ความรู้การบริหารความเสี่ยงเชิงปฏิบัติ
(ฉบับ OPPQA)

ประจำปีการศึกษา 2566

โดย: สำนักงานนโยบาย แผน และ การประกันคุณภาพ

คำนำ

การจัดการความรู้ของมหาวิทยาลัยอัสสัมชัญ เป็นกระบวนการที่เป็นระบบในการบริหารจัดการให้คณะและหน่วยงานสนับสนุนวิชาการมีการรวบรวมความรู้และถ่ายทอดความรู้ที่เป็นประโยชน์ สามารถนำไปใช้ในการปฏิบัติงานประจำอย่างมีประสิทธิภาพ ประสิทธิผล รวมทั้งส่งเสริมสนับสนุนให้บุคลากรได้ร่วมกันสร้าง แบ่งปัน ข้อมูลสารสนเทศและความรู้ที่สำคัญที่เหมาะสมกับบริบทของหน่วยงานให้เกิดการเชื่อมโยงนโยบายของมหาวิทยาลัยฯ นำไปสู่การปฏิบัติ โดยบูรณาการกับระบบประกันคุณภาพ เพื่อตอบสนองการบรรลุพันธกิจและยุทธศาสตร์ของมหาวิทยาลัย

ทั้งนี้ สำนักงานโยบาย แผน และการประกันคุณภาพมีภาระงานในการช่วยเหลือ สนับสนุน และให้คำปรึกษา(Consulting) เกี่ยวกับกระบวนการบริหารความเสี่ยงให้กับบุคลากรที่รับผิดชอบ ซึ่งการขับเคลื่อนการจัดการความรู้ ประจำปีการศึกษา 2567 ในรูปแบบคู่มือการปฏิบัติงานในหัวข้อ **“ความรู้การบริหารความเสี่ยงเชิงปฏิบัติ ฉบับ OPPQA”** เพื่อนำความรู้ตามกระบวนการบริหารความเสี่ยง นำไปสู่การปฏิบติอย่างเป็นระบบและมีความต่อเนื่อง รวมทั้งปลูกฝังวัฒนธรรมองค์กรที่มุ่งเน้นการสร้างองค์ความรู้ด้านการบริหารความเสี่ยงไปยังบุคลากรทุกระดับ ซึ่งเป็นการสร้างฐานข้อมูลความรู้ที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานบริหารความเสี่ยงให้เป็นไปในทิศทางเดียวกันทั้งองค์กร

สำนักงานนโยบาย แผน และการประกันคุณภาพ

มีนาคม 2567

ความรู้การบริหารความเสี่ยงเชิงปฏิบัติ ฉบับ OPPQA

การบริหารความเสี่ยง เป็นกระบวนการบริหารจัดการเชิงรุกที่เน้นการเตรียมความพร้อมรับมือเหตุการณ์หรือสถานการณ์ที่ไม่คาดฝัน ซึ่งอาจเกิดขึ้นภายใต้บริบทที่มีการเปลี่ยนแปลงและมีความไม่แน่นอนของปัจจัยแวดล้อมทั้งภายในและภายนอกหน่วยงาน และส่งผลกระทบต่อความสามารถในการบรรลุเป้าหมายที่ตั้งไว้ ซึ่งหากหน่วยงานสามารถบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ และประสิทธิผล จะทำให้เกิดการบริหารจัดการที่ดีมีการกำกับดูแล และควบคุมกระบวนการทำงานภายในที่ดี สามารถควบคุมให้ความเสี่ยงอยู่ในระดับที่เหมาะสม หรือยอมรับความเสี่ยงได้ภายใต้การใช้ทรัพยากรที่คุ้มค่าสร้างความมั่นใจในการดำเนินงานไปสู่ความสำเร็จตามเป้าหมาย ที่ต้องการ สามารถใช้ประโยชน์จากโอกาส หรือความได้เปรียบที่มี รวมถึงสามารถลดความสูญเสีย ความเสียหายที่จะเกิดขึ้นในอนาคตให้กับหน่วยงานและมหาวิทยาลัยได้เป็นอย่างดีอีกด้วย

OPPQA ตระหนักถึงความสำคัญของการบริหารความเสี่ยงในการดำเนินภารกิจและบรรลุวัตถุประสงค์ของมหาวิทยาลัยอัสสัมชัญ ภายใต้สภาพแวดล้อมที่เปลี่ยนแปลงอย่างพลิกโฉม (Disruption) และความท้าทาย ต่าง ๆ ที่เพิ่มขึ้น เช่น การถูกแทนที่ด้วยเทคโนโลยีสารสนเทศและนวัตกรรมสมัยใหม่หลังการระบาดของโรคโควิด19 สิ้นสุดลง เป็นต้น ทั้งนี้ OPPQA จึงมีการเชื่อมโยงกลไกบริหารความเสี่ยงจากระดับองค์กรมายัง OPPQA อย่างเป็นระบบ รอบด้านและต่อเนื่อง โดยมุ่งเน้นการระบุ/ค้นหา ประเมิน จัดการ และติดตามความเสี่ยงอย่างมีประสิทธิภาพ เพื่อให้มั่นใจว่าสามารถบรรลุวัตถุประสงค์และเป้าหมายของมหาวิทยาลัยได้อย่างยั่งยืน ทำให้ผลลัพธ์ของการบริหารความเสี่ยงสามารถสร้างคุณค่าแก่มหาวิทยาลัย

