้มีเวลาแก้ไขล่วงหน้า

เอกสารอ้างอิง

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

ภาคผนวก

แบบฟอร์มประเมินและวิเคราะห์ความเสี่ยง

แบบ Risk-MJU-01

แบบฟอร์มการวิเคราะห์และประเมินความเสี่ยง (Risk-MJU-01)

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	9 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-MJU-01)

1. วัตถุประสงค์ของแบบฟอร์ม

แบบ Risk-MJU-01 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-MJU-01 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

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

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ระดับความเสี่ยงก่อนการจัดการ				ระดับความเสี่ยงที่ยอมรับได้				วิธีจัดการ (Risk	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		(Strategic Risk) ความเสี่ยงด้านกลยุทธ์																
O1		(Operational Risk) การดำเนินงาน																
F1		(Financial Risk) การเงิน																
C1		(Compliance Risk) กฎหมาย/การกำกับดูแล																
D1		(Digital Technology Risk) ด้านเทคโนโลยีดิจิทัล																

สรุปการจัดทำแผนการบริหารความเสี่ยง ประจำปีงบประมาณ 25XX

หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริการจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 (โดยที่สมควรให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการความเสี่ยง เพื่อให้การดำเนินงานบรรลุวัตถุประสงค์ตามยุทธศาสตร์ที่หน่วยงานของรัฐกำหนด)

ประเภทความเสี่ยง	ประเด็นความเสี่ยง	จำนวนกิจกรรม/ประเด็นความเสี่ยง
1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)	S1:	
	S2:	
2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)	O1:	
	O2:	
3. ความเสี่ยงด้านการเงิน (Financial Risk)	F1:	
	F2:	
4. ความเสี่ยงด้านการปฏิบัติตามกฎหมาย/กำกับดูแล (Compliance Risk)	C1:	
	C2:	

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

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

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

1. มีกิจกรรมเพื่อลดความเสี่ยงในแผน จำนวน _____ กิจกรรม

2. มีประเด็นความเสี่ยงในแผน จำนวน _____ ประเด็น

ผ่านความเห็นชอบจากคณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน คราวประชุมครั้งที่ XXXXXXX เมื่อวันที่ XX XXXXX พ.ศ.XXXXX

ผ่านความเห็นชอบจากคณะกรรมการบริหารคณะ ในคราวประชุมครั้งที่ 21/XXXXXXX เมื่อวันที่ XX XXXXX พ.ศ.XXXXX

ชื่อ.....ลงนาม.....

(.....)

(ตำแหน่ง).....

สังกัด.....

คำอธิบายแบบฟอร์มแผนบริหารความเสี่ยง (มจ-ส-01)

แบบฟอร์มแผนบริหารความเสี่ยง (มจ-ส-01) ใช้สำหรับจัดทำแผนบริหารความเสี่ยงของส่วนงาน/หน่วยงาน ประจำปีงบประมาณ เพื่อกำหนดประเด็นความเสี่ยง แนวทางการควบคุม กิจกรรมลดความเสี่ยง และการติดตามผลการดำเนินงานให้เป็นไปตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562

1. ส่วนหัวแบบฟอร์ม

แผนบริหารความเสี่ยง ..... ประจำปีงบประมาณ พ.ศ. 25XX

ระบุชื่อส่วนงาน/หน่วยงาน และปีงบประมาณที่ดำเนินการ

ตัวอย่าง “แผนบริหารความเสี่ยง คณะวิทยาศาสตร์ ประจำปีงบประมาณ พ.ศ. 2569”

---

2. ตัวชี้วัดความสำเร็จของแผน (KPI) ภาพรวม

ใช้กำหนดตัวชี้วัดผลสำเร็จของแผนบริหารความเสี่ยงในภาพรวมของหน่วยงาน เช่น

1. ดำเนินกิจกรรมควบคุมตามแผนไม่น้อยกว่าร้อยละ 80
2. สามารถลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ไม่น้อยกว่าร้อยละ 80