OPPQA มีการทบทวน ศึกษา ทำความเข้าใจมุมมองการบริหารความเสี่ยงในอดีตและการบริหารความเสี่ยงในปัจจุบัน ดังนี้

ทบทวน ทำความเข้าใจ

“ มุมมองในอดีต & มุมมองปัจจุบัน ”

ในการบริหารความเสี่ยง

มุมมองในอดีต	มุมมองในปัจจุบัน
ความเสี่ยง (Risk) คือ ความสูญเสีย (Loss) **ที่จะเกิดขึ้นกับองค์กร**	**ความเสี่ยง (Risk) คือ โอกาส (Opportunities)** High Risk High Return ถ้าไม่ยอมเสี่ยง อาจสูญเสีย
ความเสี่ยง เป็นการป้องกันความสูญเสีย ที่จะเกิดขึ้นในอนาคต เป็นภาระ ไม่ได้ทำให้ผลการดำเนินงานขององค์กรดีขึ้น	ความเสี่ยงที่สำคัญระดับองค์กร (Enterprise Risk Management: ERM) จะต้องสนับสนุนให้วัตถุประสงค์ ภารกิจหลัก ตัวชี้วัดและเป้าหมายขององค์กรบรรลุผลสำเร็จและก้าวสู่เป้าหมายอย่างมั่นใจ
ปัญหาปัจจุบัน (Current Problem) คือ ความเสี่ยง	ปัญหาไม่ใช่ความเสี่ยง แต่ผลของปัญหาจะทำให้เกิดความเสี่ยงในอนาคต ถ้าไม่แก้ไขจัดการ
ความเสี่ยงด้านกลยุทธ์ ยิ่งมีจำนวนมาก ยิ่งดี การบริหารจัดการจัดการความเสี่ยง ควรจัดทำแผนจัดการความเสี่ยงทุกกลยุทธ์	ความเสี่ยงด้านกลยุทธ์ ควรระบุความเสี่ยงเฉพาะประเด็นที่สำคัญและมีผลกระทบต่อองค์กร (เช่น มิติชื่อเสียง ภาพลักษณ์ สถานะทางการเงิน ความปลอดภัยชีวิตและทรัพย์สินและความชะงักงันการดำเนินงานภารกิจหลัก) เพื่อ Focus ในการจัดการอย่างมีประสิทธิภาพและประสิทธิผล **ความเสี่ยงที่สำคัญ –> มีน้อย** **ความเสี่ยงที่เล็กน้อย –> มีมาก** **หากกำหนดประเด็นความเสี่ยงมากเกินไป มักละเลย**

มุมมองในอดีต	มุมมองในปัจจุบัน
การจัดการ“การควบคุมภายใน (Internal Audit)” เป็นงานเดียวกัน กับ “การบริหารจัดการความเสี่ยง (Risk Management)”	“การควบคุมภายใน (Internal Audit)” และ “การบริหารจัดการความเสี่ยง (Risk Management)” ไม่ใช่งานเดียวกัน เป็นงานที่จะต้องเชื่อมต่อข้อมูลที่สำคัญระหว่างกัน เพื่อประโยชน์ในการบริหารจัดการองค์กร อย่างมีประสิทธิภาพและประสิทธิผล อาทิ เช่น • การจัดการ กระบวนการควบคุมภายใน เป็นกระบวนการที่แทรกอยู่ในการปฏิบัติงานตามปกติ การควบคุมเกิดขึ้นโดย บุคลากรทุกระดับ ขององค์กร • การบริหารจัดการความเสี่ยง จากปัจจัยภายในและภายนอก ที่มีผลกระทบต่อองค์กร โดยอาจจัดทำ เป็นแผนงาน/โครงการ/กิจกรรม แยกต่างหากจากการดำเนินงานปกติหรือเป็นส่วนหนึ่งของการดำเนินงานตามปกติก็ได้
ต้องลดความเสี่ยงลงให้อยู่ในระดับต่ำสุด (ระดับความเสี่ยง ยิ่งต่ำ ยิ่งดี)	ในการจัดการลดความเสี่ยงย่อมมีค่าใช้จ่าย ยิ่งลดระดับความเสี่ยงมาก ยิ่งมีค่าใช้จ่ายมาก ดังนั้น ผู้บริหารจึงต้องพิจารณาตัดสินใจให้เกิดความสมดุลระหว่างระดับความเสี่ยงที่ลดลง กับค่าใช้จ่ายในการลดความเสี่ยง และจำเป็นต้องใช้ข้อมูลข้อเท็จจริง (Fact & Data)ในการประเมินและตัดสินใจจัดการความเสี่ยง

มุมมองในอดีต	มุมมองในปัจจุบัน
ดัชนีชี้วัดความเสี่ยง (KRIs) เป็นตัวเดียวกันกับดัชนีชี้วัดผลดำเนินงาน (KPIs)	➢ **KRIs** ส่วนใหญ่เป็นดัชนีชี้วัดก่อนเกิดเหตุการณ์**ความเสี่ยง (Leading Indicator) เป็นเสมือน "สัญญาณเตือนภัย"**เพื่อให้เกิดการจัดการก่อนที่ความเสี่ยงจะเกิดขึ้น ➢ **KPIs** ตัวชี้วัดผลดำเนินงาน มักเป็นตัวชี้วัดผลลัพธ์ ซึ่งเกิดขึ้นแล้ว **(Lagging Indicator)**
ต้องมีแผนงาน/กิจกรรม/โครงการในการจัดการลดระดับความเสี่ยงสำหรับทุกรายการความเสี่ยงที่ระบุขึ้น	การจัดการความเสี่ยง อาจเลือกใช้กลยุทธ์อย่างใดอย่างหนึ่ง หรือผสมผสานกัน ➢ ระดับความเสี่ยงจากการประเมินที่ต่ำ สามารถยอมรับได้ ใช้กลยุทธ์ **TAKE** ยอมรับความเสี่ยง (Accept)และดำเนินการควบคุม / ตรวจติดตาม (Control / Audit) ➢ ระดับความเสี่ยงจากการประเมินที่สูงไม่สามารถยอมรับได้ ใช้กลยุทธ์ **MITIGATION -TRANSFER - TERMINATE** ร่วมจัดการ (Share)/ลด (Reduce)/หลีกเลี่ยง (Avoid) โดยจะดำเนินการบริหารจัดการ (PDCA) เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

มุมมองในอดีต	มุมมองในปัจจุบัน
ทุกกิจกรรม/โครงการที่จะดำเนินการ สามารถลดและบริหารจัดการความเสี่ยงได้เสมอ	กิจกรรม/โครงการ ที่เป็น Exiting Control จะต้องเชื่อมโยงและสอดคล้องกับการประเมินระดับความเสี่ยงโดยมีวัตถุประสงค์เพื่อลดโอกาสเกิด (Likelihood) ลดผลกระทบ (Impact) และจะต้องจัดการที่สาเหตุของปัจจัยเสี่ยง**ดังนั้น การวิเคราะห์สาเหตุของความเสี่ยงเป็นเรื่อง ที่สำคัญ**

กระบวนการบริหารความเสี่ยงเชิงปฏิบัติของ OPPQA

กระบวนการการบริหารความเสี่ยง เป็นกระบวนการในการระบุความเสี่ยง การวิเคราะห์โอกาสที่จะเกิดและระดับความเสียหายของความเสี่ยง การกำหนดแผนการจัดการความเสี่ยงเพื่อป้องกันหรือลดโอกาสการเกิดความเสี่ยงหรือหากเกิดขึ้นและผลความเสียหายที่เกิดขึ้นจะอยู่ในระดับที่มหาวิทยาลัยยอมรับได้

OPPQA บริหารความเสี่ยง โดยนำกรอบการบริหารความเสี่ยง **COSO ERM** เป็นแนวทางในการบริหารความเสี่ยง ตามบรรทัดฐานการบริหารความเสี่ยงของมหาวิทยาลัย โดยมีกระบวนการดังนี้

1. การค้นหาความเสี่ยงและแหล่งที่มาความเสี่ยง

OPPQA เริ่มจาก**การค้นหาสถานการณ์ภายในและภายนอก**ที่มีผลกระทบเชิงลบต่อการดำเนินการของหน่วยงาน และเพื่อให้เป็นไปตามบริบทของมหาวิทยาลัยและมาตรฐาน COSO ในการบริหารจัดการความเสี่ยง OPPQA จึงพิจารณาค้นหาความเสี่ยงแยกตามประเภทความเสี่ยง ดังนี้

1. **ความเสี่ยงด้านกลยุทธ์ (SR : Strategic Risk)** ความเสี่ยงที่มีผลกระทบต่อทิศทาง หรือ ภารกิจหลักของ หรือมีผลกระทบต่อการบรรลุวัตถุประสงค์ของมหาวิทยาลัย เนื่องจากการเมือง เศรษฐกิจ

ความเปลี่ยนแปลงของสถานการณ์ภายนอก หรือความเสี่ยงที่เกิดจากการกระบวนการตัดสินใจเชิงกลยุทธ์ผิดพลาด

2. **ความเสี่ยงด้านการดำเนินงาน (OR : Operational Risk)** ความเสี่ยงที่มีผลกระทบต่อการดำเนินงานของมหาวิทยาลัย เนื่องจากการปฏิบัติงานภายในมหาวิทยาลัย อันเกิดจากกระบวนการ บุคลากร ความเพียงพอของข้อมูล
3. **ความเสี่ยงด้านการจบการศึกษา (GR: Student Graduation)** ความเสี่ยงที่มีผลกระทบต่อการสำเร็จการศึกษาตามหลักสูตรของนักศึกษาในแต่ละระดับ อาทิ หลักสูตรที่จบการศึกษาไม่ตรงกับความต้องการของตลาดแรงงาน
4. **ความเสี่ยงด้านการเงิน (FR : Financial Risk)** ความเสี่ยงที่ส่งผลกระทบต่อฐานะการเงินและขัดขวางการบรรลุเป้าประสงค์ของมหาวิทยาลัยด้านการเงิน เนื่องจากการใช้งบประมาณและรายได้ไม่เป็นไปตามแผน การขาดการรวบรวมข้อมูลอย่างเป็นระบบเพื่อวิเคราะห์ สังเคราะห์ การวางแผนทางการเงิน
5. **ความเสี่ยงด้านทรัพยากรบุคคล (P: People Risk)** ความเสี่ยงที่ส่งผลกระทบต่อการบริหารจัดการทรัพยากรบุคคลของมหาวิทยาลัย อาทิ ช่องว่างระหว่างสมรรถนะของบุคลากรกับเป้าหมายของมหาวิทยาลัย ความผูกพันของบุคลากรต่อองค์กร การเคลื่อนย้ายของบุคลากรมืออาชีพ
6. **ความเสี่ยงทางชื่อเสียง (RR: Reputation Risk)** ความเสี่ยงที่ส่งผลกระทบต่อการดำเนินการที่มีผลกระทบต่อภาพลักษณ์และชื่อเสียงของมหาวิทยาลัย
7. **ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ/กฎหมาย (CR : Compliance Risk)** ความเสี่ยงที่ส่งผลกระทบต่อการปฏิบัติตามกฎระเบียบและข้อบังคับกฎหมาย รวมถึงข้อบังคับภายในมหาวิทยาลัย