ทั้งนี้ ส่วนงานสามารถกำหนด KPI เพิ่มเติมได้ตามบริบทของหน่วยงาน

---

3. คำอธิบายการกรอกข้อมูลรายช่อง

ลำดับ	รายการ	คำอธิบาย
(1)	รหัส	ระบุรหัสความเสี่ยง เช่น S1, O1, F1, C1
(2)	ความเสี่ยง	ระบุชื่อหรือประเด็นความเสี่ยง
(3)	ประเภทความเสี่ยง	ระบุประเภทความเสี่ยง เช่น Strategic, Operational, Financial, Compliance
(4)	L (Likelihood)	ระดับโอกาสเกิดความเสี่ยงก่อนการจัดการ
(5)	I (Impact)	ระดับผลกระทบก่อนการจัดการ
(6)	คะแนน	คำนวณจากค่า L × I
(7)	ระดับ	ระดับความเสี่ยง เช่น ต่ำ ปานกลาง สูง สูงมาก
(8)	L	ระดับโอกาสเกิดความเสี่ยงที่ยอมรับได้
(9)	I	ระดับผลกระทบที่ยอมรับได้
(10)	คะแนน	คำนวณระดับความเสี่ยงที่ยอมรับได้
(11)	ระดับ	ระดับความเสี่ยงที่ยอมรับได้
(12)	Risk Treatment	แนวทางจัดการความเสี่ยง เช่น Treat, Transfer, Terminate, Tolerate
(13)	สาเหตุ (Root Causes)	วิเคราะห์สาเหตุที่แท้จริงของความเสี่ยง
(14)	ตัวบ่งชี้ความเสี่ยง / สัญญาณเตือนภัย (KRI)	ตัวชี้วัดหรือสัญญาณเตือนที่ใช้ติดตามความเสี่ยง
(15)	RA	ค่าเป้าหมายหรือค่าที่ยอมรับได้ (Risk Appetite)
(16)	RT	ค่าระดับที่ต้องเฝ้าระวังหรือจุดวิกฤต (Risk Threshold)
(17)	มาตรการ/กิจกรรมลดความเสี่ยง	กิจกรรมหรือแนวทางที่ใช้ควบคุมและลดความเสี่ยง
(18)	ผู้รับผิดชอบกิจกรรม	ผู้รับผิดชอบหลักในการดำเนินกิจกรรม
(19)	ระยะเวลาดำเนินการ	ระบุช่วงเวลาการดำเนินงาน เช่น ต.ค. 68 – ก.ย. 69

4. การกำหนดประเภทความเสี่ยง

ประเภทความเสี่ยง	ความหมาย
Strategic Risk	ความเสี่ยงด้านยุทธศาสตร์หรือเป้าหมายองค์กร
Operational Risk	ความเสี่ยงด้านการดำเนินงานหรือกระบวนการปฏิบัติงาน
Financial Risk	ความเสี่ยงด้านการเงิน งบประมาณ หรือสภาพคล่อง
Compliance Risk	ความเสี่ยงด้านกฎหมาย ระเบียบ ข้อบังคับ และธรรมาภิบาล
Digital/Technology Risk	ความเสี่ยงด้านระบบสารสนเทศและเทคโนโลยีดิจิทัล

---

5. แนวทางการกำหนดคะแนนความเสี่ยง

การประเมินระดับความเสี่ยงให้พิจารณาจาก

- โอกาสเกิด (Likelihood : L)
- ผลกระทบ (Impact : I)

โดยใช้เกณฑ์ระดับ 1–5 และคำนวณคะแนนจาก

คะแนนความเสี่ยง = L × I

ตัวอย่าง L = 4 และ I = 5 คะแนนความเสี่ยง = 20 (ระดับสูงมาก)

---

6. การสรุปผลแผนบริหารความเสี่ยง

ส่วนท้ายของแบบฟอร์มใช้สำหรับสรุปจำนวนประเด็นความเสี่ยงและจำนวนกิจกรรมลดความเสี่ยงของหน่วยงาน เช่น

- จำนวนกิจกรรมลดความเสี่ยงทั้งหมด
- จำนวนประเด็นความเสี่ยงทั้งหมด
- จำแนกตามประเภทความเสี่ยง

เพื่อใช้ประกอบการรายงานภาพรวมระดับมหาวิทยาลัย

---

7. การรับรองและให้ความเห็นชอบ

ให้ระบุข้อมูลการผ่านความเห็นชอบจากคณะกรรมการที่เกี่ยวข้อง เช่น

- คณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน
- คณะกรรมการบริหารส่วนงาน
- คณะกรรมการประจำคณะ/สำนัก/สถาบัน