ในการพิจารณาแหล่งที่มาของความเสี่ยงนั้น **OPPQA**พิจารณาครอบคลุมทั้ง**ปัจจัยภายใน** เช่น แผนยุทธศาสตร์ กฎระเบียบ นโยบาย วิสัยทัศน์ พันธกิจ และ**ปัจจัยภายนอก** เช่น นโยบายภาครัฐ กฎหมาย สภาพภูมิอากาศ โรคระบาด ภัยพิบัติ ภัยคุกคามทางเทคโนโลยี และอื่นๆ เพื่อจะค้นหา **ปัญหา หรือ ความเสี่ยง** ของหน่วยงาน

OPPOAทบทวน  ปัญหา & ความเสี่ยง 

ปัญหา (Problem) คือ **สิ่งที่เกิดขึ้น รับรู้ และเห็นได้ชัดเจนแน่นอนตั้งแต่อดีต และยังคงเป็นอุปสรรคต่อการดำเนินงานในปัจจุบัน** ส่งผลให้งานขาดประสิทธิภาพ เกิดความเสียหายหรือความสูญเสียแก่องค์กร จึงจำเป็นต้องมี**มาตรการแก้ไขและปรับปรุง เพื่อควบคุม/จัดการกับปัญหาที่เกิดขึ้น** เพื่อไม่ให้ปัญหานั้นพัฒนากลายเป็นความเสี่ยง

ความเสี่ยง(Risk) คือ **สิ่งที่ยังไม่เกิดขึ้น ไม่แน่นอน เป็นเพียงการคาดการณ์ที่อาจจะเกิดขึ้นในอนาคต** สามารถส่งผลได้ทั้งในเชิงบวกและเชิงลบต่อวัตถุประสงค์และเป้าหมายของหน่วยงาน จึงควรกำหนด **มาตรการป้องกันโอกาสเกิดและลดผลกระทบ เพื่อควบคุม/จัดการกับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้**

ตัวอย่าง

ปัญหา & ความเสี่ยง

ปัญหา	ความเสี่ยง
บุคลากรขาดแรงจูงใจในการปฏิบัติงาน	การดำเนินงานไม่บรรลุเป้าประสงค์ของหน่วยงาน
บุคลากรขาดองค์ความรู้/ทักษะสำคัญที่จำเป็นต่อการบรรลุยุทธศาสตร์	การดำเนินงานตามแผนยุทธศาสตร์ใน บางแผนปฏิบัติงาน/กิจกรรม ที่สำคัญไม่เป็นไปตามเป้าหมายที่วางไว้
อาคารปฏิบัติงานสั่นสะเทือนทุกครั้งที่มีรถบรรทุกวิ่งผ่าน	ความปลอดภัยของชีวิตและทรัพย์สินในสถานที่ปฏิบัติงาน
การขัดข้องหรือการหยุดชะงักของระบบงานและระบบคอมพิวเตอร์	ระบบสารสนเทศไม่สามารถเชื่อมข้อมูล ระหว่างส่วนงานที่จำเป็นต้องใช้ข้อมูลร่วมกัน
ความผิดพลาดจากการปฏิบัติงานของบุคลากร	ข้อมูลของหน่วยงานเกิดการสูญหาย/ข้อมูลรั่วไหล
รับนักศึกษาใหม่ได้ไม่ตรงตามเป้าหมายที่ตั้งไว้ในเชิงปริมาณ	เสถียรภาพทางการเงินลดลง (ความไม่สมดุลของรายรับ และรายจ่าย
นักศึกษา อาจารย์และบุคลากรขาดความรับผิดชอบและความรู้เท่าทันในการใช้สื่อโซเชียล	ชื่อเสียงมหาวิทยาลัยเสียหาย

ปัญหา	ความเสี่ยง
นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศไม่ปรับปรุงให้ทันต่อเทคโนโลยีที่เปลี่ยนแปลง	ความปลอดภัยทางไซเบอร์
การร้องเรียนจากนักศึกษา เรื่องการแอบอ้างนำข้อมูลส่วนบุคคลไปใช้เผยแพร่ประชาสัมพันธ์มหาวิทยาลัย	มหาวิทยาลัยอาจจะโดนฟ้องร้องคดีจากนักศึกษา
บุคลากรไม่ปฏิบัติตามกฎระเบียบละเมิด จริยธรรม จรรยาบรรณ การทุจริตทางวิชาการ	การละเมิดจริยธรรมทางวิชาการ

2.การประเมินความเสี่ยงเพื่อเลือกความเสี่ยงที่สำคัญมาจัดการ

เมื่อทราบความเสี่ยง OPPQA จะประเมินความเสี่ยงเพื่อกำหนดความสำคัญก่อนหลังในการจัดการความเสี่ยงรวมทั้งช่วยกำหนดแผนการจัดการความเสี่ยงที่มีประสิทธิภาพ ในการประเมินความเสี่ยง OPPQA พิจารณา ดังนี้

1. **สาเหตุที่แท้จริงของความเสี่ยง** เพื่อช่วยในการกำหนดแผนการจัดการความเสี่ยงได้ถูกต้อง
2. **ระดับความเสี่ยง** เพื่อใช้ในการประเมินว่าความเสี่ยงใดสำคัญมากน้อย หรือเร่งด่วน โดยจะมีการกำหนดเกณฑ์ในแต่ละระดับที่แตกต่างกันตามความเหมาะสม หรือตามระดับความเสี่ยงที่ยอมรับได้ สำหรับ OPPQA **ประเมินความเสี่ยงและจัดลำดับความเสี่ยงตามเกณฑ์ที่มหาวิทยาลัยกำหนด** ในการประเมินระดับความเสี่ยงจะพิจารณาจาก 2 มิติ คือ
    - พิจารณาโอกาส/ความถี่ในการเกิดเหตุการณ์ต่างๆ (Likelihood) ว่ามีโอกาส/ ความถี่ที่จะเกิดขึ้นมากน้อยเพียงใด ตามเกณฑ์มาตรฐานที่มหาวิทยาลัยกำหนด
    - พิจารณาความรุนแรงของผลกระทบของความเสี่ยง (Impact) ว่ามีระดับความรุนแรงหรือความเสียหายมากน้อยเพียงใด ตามเกณฑ์มาตรฐานที่มหาวิทยาลัยกำหนด

ระดับโอกาสเกิดและผลกระทบจะถูกนำมาพิจารณาร่วมกันใน Risk Matrix จึงทำให้ทราบว่าความเสี่ยงมีระดับ ความรุนแรงมากเพียงใด ควรดำเนินการจัดการความเสี่ยงใดก่อนหลัง

Likelihood

5	สูงมาก
4	สูง
3	ปานกลาง
2	น้อย
1	น้อยมาก

Impact

5	สูงมาก
4	สูง
3	ปานกลาง
2	น้อย
1	น้อยมาก

OPPQA RISK MATRIX

ระดับผลกระทบ(Impact)						
	I5	1X5	2X5	3X5	4X5	5X5
	I4	1X4	2X4	3X4	4X4	5X4
	I3	1X3	2X3	3X3	4X3	5X3
	I2	1X2	2X2	3X2	4X2	5X2
	I1	1X1	2X1	3X1	4X1	5X1
		L1	L2	L3	L4	L5
		ระดับโอกาสเกิด (Likelihood)				

ระดับความเสี่ยง	แนวทางการจัดการความเสี่ยง
สูงมาก (Extreme Risk, E)	เป็นระดับที่ไม่สามารถยอมรับความเสี่ยงได้ จำเป็นต้องเร่งจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้ทันที
สูง (High Risk, H)	เป็นระดับที่ไม่สามารถยอมรับความเสี่ยงได้จำเป็นต้องเร่งจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้ต่อไป
ปานกลาง (medium Risk, M)	เป็นระดับที่พอยอมรับความเสี่ยงได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปอยู่ในระดับที่ไม่สามารถยอมรับได้
ต่ำ (Low Risk, L)	เป็นระดับที่สามารถยอมรับความเสี่ยงได้ ไม่ต้องมีการควบคุม หรือจัดการเพิ่มเติม

OPPQA พิจารณาจากโอกาสและผลกระทบของความเสี่ยงแต่ละอย่างแล้วจัดวางแต่ละความเสี่ยงลงใน Risk Matrix ซึ่งจะช่วยให้มองเห็นภาพว่าความเสี่ยงไหนมีความรุนแรงมากที่สุดแล้วไปจัดการความลดความเสี่ยงนั้นก่อน อีกทั้งยังช่วยในการวิเคราะห์ความเสี่ยงเพื่อหาแนวทางเตรียมรับมือก่อนจะเกิดขึ้น แต่ Risk Matrix เป็นเพียงเครื่องมือในการทำให้ OPPQA มีจุดเริ่มต้นในการจัดการความเสี่ยงและการพัฒนากลยุทธ์การบรรเทาผลกระทบที่เกิดขึ้นต่อหน่วยงานต่อไป

3.การตอบสนองความเสี่ยง (Risk Response Planning)ที่อาจเกิดขึ้นในอนาคต

เมื่อเลือกความเสี่ยงที่สำคัญมาจัดการ **OPPQA** จะหาแนวทางป้องกันและการแก้ไขจัดการความเสี่ยง (Risk Management) โดยหาวิธีการที่ดีที่สุด เพื่อใช้เป็นแนวทางในการตัดสินใจแก้ไขปัญหาต่างๆที่อาจเกิดขึ้นในอนาคต เพื่อลดความเสียหายที่อาจเกิดขึ้นให้น้อยที่สุด โดยมีค่าใช้จ่ายน้อยที่สุดในการดำเนินการ ซึ่งทางเลือกที่ OPPQA จะรับมือกับความเสี่ยงมี 4 วิธีการ (4T) ตามมาตรฐาน COSO ERM (The Committee of Sponsoring Organization of the Treadway Commission Enterprise Risk Management) ดังนี้