พร้อมระบุเลขที่ประชุมและวันที่ประชุมให้ครบถ้วน

---

8. หมายเหตุเพิ่มเติม

1. ส่วนงานสามารถเพิ่มเติมรายละเอียดหรือปรับรูปแบบเอกสารได้ตามความเหมาะสม แต่ต้องมีข้อมูลสาระสำคัญครบถ้วนตามที่มหาวิทยาลัยกำหนด
2. ควรกำหนดกิจกรรมลดความเสี่ยงให้สอดคล้องกับสาเหตุของความเสี่ยง (Root Causes) และสามารถติดตามผลได้อย่างเป็นรูปธรรม
3. ควรมีตัวชี้วัดความสำเร็จ (KPI/KRI) ที่สามารถวัดผลและตรวจสอบได้
4. ให้มีการติดตามผลและรายงานความก้าวหน้าตามรอบระยะเวลา 6 เดือน 9 เดือน และ 12 เดือน
5. เอกสารสามารถจัดทำได้ทั้งในรูปแบบ Microsoft Word และ Microsoft Excel ตามวัตถุประสงค์การใช้งาน

แบบฟอร์มรายงานผลการดำเนินการตามแผนบริหารความเสี่ยง

(มจ-ส-02)

.....
.....
.....
.....
.....
.....
.....
.....
.....

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

1. **รหัสและชื่อประเด็นความเสี่ยง** ตามแผนที่ได้รับอนุมัติ โดยใช้ประเภทความเสี่ยงหลัก 5 ประเภท ได้แก่
    - **S:** ความเสี่ยงด้านยุทธศาสตร์ (Strategic Risk)

    - **O:** ความเสี่ยงด้านการดำเนินงาน (Operational Risk)
    - **F:** ความเสี่ยงด้านการเงิน (Financial Risk)
    - **C:** ความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (Compliance and Governance Risk)
    - **D:** ความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Technology Risk)
2. **ตัวชี้วัดความเสี่ยงที่สำคัญ (KRI)** ระบุชื่อ หน่วยวัด และทิศทางของตัวชี้วัด เช่น ค่ายิ่งสูงยิ่งดี หรือค่ายิ่งต่ำยิ่งดี โดยใช้นิยามและสูตรคำนวณที่กำหนดไว้
3. **เกณฑ์ที่ถ่ายทอดจากระดับความเสี่ยงที่ยอมรับได้ (RA)** ระบุค่าหรือเงื่อนไขที่ใช้พิจารณาว่าผลตัวชี้วัดอยู่ภายในขอบเขตที่กำหนด
4. **ระดับความเบี่ยงเบนที่ยอมรับได้ (RT)** ระบุขอบเขตความเบี่ยงเบน เงื่อนไข และระยะเวลาที่อนุญาต พร้อมเกณฑ์การดำเนินการเมื่อเกินขอบเขต
5. **ผลตัวชี้วัดในรอบรายงาน** ระบุค่าที่เกิดขึ้นจริง ช่วงเวลาของข้อมูล แหล่งข้อมูล และเจ้าของข้อมูล (Data Owner)
6. **สถานะและแนวโน้ม** เปรียบเทียบผลกับ RA/RT และรอบก่อน พร้อมอธิบายสาเหตุของการเปลี่ยนแปลง
7. **การดำเนินการและประเด็นยกระดับ** ระบุมาตรการแก้ไข ผู้รับผิดชอบ กำหนดแล้วเสร็จ และการรายงานเมื่อเข้าเงื่อนไขกระตุ้นการดำเนินการ (Trigger)

ผล KRI ใช้ประกอบการประเมินความเสี่ยงและการตัดสินใจร่วมกับข้อมูลเหตุการณ์และหลักฐานการควบคุม ไม่ควรสรุปว่าการควบคุมมีประสิทธิผลหรือความเสี่ยงคงเหลือลดลงจากค่า KRI เพียงตัวเดียว

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 เพื่อให้ทุกส่วนงานจัดทำรายงานในรูปแบบเดียวกัน และสามารถเปรียบเทียบข้อมูลได้อย่างเป็นระบบ
- 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