- **วิธีการหลีกเลี่ยงความเสี่ยง (Terminate/ Avoid)** เป็นการตัดสินใจที่จะไม่เข้าไปเกี่ยวข้องกับสถานการณ์ความเสี่ยงนั้นๆ โดยการ “ยุติ งดเว้น ยกเลิก หรือเปลี่ยนแปลง” กิจกรรม หรืองานที่ก่อให้เกิดความเสี่ยง สำหรับการเลือกใช้กลยุทธ์นี้ โดยจำเป็นต้องถามและตอบตนเองว่า **“งาน/ โครงการ หรือกิจกรรมนั้นๆ ไม่ต้องมีหรือเลิกทำจะดีกว่า”**
- **วิธีการยอมรับความเสี่ยง (Take/ Accept)** เป็นกลยุทธ์เลือกที่จะ **“ไม่ดำเนินการใดๆ เพิ่มเติม”** เพื่อจัดการความเสี่ยง สามารถใช้ได้ใน 2 กรณี
    - **กรณีที่ระดับความเสี่ยงต่ำมาก** และสามารถควบคุมความเสี่ยงได้ด้วยภาระงานที่มีอยู่ (Internal Control or Existing Control) รวมถึงความเสี่ยงนั้นๆ ไม่คุ้มค่าที่จะดำเนินการ
    - **กรณีที่ระดับความเสี่ยงสูงมากและไม่มีแนวทางที่จะสามารถจัดการความเสี่ยงได้จริง** หรือพิจารณาแล้วว่าแนวทางการจัดการความเสี่ยงให้ผลลัพธ์ที่ไม่คุ้มค่า อีกทั้ง งาน/ โครงการ หรือกิจกรรม นั้นๆ ใช้กลยุทธ์การหลีกเลี่ยงไม่ได้
- **วิธีการโอน หรือกระจายความเสี่ยง (Transfer/ Share)** เป็นกลยุทธ์ที่ใช้เมื่อรับรู้ว่ามีความเสี่ยง และจำเป็นต้องดำเนินการจัดการความเสี่ยง แต่องค์กรไม่มีความชำนาญในการดำเนินการหรือมีต้นทุนในการดำเนินการสูงกว่าที่จะยอมรับได้ และให้หน่วยงานอื่นเป็นผู้จัดการแทนเป็นการถ่ายโอนความรับผิดชอบ หรือแบ่งภาระการสูญเสียแก่ผู้อื่น โดยที่ความเสี่ยงยังเป็นขององค์กร

- **วิธีการลดความเสี่ยง (Treat/ Reduce)** เป็นกลยุทธ์เพื่อลดหรือควบคุมโอกาส และ/หรือ ผลกระทบของความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ โดยการจัดกิจกรรมเพื่อใช้ในการควบคุม จำกัด แก้ไข ปรับปรุง หรือ ป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

สรุป การเลือกใช้ 4T ในการจัดการความเสี่ยงของ OPPQA

สำหรับความเสี่ยงที่มีสาระสำคัญ OPPQA **จะกำหนดตัวชี้วัดความเสี่ยง (Key Risk Indicator: KRIs)** เป็นเครื่องมือที่จะช่วยติดตาม ความเสี่ยง รวมถึงเป็นสัญญานเตือนภัย เพื่อให้สามารถ คาดการณ์เหตุการณ์ความเสี่ยงในอนาคต และมีมาตรการป้องกันก่อนเกิด เหตุการณ์ความเสียหาย โดยใช้สถิติและ/หรือการวัดความเสี่ยงจากการ ดำเนินงานของมหาวิทยาลัย ในแต่ละช่วงเวลา **OPPQA** กำหนดตัวชี้วัดความเสี่ยง(KRIs) ดังนี้

- ควรเป็นตัวชี้วัดนำ (Leading Indicator)
- ควรเป็นข้อมูลเชิงสถิติ หรือข้อมูลที่สามารถวัดค่าได้จริง
- สัมพันธ์กันกับเหตุการณ์ความเสี่ยง(อาจเชื่อมโยงมาจากสาเหตุของปัจจัยเสี่ยง)

- สามารถกำหนดตัวชี้วัดความเสี่ยงได้มากกว่า 1 ตัวชี้วัด/ 1 ประเด็นความเสี่ยง
- KRIs ไม่ควรใช้เป็นตัววัดความก้าวหน้าของแผน/มาตรการจัดการความเสี่ยงแต่ควรเป็นเครื่องมือตรวจสอบความมีประสิทธิผล(Effectiveness) ของแผน/มาตรการจัดการความเสี่ยง ในกระบวนการ Monitoring and Review
- สามารถติดตาม/รายงานสถานะที่เกิดขึ้นจริงอย่างทันเวลาและเป็นไปอย่างต่อเนื่อง เพื่อให้มีการปรับตัวอย่างทันท่วงที ก่อนที่สถานกรณ์จะถึงจุดที่เป็นอันตราย

ดังนั้น **KRIs ของ OPPQA จึงเป็นเสมือน Risk Metrics หรือมาตรวัดความเสี่ยง** เพื่อให้เกิดความมั่นใจว่าการบริหารจัดการความเสี่ยงดังกล่าว กับ การบริหารผลการดำเนินงานมีความสอดคล้องและสนับสนุนเกื้อกูลกัน จนทำให้ผลการดำเนินงานบรรลุเป้าหมาย

4. การจัดกิจกรรมเพื่อควบคุม (Control Activities)

เมื่อตัดสินใจเลือกแนวทางในการจัดการความเสี่ยง **OPPQA จะกำหนดกิจกรรมควบคุมความเสี่ยง (Control Activities)** ที่จะช่วยให้มีความมั่นใจว่าการปฏิบัติงานและการประกอบกิจกรรมของหน่วยงานมีการดำเนินงานที่สอดคล้องกับเป้าหมายยุทธศาสตร์ และเป็นกิจกรรมที่สามารถช่วยป้องกันและบ่งชี้ความเสี่ยงให้เห็นความเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของหน่วยงาน ทั้งนี้ OPPQA มีกิจกรรมการควบคุม 3 ประเภท คือ

- **การควบคุมเพื่อการป้องกัน (Preventive Controls)** เป็นการควบคุมที่กำหนดขึ้น **เป็นการขัดขวางหรือยับยั้งปัญหาก่อนที่ปัญหานั้นจะเกิดขึ้น** เช่น การแบ่งแยกหน้าที่ การควบคุมการเข้าถึงสินทรัพย์ (กำหนดระดับการอนุมัติ) การใช้รหัสผ่าน (Password) ก่อนเข้าสู่ระบบ เป็นต้น
- **การควบคุมเพื่อการค้นพบ (Detective Controls)** เป็นการควบคุมที่กำหนดขึ้น เป็น**การค้นหาความผิดพลาดหรือปัญหาที่เกิดขึ้นแล้วให้เร็วที่สุด** เพื่อลดผลกระทบและความเสียหายจากปัญหานั้น เช่น การสอบทานงาน รายงานสิ่งผิดปกติ การสอบยันยอด การตรวจนับ เป็นต้น

- **การควบคุมเพื่อการแก้ไข(Corrective Controls)** เป็นวิธีการควบคุมที่กำหนดขึ้น เป็นการขจัดปัญหาที่เกิดขึ้น โดยค้นหาให้เจอสาเหตุของปัญหา แล้ว**พยายามแก้ไข จนถึงการปรับระบบการทำงาน เพื่อไม่ให้ปัญหานั้นเกิดขึ้นอีกในอนาคต** เช่น กำหนดนโยบาย คู่มือแนวทางการปฏิบัติงาน การฝึกอบรม เป็นต้น

หลักการจัดกิจกรรมควบคุมความเสี่ยง ของ OPPQA คือ

1. การคัดเลือกและพัฒนากิจกรรมการควบคุมที่นำไปสู่การลดความเสี่ยงที่มีผลกระทบต่อความสำเร็จตามวัตถุประสงค์ที่วางไว้ให้อยู่ในระดับที่ยอมรับได้ โดยคำนึงถึงต้นทุน รวมถึงชื่อเสียงและภาพลักษณ์ของมหาวิทยาลัย
2. การปรับใช้กิจกรรมการควบคุมผ่านทางนโยบาย (กำหนดสิ่งที่คาดหวัง) และขั้นตอนปฏิบัติงานที่นำนโยบายไปสู่การปฏิบัติ กำหนดผู้รับผิดชอบในการจัดการความเสี่ยง รวมถึงระยะเวลาในการดำเนินการให้ชัดเจน

หมายเหตุ

1. กิจกรรมควบคุมไม่ควรเป็นกิจกรรมที่สร้างมาพิเศษ แต่ควรเป็นกิจกรรมที่แทรกหรือบูรณาการในกระบวนการปฏิบัติงานตามปกติ

2. กิจกรรมการควบคุมนั้นแต่ละหน่วยงานอาจมีวิธีการที่แตกต่างกันออกไปขึ้นกับ นโยบายการบริหาร การดำเนินงาน สภาพแวดล้อมภายในหน่วยงาน และวัฒนธรรมองค์กร

3. การจัดการความเสี่ยงจึงเป็นการบริหารงานภายในขอบเขตที่ผู้ที่เกี่ยวข้องยอมรับความเสี่ยงได้เท่านั้นมิใช่การบริหารความเสี่ยงเพื่อขจัดความเสี่ยงในการบริหาร การบริหารความเสี่ยงจึงเป็นกระบวนการที่มุ่งสู่การตัดสินใจภายใต้สภาวะที่มีความเสี่ยงตามข้อมูล ที่ได้รับกับการตัดสินใจภายใต้ภาวะที่มีความไม่แน่นอนของปัจจัยที่ควบคุมได้

5. การติดตามและและประเมินผล (Monitoring)

เมื่อดำเนินกิจกรรมตามแผนบริหารความเสี่ยง **การติดตามและประเมินผลของ OPPQA** ถือว่าเป็นขั้นตอนสำคัญที่จะช่วยให้กลไกกระบวนการบริหารความเสี่ยงขับเคลื่อนไปอย่างมีประสิทธิภาพ ทำให้ทราบถึงสถานะการจัดการ การดำเนินการตามกิจกรรมการควบคุมว่ามีการดำเนินการตามที่กำหนดไว้หรือไม่? มีผลการดำเนินการตามเป้าหมายหรือไม่? ซึ่ง OPPQA กำหนดผลดัชนีชี้วัดความเสี่ยง (KRI) ซึ่งเป็นเสมือนตัวเตือนภัยตัวบ่งชี้ก่อนเกิดเหตุการณ์ความเสี่ยงมีแนวโน้มในระดับที่น่ากังวลใจหรือไม่อย่างไร? รวมถึงผลการประเมินระดับความเสี่ยงที่เหลืออยู่สามารถลดลงในระดับที่หน่วยงานยอมรับได้แล้วหรือยัง? เพื่อให้เกิดการตัดสินใจพิจารณาทบทวนในการปรับแผนจัดการ กิจกรรมควบคุมและการสั่งการมอบหมาย ดำเนินการที่สำคัญที่สอดคล้องและทันต่อสถานการณ์ โดยกำหนดกิจกรรมหลักในขั้นตอนดังนี้

- กำหนดติดตามผล ดัชนีชี้วัดความเสี่ยง
- ติดตามการนำแผนบริหารความเสี่ยงไปปฏิบัติ และผลการจัดการความเสี่ยง
- ประเมินผลระดับความเสี่ยงที่เหลือ เทียบกับระดับความเสี่ยงที่ยอมรับได้
- ประเมินผลตามเป้าหมายที่ต้องการ
- พิจารณาทบทวน ปรับเปลี่ยนแผนบริหารจัดการความเสี่ยง กิจกรรมควบคุม (เพิ่มเติม) ให้เหมาะสมและสอดคล้องกับสถานการณ์

หมายเหตุ การตัดสินใจทางการบริหารจัดการของ OPPQA ใน**บางครั้งยอมที่จะเพิ่มระดับความเสี่ยงให้สูงขึ้น เพื่อให้สามารถเตรียมพร้อมรับมือการเปลี่ยนแปลงที่อาจเกิดขึ้นกับหน่วยงาน ทั้งที่เป็นโอกาสใหม่ๆ และภัยคุกคามในอนาคต** รวมถึงเพื่อพิจารณาในการลดกิจกรรมการควบคุมที่มากเกินจำเป็นจนทำให้เกิดความล่าช้า ขาดประสิทธิภาพ และประสิทธิผล จนเกิดผลเสียหายต่อหน่วยงาน แต่อย่างไรก็ตาม ยังจำเป็นที่จะต้องควบคุมระดับความเสี่ยงให้อยู่ในระดับเหมาะสมที่ OPPQA ยอมรับ ได้

OPPQA RISK MANAGEMENT

สรุปกระบวนการบริหารความเสี่ยง

ขั้นตอนที่ 1	ขั้นตอนที่ 2	ขั้นตอนที่ 3	ขั้นตอนที่ 4	ขั้นตอนที่ 5
ระบุประเด็นความเสี่ยง	ประเมินความเสี่ยง	ตอบสนองความเสี่ยง	ทำกิจกรรมเพื่อควบคุม	ติดตามผล
วิเคราะห์องค์กรและระบุประเด็นความเสี่ยง	ประเมินระดับความเสี่ยงประเมินจากเกณฑ์โอกาสเกิดและผลกระทบ	ออกแบบแผนบริหารความเสี่ยง	ออกแบบแผนบริหารความเสี่ยงมาตรการเพิ่มเติม/กิจกรรมควบคุม	ติดตามและทบทวนการบริหารความเสี่ยง
ขั้นตอน	**ขั้นตอน**	**ขั้นตอน**	**ขั้นตอน**	**ขั้นตอน**
1. กำหนดเป้าหมายของการบริหารความเสี่ยง 2. ระบุความเสี่ยง 3. ระบุประเภทความเสี่ยง (7ประเภท) 4. ระบุปัจจัยและสาเหตุความเสี่ยง	5. ระบุกิจกรรมความเสี่ยงที่มี 6. ประเมินความเสี่ยงและจัดลำดับความเสี่ยงตามเกณฑ์ที่มหาวิทยาลัยกำหนด	7. จัดทำแผนบริหารความเสี่ยง • กรณีระดับความเสี่ยงสูงมากหรือสูงให้จัดทำมาตการเพิ่มเติม • กรณีระดับความเสี่ยงปานกลาง-ต่ำให้จัดทำกิจกรรมควบคุม 8. กำหนดตัวชี้วัดเตือนภัย(Lagging Indicator)และระดับที่ยอมรับได้ (Risk Appetite)	9.มอบหมายผู้รับผิดชอบนำไปปฏิบัติ 10. ดำเนินกิจกรรมตามแผนงานโครงการ/กิจกรรม	11. ติดตามผลการบริหารความเสี่ยงตามตัวชี้วัด (KRIs) 12.ประเมินความเสี่ยงหลังการบริหารจัดการ 13. ประเมินผลตามเป้าหมาย

สารสนเทศเพื่อการบริหารความเสี่ยงและการควบคุมภายใน